**Dissertation Title**: Analysis of the Challenges of Child Protection and Effectiveness of the International Legal Frameworks Against Exploitation in the Digital Era

# Contents

# 1 Introduction

## 1.1 Background and Context

New technology has greatly influenced the manner in which information is disseminated, communicated and individuals and groups interact in the society. Although these technologies have had their pros, they have also ushered into society new issues mainly in relation to child abuse. The advanced development of the Internet and communication technologies generated increased use of channels of social networks, games, and communication applications, which are today's most popular schemes for the recruitment of children by terrorist organizations[1].

### 1.1.1 Methods of Recruitment and Child Vulnerability

Main tactics used by terrorists to attract children include cyber deception, interactive media, and chat rooms. These groups take advantage of psychologically vulnerable aspects of children including affiliation, identity and call to purpose by training them with extremities[2]. The radicalisation process on the Internet is usually not abrupt but rather a process where the children are gradually introduced initially to the idea of a group where they belong to and are then gradually drifted towards the use of violence. Among all the age groups, children are most vulnerable since they are easily influenced and incapable of critical analysis, thus making them appropriate for use as soldiers or spies or even suicide bombers by these organizations.

### 1.1.2 Violation of Children's Rights

The commodification of children within online platforms leads to a violation of multiple fundamental rights. Some of the rights include the right to protection from being abused as well as exploited, the right to education and the right to life and living without being threatened. Terrorist groups recruiting children for such actions undermines their childhood, education and safety[3]. Many of these children are condemned as criminals especially when they are apprehended participating in terrorist acts. This categorization ignores their exploitation and the coercion they often face, leading to further violations of their rights.

### 1.1.3 Critical Analysis of the International Legal Frameworks

The foundation of child protection is provided by the United Nations Convention on the Rights of the Child (CRC), the Optional protocol on the sale of children, child prostitution, and child pornography (OPSC), and the UN General Comment No. 25 addressing children's rights in the digital environment. However, these instruments were developed before the digital revolution and they have drawbacks in addressing the contemporary finer issues of cybercrime and terroristic radicalization[4]. Although these frameworks afford a fair amount of protection, they do not provide enough detail to address the

---

[1] Sharma, Priya. "Digital revolution of education 4.0." *International Journal of Engineering and Advanced Technology* 9, no. 2 (2019): 3558-3564.

[2] Alava, Séraphin, Divina Frau-Meigs, and Ghayda Hassan. *Youth and violent extremism on social media: mapping the research*. UNESCO Publishing, 2017

[3] Unicef for every child. 2021. *Children recruited by armed forces or armed groups* . 22 12. Accessed 8 27, 2024. https://www.unicef.org/protection/children-recruited-by-armed-forces.

[4] Weithorn, Lois A. "A constitutional jurisprudence of children's vulnerability." *Hastings LJ* 69 (2017): 179.

complex methodologies utilized in cyberspace by terrorists[5]. For instance, while the CRC focuses on physical cruelty, it fails to address the complexities of psychological grooming that occur on the Internet. Moreover, the categorization of children involved in terrorism as either criminals or victims is inconsistent across jurisdictions. Some countries treat these children as perpetrators, subjecting them to punitive measures, while others recognize their victimhood and offer rehabilitation. This disparity necessitates the need for a harmonized international approach that considers the complex realities of child exploitation in the digital age. This discrepancy underscores the need for a harmonized international approach that considers the complex realities of child exploitation in the digital age[6].

Primary sources of child protection are the international legal instruments that include the United Nations Convention on the Rights of the Child (CRC), Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC), and UN General Comment No. 25 on children's rights in the digital environment. However, these frameworks were developed before the emergence of digital technologies and can only capture some of the requisite threats of the digital world. This dissertation seeks to critically evaluate these legal instruments, identify gaps, and propose necessary enhancements to safeguard children in the digital age better.

## 1.1 Research Aim:

To identify the issues and explore the challenges to the protection of children against digital exploitation, particularly in the context of terrorism and radicalisation.



[5] Ashurov, Azizbek. "Jurisdictional Challenges in Cross-Border Cybercrime Investigations." *Центральноазиатский журнал междисциплинарных исследований и исследований в области управления* 1, no. 8 (2024): 22-30.

[6] Ashurov, Azizbek. "Jurisdictional Challenges in Cross-Border Cybercrime Investigations." *Центральноазиатский журнал междисциплинарных исследований и исследований в области управления* 1, no. 8 (2024): 22-30.

## 1.2 Primary Research Questions:

a) Are the international legal frameworks effective in addressing exploitation in the digital era?

b) How can they address the issue of children in terrorism-related activities?

## 1.3 Secondary Research Questions:

a) What are the specific digital recruitment channels used by terrorist groups?

b) How do children's online vulnerabilities differ across regions?

c) What preventive measures can mitigate digital exploitation?

d) What role can technology companies play in safeguarding children?

e) What impact does this issue have on exploited children?

f) Are the current legal frameworks effective in prohibiting the use and exploitation of children in terrorism-related activities?

g) How are exploited children categorised and treated (victims vs. criminals)?

h) How will exploited children be treated (detention and interrogation) in cases where they have participated in terrorist activities, and what measures are available under international legal frameworks?

## 1.4 Methodology

This dissertation employs a mixed-method approach through the intersection of doctrinal legal analysis and socio-legal approaches to assess how well the international legal frameworks prevent children from being digitally exploited by terrorists. The doctrinal method[7] involved a critical evaluation of the primary legal frameworks, treaties, and conventions, including international treaties and UN resolutions, as well as reports on child exploitation in the digital age. This method is appropriate for this study as it enables examination of the legal texts and their

[7] Smits, Jan M. "What is legal doctrine? On the aims and methods of legal-dogmatic research." (2017): 207-228.

interpretations, providing a robust foundation for understanding the current legal landscape[8]. On the other hand, the socio-legal approach enabled contextualising the legal texts into the social and practical environments[9]. To achieve this, the method examined how legal frameworks are realised in actual cases, the challenges faced by their enforcement, and their effects on safeguarding children from perpetrators. Integrating the two methods enabled this study to bridge the gap between legal theory and practice, thereby providing a holistic understanding of the challenges facing this demographic population in the digital era.

Adopting both doctrinal and socio-legal approaches is particularly suited for this project because it enables the study to provide an overarching critique of international legal frameworks. Where the doctrinal method provides the legal analysis needed, the socio-legal approach enabled the assessment of children's lived experiences and the operational realities prevalent in these digital platforms[10]. Further, this methodology helps to provide a critical analysis of the adaptability of current legal frameworks in facing new challenges brought by digital technologies. This approach enabled the study to achieve a more effective legal response to children's digital rights based on greater awareness of the content and how existing frameworks are implemented. The results of this study will help shape recommendations for the development of international legal treaties for a more effective prevention of terrorist organisations exploiting children and radicalising them into violent behaviour.



[8] Tyler, Tom R. "Methodology in legal research." *Utrecht L. Rev.* 13 (2017): 130.
[9] Akinkugbe, Olabisi D. "Reflections on the Value of Socio-Legal Approaches to International Economic Law in Africa." *Chi. J. Int'l L.* 22 (2021): 24.

[10] Livingstone, Sonia, and Amanda Third. "Children and young people's rights in the digital age: An emerging agenda." *New media & society* 19, no. 5 (2017): 657-670.

# 2 Digital Recruitment Channels and Vulnerabilities

## 2.1 Digital Platforms Used for Recruitment

Due to the advancements in information technology in the modern world, children among other young people spend most of their time on social networks, virtual games and other interactive spaces[11]. These platforms provide direct interactions among users, hence enabling discreet interactions among perpetrators and their targets internationally. Currently, social sites such as Facebook, Twitter, and Instagram have been cited among the most used for radicalisation mainly because they are easily reachable and easily impart content within a short period of time[12]. Virtual gaming platforms, commonly accessed by the younger population, are other places that offer a different form of intersession where a recruiter can create relationships as gaming companions, spot a target and then introduce them to radicalism gradually.

Terrorist groups also engage these platforms by producing and posting content like videos and memes, which creates an appeal to the emotional and cognitive domain of their targets, especially children and youth[13]. Due to their operational features, these platforms enable the rapid dissemination of hateful content while promoting other content that strengthen radicals' ideas[14]. Since the targets are unknown to the recruiters, interactions can be sustained for long periods akin to grooming, without necessarily having to unmask their identity[15]. The role of online propaganda in radicalising individuals and the legal challenges of prosecuting digital era perpetrators has been



[11] Kan, Matthew PH, and Leandre R. Fabrigar. "Theory of planned behavior." In *Encyclopedia of personality and individual differences*, pp. 5476-5483. Cham: Springer International Publishing, 2020.

[12] Zeiger, Sara, and Joseph Gyte. *Prevention of radicalization on social media and the internet*. International Centre for Counter-Terrorism (ICCT), 2020.

[13] Scheepers, Daan, and Naomi Ellemers. "Social identity theory." *Social psychology in action: Evidence-based interventions from theory to practice* (2019): 129-143

[14] Cui, Ruomeng, Santiago Gallino, Antonio Moreno, and Dennis J. Zhang. "The operational value of social media information." *Production and operations management* 27, no. 10 (2018): 1749-1769.

[15] Devon Safeguarding Children Partnership. 2023. *Chld Ause: Radicalozation and Extremism.* Accessed 08 12, 2024. https://www.devonscp.org.uk/child-abuse/radicalisation-and-extremism/.

demonstrated by the (R v Gul (Appellant) 2013)[16] case. The Supreme Court emphasised the need for legal frameworks to adapt to the evolving nature of digital communication and accommodate addressing the various aspects that extremist groups manipulate these platforms to their advantage.

## 2.2 Techniques and Strategies Used by Terrorist Groups

Terrorist organisations use different strategies to manipulate and recruit children by focusing on the children's vulnerabilities associated with adolescence including the need for an identity, friends, and vocation to gain their attention and enlist their support[17]. Grooming, previously carried out by sexual predators, is slowly being adopted by terrorist recruiters. The process involves establishing an informal relationship by regular communication under the pretence of friendship or shared interest before gradually promoting extremist programmes[18].

The echo chambers are another technique in which children are exposed to a selected stream of content that reinforces radical ideologies while excluding opposing viewpoints[19]. This technique is enabled by the repetition theorem of social media platforms that recommends content with features familiar to the content the user has mostly engaged with, thereby putting the victim in a loop that constantly feeds extremism beliefs[20].



[16] *R v Gul (Appellant).* 2013. [2013] UKSC 64 (The Supreme Court, 23 10).

[17] Centre for the Prevention of Radicalization Leading to Violence. 2017. *Radicalization and Volent Extremism: How do talk about it with my child?* information Gude for Parents, Montreal: Centre for the Prevention of Radicalization Leading to Violence.

[18] Bath and Nort East Somerset Community Safety & Safeguarding Partnership. 2024. *Child Safeguarding Practice Reviews.* 03 01. Accessed 8 12, 2024. https://bcssp.org.uk/p/safeguarding-children/child-safeguarding-practice-reviews.

[19] Whittaker, Joe. "Online echo chambers and violent extremism." *The Digital Age, Cyber Space, and Social Media: The Challenges of Security & Radicalization* (2020): 129-150.

[20] Centre for the Prevention of Radicalization Leading to Violence. 2017. *Radicalization and Volent Extremism: How do talk about it with my child?* information Gude for Parents, Montreal: Centre for the Prevention of Radicalization Leading to Violence.

Moreover, extremist groups often exploit online anonymity to create multiple identities, allowing them to target the same individual through various personas, each reinforcing the radicalisation process from different angles[21]. The exploitation of anonymity was demonstrated in the Regina v Faraz 2012[22] case, where the defendant was found guilty of disseminating terrorist publications that were specifically designed to radicalise vulnerable individuals, including children. The effectiveness of these strategies is amplified by the shortcomings in existing legal frameworks, which struggle to keep pace with the rapid evolution of digital technology. While the UK's Counter-Terrorism and Security Act 2015[23] have introduced measures to combat online radicalisation, these efforts are often hindered by the globalisation of the Internet and the ability of recruiters to operate across multiple jurisdictions.

The increasing use of digital platforms for recruitment by terrorist organisations presents significant challenges for safeguarding children. While platforms like social media and online gaming offer opportunities for connection and community, they also expose children to significant risks of radicalisation. The techniques employed by recruiters are sophisticated and exploit features that popularise them among youth such as interactivity, anonymity, and the ability to create echo chambers.

While evolving, current legal frameworks need improvement to address the full scope of these threats. Devon Safeguarding Children Partnership[24] demonstrate the difficulty of prosecuting digital radicalisation due to the complex nature of online interactions and the Internet's global



[21] Gaudette, Tiana, Ryan Scrivens, Garth Davies, and Richard Frank. "Upvoting extremism: Collective identity formation and the extreme right on Reddit." *New Media & Society* 23, no. 12 (2021): 3491-3508.
[22] *Regina v Faraz.* 2012. 201200251 C5 (Court of Appeal, 21 12).

[23] *Counter-Terrorism and Security Act 2015.* 2015. (Legislation.gov. uk).

[24] Devon Safeguarding Children Partnership, Radicalisation and extremism, accessed 2024.

reach. Furthermore, the reliance on reactive measures, such as content takedowns and prosecution after radicalisation highlights a gap in preventive strategies.

To successfully address these threats, it is necessary to strengthen the legal measures as well as the cooperation between platform providers, governments and civil society organisations. It is also important to focus on the educational programs which would create awareness among children on recognising and resisting radicalisation efforts, as well as parents to be actively involved in monitoring and discussing online experiences with their children. Therefore, the responsibility of protection and supervision of children in the use of information and communication technology is not the sole preserve of legal frameworks but a shared effort across society as a `whole.



# 3 Literature review

## 3.1 Overview of child exploitation in the digital era

The use of technology in the society has posed many challenges in child protection especially in terrorist related issues. However, the international legal tools designed to protect children are rather blunt in their ability to account for the emerging trends and types of abuse. Despite international legal frameworks intended to safeguard children, these instruments display significant shortcomings in addressing the evolving methods of digital exploitation. The recruitment and exploitation of children through online platforms violate several fundamental rights, including the right to protection from exploitation, abuse, and neglect as enshrined in the United Nations Convention on the Rights of the Child (CRC), particularly Articles 19 and 34[25].

[25] United Nations. 1989. *Convention on the Rights of the Child.* 20 11. Accessed 08 27, 2024. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

The failure to protect children from online recruitment and radicalization also undermines their right to education and development (Article 28) and the right to freedom from harmful influences.

While there are specific provisions in the United Nations Security Council Resolution 2427[26] concerning the protection of children affected by armed conflict, it lacks measures to tackle complex issues such as online recruitment by terrorists' organizations. The Resolution does not specify areas that can address the elaborate measures employed by such groups of reaching out to children through the social sites. Likewise, the United Nations Security Council resolution 2250[27], recognizes the youth exposure to violence, but lacks a clear framework on how to tackle online radicalization. Both resolutions pay particular attention to the traditional forms of security, while failing to address the digital risks that are increasingly prevalent.

Such shortcomings highlight a gap between legal provision of international law in lieu with present day technology. The increasing rate at which technology is changing is very alarming in this respect because children's rights are frequently violated, and the legal redress available to protect them is inadequate. Therefore, there is a need for a more revamped legal frameworks in relation to the recruitment and radicalization of children online. Despite being close in addressing the challenges faced by children, the existing frameworks do not capture all the protection needed in the face of digital exploitative actions. For example, the Optional Protocol on the Sale of



[26] United Nations Security Council Resolution 2427 (9 July 2018) UN Doc S/RES/2427

[27] United Nations Security Council Resolution 2250 (2015) UN Doc S/RES/2250

Children, Child Prostitution, and Child Pornography[28] touches on some aspects of digital abuse but does not encompass the recruitment for terrorism or radicalization.

## 3.2 Theoretical framework

Social Identity Theory[29] and the Theory of Planned Behaviour (TPB)[30] effectively inform the process of child radicalisation. They illustrate the psychological manipulation and interpersonal dynamics terrorist organisations use to create bonds. However, no national legal framework integrates these theoretical insights into operational policy. This lack of coherence demonstrates the inability to tackle the underlying causes of digital exploitation adequately. For interventions to become more successful, strategies addressing the psychological and social aspects of online radicalisation need to be integrated into legal frameworks. Moreover, the routine activities theory[31] also emphasises children's increased exposure to online risks of frequent Internet use. Nevertheless, international legal frameworks have remained unchanged in accommodating daily digital doings. The absence of accounting for everyday digital actions from children in the frameworks makes them more susceptible to exploitation[32]. This gap highlights the necessity of a



[28] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) UNGA Res 54/263 (25 May 2000).

[29] Scheepers, Daan, and Naomi Ellemers. "Social identity theory." *Social psychology in action: Evidence-based interventions from theory to practice* (2019): 129-143.

[30] Kan, Matthew PH, and Leandre R. Fabrigar. "Theory of planned behavior." In *Encyclopedia of personality and individual differences*, pp. 5476-5483. Cham: Springer International Publishing, 2020.

[31] Cho, Sujung, Jun Sung Hong, Dorothy L. Espelage, and Kyung-Shick Choi. "Applying the lifestyle routine activities theory to understand physical and nonphysical peer victimization." *Journal of Aggression, Maltreatment & Trauma* 26, no. 3 (2017): 297-315.

[32] Keeley, Brian, and Céline Little. *The State of the Worlds Children 2017: Children in a Digital World*. UNICEF. 3 United Nations Plaza, New York, NY 10017, 2017.

legal framework that is continuously updated to take into account technological innovations and differences in digital behaviour.

The dominant theme throughout the literature is criticism of international legal frameworks for being too broad in scope and out-of-date. Due to the fast pace of technology advancements, these frameworks need to provide specific provisions for child protection. New and specially adapted legal measures are urgently required to deal with the challenges arising from digital exploitation. However, simply passing the rules is not enough, but capability to enforce these laws and ensure they practically deliver protections to children as part of their defence against online risks.

## 3.3 International Legal Frameworks

### 3.3.1 Convention on the Rights of the Child (CRC)

The International law centred on children's rights is the United Nations Convention on the Rights of the Child which was ratified in 1989. Article 19 of the CRC requires States parties to take appropriate legislative, administrative, social, and educational measures to protect children from all forms of physical or mental violence, injury, abuse, neglect, maltreatment, and exploitation, including sexual abuse[33]. However, while Article 19 defines a broad protective standard, it appears outdated in an era when terrorist and radicalization threats occur over cyberspace.

The standard provisions that the CRC suggests include regulations to stop the sophisticated methods terrorists use for online recruitment[34]. The advancement of technology has made terrorist organizations more dangerous, preying on unsuspecting children in ways not considered during

[33] UN Committee on the Rights of the Child, 'General Comment No 25 on Children's Rights in Relation to the Digital Environment' (2021) UN Doc CRC/C/GC/25

[34]

the CRC's original drafting. This does not address the complex manipulations terrorists use to train children by exploiting the internet, social networks, or other mechanisms of encrypted communication[35]. This oversight highlights a failing of the CRC in addressing emerging threats due to new technology, particularly concerning terrorism and the exploitation of children.

The use of children in armed conflict (OPAC) recognizes the illegal recruitment of children by armed forces, groups, or militias (Articles 1-4), it does not account for the systematic and covert nature of internet radicalization that precedes direct recruitment. The gaps in international legal standards, such as those in the CRC and its OPAC, are significant shortcomings in addressing these new threats.

### 3.3.2 Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography (OPSC)

The Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography (OPSC) seeks to further expand security measures, particularly concerning the sale of children, child prostitution, and child pornography[36]. Articles 1-3 of the OPSC identify and criminalize these acts, providing a robust framework for combating offline exploitation. However, the protocol's effectiveness is when applied to online context is insufficient. This ineffectiveness is attributed to its lack on provisions for contemporary cybercrimes such as online grooming, digital radicalization, and the recruitment of children by terrorist organizations through digital platforms.

The pace at which digital exploitation methodologies evolve far outstrips the development of international legal frameworks like the OPSC. For instance, the protocol does not address how

[35] United Nations Human Rights, 'Guidance Establishes Children's Rights Carry into Digital World' (26 March 2021)

[36] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) UNGA Res 54/263 (25 May 2000).

terrorist groups use social media and encrypted messaging platforms to prey on children. These digital tools enable exploitation in novel ways that transcend traditional legal boundaries, making cross-border enforcement and investigation challenging. While Article 10 of the OPSC refers to international collaboration to combat the sale and trafficking of children, as well as child pornography[37], it falls short of providing clear guidelines for handling challenges related to digital evidence and jurisdiction in cyber-radicalization. Moreover, although the OPSC extensively covers child pornography, it does not encompass newer forms of exploitation such as sextortion and live-streaming abuse, which also serve as tools for radicalization[38]. This gap underscores the importance of an updated legal framework capable of countering the new digital tactics employed by terrorist organizations.

### 3.3.3 UN General Comment No. 25 on Children's Rights about the Digital Environment

UN General Comment No. 25 offers vital guidance on applying children's rights within the digital environment, particularly emphasizing the need for enhanced protections against terrorism and radicalization[39]. This commentary is grounded in Article 19 of the Convention on the Rights of the Child, which mandates safeguarding children from all forms of physical and mental violence, neglect, maltreatment, or exploitation[40]. However, the General Comment inadequately addresses the unique and growing risks posed by online radicalization. Although it guides states on best practices, the absence of a clear enforcement mechanism results in reliance on voluntary compliance. This is especially concerning due to the varying technological and legal capabilities



[37] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) UNGA Res 54/263 (25 May 2000).
[38] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) UNGA Res 54/263 (25 May 2000).
[39] General Comment No 25 (2021) on children's rights about the digital environment, CRC/C/GC/25, 2 March 2021.
[40] General Comment No 25 (2021) on children's rights about the digital environment, CRC/C/GC/25, 2 March 2021.

across states, leaving children in less developed regions more vulnerable to online exploitation by terrorist groups.

Moreover, the General Comment references broad protection measures, offering general strategies without addressing the sophisticated, technology-driven methods terrorists use to radicalize children. While it recognizes the importance of global cooperation to ensure children's online safety[41], it lacks a clear framework for international collaboration or specific legal obligations for states to counter cross-border online recruitment. This deficiency highlights the shortcomings of international legal instruments, which lack the necessary specificity and enforceability to close significant protection gaps against digital radicalization.

UN Security Council Resolution 2250 (2015) captures the youth and their role in promoting peace and security[42]. Its goal is not specifically to educate children, but its impact on preventing the radicalisation of youth through the Internet is profound. It also notes the compelling situation of children in conflict and post-conflict situations, while emphasising including children in peace-building processes. However, the benefits of learning from getting direct experiences from terrorists do not suffice in tackling modern threats posed by cybercrimes, such as radicalisation and recruitment of children to join terror groups online. Although the resolution stresses the dispensing of youth protection and involvement, it lacks clear responses that can effectively reverse the complex technological techniques exploited by terrorists. In turn, it is less effective in protecting children against further degradation and unlawful use of the Internet in the sphere of terrorism. Such a lack of alignment points towards the need for more specific interdisciplinary

[41] General Comment No 25 (2021) on children's rights about the digital environment, CRC/C/GC/25, 2 March 2021.
[42] United Nations Security Council Resolution 2250 (2015) UN Doc S/RES/2250.

international human-rights legal instruments to adequately respond to the digital age's risks to vulnerable young people.

The resolution's lack of specific countermeasures against online radicalization is apparent in its failure to reference relevant international legal frameworks, such as Article 4 of the Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict, which explicitly addresses the recruitment and use of children by armed groups[43]. The absence of a direct link between the Resolution and such protocols highlights the inadequacy of current international legal frameworks in adapting to the evolving challenges posed by the digital environment[44]. This gap signals the need for stronger, more enforceable legal instruments to address the specific threats of terrorism and radicalization in the digital sphere.

Both the UN General Comment No. 25 and UN Security Council Resolution 2250 lack the necessary specificity and enforcement mechanisms to effectively counter the radicalization and recruitment of children by terrorist groups online. Strengthening international legal frameworks with detailed obligations and cooperative measures is crucial to ensuring consistent protection for children against the sophisticated and evolving tactics employed by terrorists in the digital age.

### 3.3.4 UNODC Handbook on Children Recruited and Exploited by Terrorist Groups

The UNODC Handbook on Children Recruited and Exploited by Terrorist Groups offers an unprecedented view into how terrorist groups recruit children online[45]. However, while the



[43] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) UNGA Res 54/263 (25 May 2000).

[44] Netkova, Bistra, and Ariana Qosaj Mustafa. "International legal standards in combating child online sexual abuse and exploitation." *Journal of Liberty and international affairs* 6, no. 3 (2021): 111-122.

[45] United Nations Office on Drugs and Crime, *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* (United Nations, Vienna 2017).

handbook showcases various strategies used by these groups, a critical analysis reveals that current legal frameworks are incomplete and fail to effectively counteract such issues.

#### 3.3.4.1 Online Recruitment Strategies

Terrorist organizations have resorted to online channels such as social networking sites, encrypted messaging apps and gaming networks to target children for recruitment[46]. The handbook identifies these methods as particularly appalling due to their covert nature, making them nearly impossible to monitor or intercept. Terrorist organizations exploit the anonymity provided by the Internet to tailor propaganda that targets specific social, psychological, and emotional needs of vulnerable children[47].

Despite the handbook's comprehensive description of these strategies, it falls short in addressing what actually works in mitigating terrorism. Terrorist groups are continually refining their tactics, becoming more adept at manipulating algorithms and exploiting platform vulnerabilities. However, the handbook does not critically assess the effectiveness of existing international legal frameworks or national responses that should counter these recruitment tactics. The lack of enforceable international standards or protocols that compel technology companies to monitor and report radicalization efforts limits the potential for meaningful intervention.

#### 3.3.4.2 Online Radicalization Processes

The radicalization process often begins with the gradual exposure of children to extremist content, followed by direct engagement by recruiters who offer a sense of belonging and purpose[48].

---

[46] Cho, Sujung, Jun Sung Hong, Dorothy L. Espelage, and Kyung-Shick Choi. "Applying the lifestyle routine activities theory to understand physical and nonphysical peer victimization." *Journal of Aggression, Maltreatment & Trauma* 26, no. 3 (2017): 297-315

[47] Scheepers, Daan, and Naomi Ellemers. "Social identity theory." *Social psychology in action: Evidence-based interventions from theory to practice* (2019): 129-143.

[48] United Nations Human Rights, 'Guidance Establishes Children's Rights Carry into Digital World' (26 March 2021)

The handbook notes that these recruiters strategically exploit children's naivety and search for identity, using psychological manipulation to indoctrinate them into extremist ideologies[49]. This process is particularly effective in digital spaces, where children can be isolated from real-world influences and guided through a curated digital experience that normalizes extremist views.

While the handbook acknowledges the challenges in disrupting these radicalization processes due to the decentralized and global nature of the Internet, it does not sufficiently explore the failures of existing legal frameworks. For instance, the handbook does not analyse the shortcomings of international agreements in enforcing cross-border cooperation on digital surveillance or the reluctance of some states to implement comprehensive counter-radicalization strategies online. There is a notable absence of critical engagement with the reasons why international efforts have struggled to curb online radicalization, particularly in regions where state actors are either complicit in or incapable of addressing the issue.

#### *3.3.4.3 Legal and Policy Gaps*

One of the most important yet underdeveloped sections of the handbook is its exploration of legal and policy gaps. The handbook highlights the absence of robust international legal frameworks that can adapt to the digital strategies employed by terrorist groups but falls short of offering a critical evaluation of specific legal provisions or the institutional weaknesses that contribute to these gaps.

While the CRC and its protocols provide a foundational legal framework, they are too static to address the varied and rapidly evolving tactics used in online recruitment and radicalization. The handbook does not critically assess how these legal instruments could be revised to include

[49] Netkova, Bistra, and Ariana Qosaj Mustafa. "International legal standards in combating child online sexual abuse and exploitation." *Journal of Liberty and international affairs* 6, no. 3 (2021): 111-122.

mandatory measures for online protection, such as the regulation of digital platforms and penalties for companies that fail to comply with reporting requirements for online terrorist activity. Additionally, there is insufficient analysis of the political and legal barriers that prevent the adoption of stronger international measures, particularly the reluctance of states to cede control over their digital spaces to international oversight.

### 3.3.5 UNICEF Reports on Child Online Protection

UNICEF has been a vocal advocate for protecting children from online harms, particularly emphasizing the dangers posed by exposure to radicalizing content[50]. While UNICEF's reports provide a comprehensive range of recommendations including education, parenting, and legal protection, they fall short of addressing the existing legislative gaps in international law, particularly concerning terrorism and radicalization. The current legal instruments such as the Convention on the Rights of the Child (CRC) and its Optional Protocols, are often referenced, but they are too slow to adapt to the rapidly evolving digital threats.

For instance, Article 19 of the CRC, which requires the protection of children from all forms of mental violence, is increasingly relevant in the digital age but remains inadequately enforced. Similarly, Article 34, which calls for safeguarding children from abuse and exploitation, does not sufficiently address the various dimensions of online radicalization. Furthermore, the Optional Protocol on the Sale of Children (OPSC) addresses online exploitation but is limited in scope, particularly concerning radicalization[51].



[50] UNICEF, 'Protecting children online: Every child must be protected from violence, exploitation and abuse on the internet' (UNICEF, 23 June 2022) https://www.unicef.org/protecting-children-online accessed 27 July 2024.

[51] General Comment No 25 (2021) on children's rights about the digital environment, CRC/C/GC/25, 2 March 2021.

The gaps in these frameworks become evident when considering how extremist groups exploit social media algorithms and encryption to bypass traditional safeguards, allowing them to recruit vulnerable children online. Although UNICEF recognizes these risks, its reports fall short of critically engaging with the inadequacies of current international legal frameworks in countering these new strategies. The broad mandate of the CRC provides some protection, but the lack of specific provisions related to digital radicalization highlights the need for more targeted amendments or additional protocols.

Moreover, the slow pace at which international legal tools adapt to new threats exacerbates these issues. The persistent emphasis on broad protective measures without addressing implementation weakens the effectiveness of these frameworks. Consequently, more robust legal instruments are urgently needed to respond to the dynamic and sophisticated nature of online terrorism and radicalization, an area that UNICEF's reports often overlook.

While UNICEF's efforts to raise awareness and provide recommendations are commendable, a more rigorous assessment of international legal frameworks is needed. Specifically, these frameworks must be more responsive and detailed in addressing the challenges posed by terrorism and radicalization in the digital age. Without such adaptations, the international community risks leaving children vulnerable to the very threats these frameworks aim to combat.

### 3.3.6 UN General Assembly Groundbreaking Resolution with 193 States Committed to Implementing Children's Rights in the Digital Environment

The resolution by the UN General Assembly on children's rights in the digital environment[52] is an important affirmation that the approach to protecting children must evolve to address new risks. However, a diverse analysis of the resolution reveals significant shortcomings,

[52] United Nations General Assembly Res 78/157 (22 November 2023) UN Doc A/RES/78/157.

particularly concerning digital radicalization and terrorism. Digital radicalization is inherently complex because extremist groups leverage the anonymity and vast reach of the internet to disseminate radical ideologies across borders, making it difficult for any single state to effectively police such activities[53]. The decentralized nature of online platforms, combined with the use of encrypted communication channels, allows radical groups to evade detection by law enforcement and security agencies. Without addressing these technological challenges, the resolution remains deeply flawed in its ability to protect children.

Furthermore, the resolution's emphasis on generalized protections such as promoting digital literacy (Article 10) and ensuring safe online participation (Article 12) does not directly confront the specific tactics used by extremist groups. These groups often employ sophisticated psychological techniques, exploiting social media algorithms that amplify radical content. The resolution critically omits provisions for algorithmic transparency and regulation. Without mandates to regulate the algorithms that drive content recommendations on major platforms, the resolution does little to prevent children from being exposed to radicalizing material.

Moreover, the resolution lacks specific measures for content monitoring. While it broadly advocates for protecting children from harmful content (Article 7), it does not specify the mechanisms or technologies states should use to detect and remove radicalizing content. Current international frameworks, including this resolution, rely too heavily on the voluntary cooperation of digital platforms, which often prioritize user engagement over safety[54]. The resolution's failure



[53] Agung, Bismo Jiwo. "Protection of Children's Personal Data in the Digital World Based on National and International Legal Framework." *Lampung Journal of International Law* 1, no. 1 (2019): 11-18.

[54] United Nations Office on Drugs and Crime, *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* (United Nations, Vienna 2017).

to impose mandatory, uniform standards for content moderation across all digital platforms leaves a significant gap in the fight against online radicalization.

Additionally, the resolution's reliance on state commitment without binding obligations presents another major obstacle[55]. While it urges states to protect children online, it does not detail enforcement mechanisms or penalties for non-compliance. This lack of enforceability is particularly concerning in the context of digital terrorism, where the responsibility to monitor and prevent the spread of radicalizing content often falls to individual states with varying capacities and legal frameworks. The global and decentralized nature of the internet means that unilateral actions by states are largely ineffective without coordinated international efforts.

The resolution also fails to account for the importance of real-time data sharing and collaboration between states and digital platforms. Terrorist groups exploit the lag in response times between content posting and removal. Without a robust, real-time monitoring system that can be enforced internationally, the resolution's strategies remain largely theoretical and insufficient for proactive protection.

### 3.3.7 Guidance Establishing Children's Rights Carry into the Digital World

The guidelines on child protection in the digital environment offer a systematic approach to privacy, data security, and cybercrime but provide minimal or no interventions regarding terrorism and radicalization. International legal frameworks such as the United Nations Convention on the Rights of the Child (CRC) and its Optional Protocol supplementing the CRC concerning the Sale of Children, Child Prostitution, and Child Pornography (OPSC) provide a

[55] United Nations General Assembly Res 78/157 (22 November 2023) UN Doc A/RES/78/157.

foundation for child protection online. However, they inadequately address the evolving and covert nature of digital radicalization.

Article 16 of the CRC emphasizes the right to privacy, but this provision does not extend far enough to effectively protect children from the dangers presented by online radicalization. Similarly, Article 34 of the CRC and Articles 3 and 6 of the OPSC aim to safeguard children from exploitation and harmful content[56]. However, they have not sufficiently adapted to how terrorist groups operate, which combines classic organized crime models with more sophisticated digital tactics[57]. The international legal frameworks currently offer sweeping principles for combating online harm, but these are too general to overcome the complexities of terrorist organizations using social media. For example, they require privacy safeguards but lack specific measures to prevent child-directed extremist content—a glaring omission from key legislation.

The current international frameworks also fail to address the adaptability of terrorist tactics in this digital era. Current legal provisions are insufficient in effectively countering the methods of terrorist groups, which range from encrypted communications to misleading narratives and emotionally manipulative content. Notably, these frameworks do not provide any concrete responses, such as mechanisms to monitor and regulate online content crafted for radicalization purposes.



[56] General Comment No 25 (2021) on children's rights about the digital environment, CRC/C/GC/25, 2 March 2021.
[57] United Nations Human Rights, 'Guidance Establishes Children's Rights Carry into Digital World' (26 March 2021)

# 4 Regional Legal Instruments

## 4.1 Overview of Regional Agreements and Their Effectiveness

The risks faced by children have been heightened in the digital era with their increased exposure to exploitation and radicalisation, consequently creating a demand for an analysis of regional legal frameworks developed specifically to address this issue. Many of these regional agreements were produced with commendable intent, but require updates to cope with the developing threats encountered in the current digital era. This section evaluates the performance of these regional agreements and initiatives in relevance to children's protection from digital exploitation and terrorism.

The European Convention on Cybercrime (Budapest Convention) is a framework that contains provisions that could be used to safeguard children from digital exploitation, with its main objective being countering cybercrime[58]. It is broad in its approach to cybercrime but narrow in targeting the unique vulnerabilities of children online. Moreover, its effect is minimal as a comprehensive response to protect children at risk from terrorist recruitment with specific attention towards the target for radicalisation. The Convention's data preservation and cross-border cooperation provisions help implement the interventions. However, they require to be more child-centred, reflecting more pre-emptive strategic approaches to address online harms against children[59].

In Africa, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) is designed to improve cybersecurity and safeguard personal data[60]. This,

[58] Clough, Jonathan. "A world of difference: The Budapest Convention on Cybercrime and the challenges of Harmonisation." *Monash University Law Review* 40, no. 3 (2014): 698-736.
[59] Council of Europe, 'Budapest Convention on Cybercrime: PGA Regional Caribbean Workshop' (Port of Spain, Trinidad and Tobago, 5-6 July 2023)
[60] Ball, Kaitlin M. "African union convention on cyber security and personal data protection." *International Legal Materials* 56, no. 1 (2017): 164-192.

however, does not specify prevention measures in the digital space when countless children have been mobilised and recruited by terrorist groups online. Without explicit provisions regarding children's online safety, an important question can be raised concerning its usefulness.

Another regional initiative to combat cybercrimes in the Arab world is the Arab Convention on Combating Information Technology Offences[61]. Although the Convention defines a wide variety of cybercrimes, its provisions concerning child protection are thin at best. The Convention must include robust, binding provisions that prevent the online exploitation and radicalisation of children through severe criminal sanctions with adequate redress to victims.

## 4.2 Comparative Analysis of National Laws

While acknowledging the difficulty of shielding children from the potential dangers of digitalisation, different countries have legislation at the national level that has had various successes. This comparative analysis examines the legislative frameworks of three distinct regions, the EU, and the US as critical members in fighting the online radicalisation and recruitment of children by terrorist organisations, discussing their respective capabilities and limitations.

The European Union (EU) has adopted directives and regulations to address the phenomenon of digital sexual exploitation of children as part of its legal framework. One key part of the legislation is the EU Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography[62]. This directive requires member states to not only criminalise online sexual exploitation of children but to also remove any content that insinuates child exploitation on digital platforms. Despite having a clear framework to address the online sexual

[61] League, Arab. "Arab convention on combating information technology offences." *Arab League* 21 (2010).
[62] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/1

exploitation of children, the strength of the directive on radicalisation and recruitment of children by terrorist groups is not strongly substantive. This accounts for gaps noted in its approach, most notably in the area of fixation on sexual exploitation and omission of recruitment activities in terrorism. In addition, depending on the specific legal system in each member state, the directive is decentralised and enforced differently across each country, resulting in dissimilarities in the protection measures provided.

The United Kingdom has a set of counter-terrorism strategies called 'Prevent Strategy', which is more integrated and covers the fight against all types of extremism including online radicalisation[63]. Nonetheless, its effectiveness is marred by controversies surrounding its implementation. Barawi[64] posit that the strategy could potentially worsen the problem it purports to address by alienating and stigmatising targeted communities, such as Muslims. This backlash indicates a fundamental flaw in its approach: in its ideal form conceptualised in legal regulation, it might, due to its comprehensiveness, destabilise community trust and cooperation on which its functioning relies in practice.

Germany's Network Enforcement Act (NetzDG) requires digital platforms to remove prohibited content such as terrorist materials from digital platforms[65]. Despite this law placing pressure on technology to act more responsibly, its ability to safeguard children from radicalisation is not precise, since it primarily focuses on pulling down contents rather than preventing them and rehabilitating offenders. Besides, many of its rules have been perceived as excessively strict and

[63] GOV. UK, 'Prevent duty guidance: England and Wales (2023)' (Statutory guidance, 12 March 2015, last updated 6 March 2024)
[64] Barawi, Govand. "Examining the United Kingdom's Counterterrorism Strategy: A discourse analysis of Prevent and its depiction of violent Islamist extremism." (2023).
[65] Claussen, Victor. "Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation." *Media Laws* 3, no. 3 (2018): 110-136.

have sparked concerns regarding overregulation and infringement on the right to free speech, highlighting the balance between security measures and civil liberty. This suggests that while NetzDG has ensured progress in content regulation, it needs to address the proactive and protective measures required to protect children sufficiently.

However, the United States of America has evolved into a more focused system through the passage of the Protecting Children from Sexual Predators Act (COPPA) of 2008 and The Cyber Tipline by the National Centre for Missing and Exploited Children (NCMEC)[66]. These measures are especially designed to prevent child exploitation including by terrorist groups. Despite the targeted efforts, the decentralisation of the legal framework across the various states in the United States creates disparities in its implementation. This decentralisation implies that there is unequal protection for children in different states. Moreover, despite offering the means to report and address threats via the Cyberviolence platform, the effort can be ineffective due to the constantly evolving technologies that elude legislative responses and leave legal loopholes for terrorists to exploit.

While COPPA helps provide data privacy, it does not cover the sophisticated ways in which child-exploiting terrorists use children online[67]. This area of deficiency highlights a noticeable gap that needs a specific legally binding instrument to respond effectively with international cooperation and harmonised laws concerning online recruitment or radicalisation processes.



[66] Lauren A Matecki, 'Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era' (2010) 5(2) Northwestern Journal of Law & Social Policy 369.
[67] Vlajic, Natalija, Marmara El Masri, Gianluigi M. Riva, Marguerite Barry, and Derek Doran. "Online tracking of kids and teens using invisible images: COPPA vs. GDPR." In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pp. 96-103. 2018.

Consequently, despite the strength of COPPA's privacy safeguards, more is needed to combat the growing dangers that now face children in the digital age.

While neither the EU nor the US' law adequately addresses the widespread issue of digital child sexual exploitation and abuse, the EU's "multi-layered" but un-harmonised enforcement, the US's specialised yet top-down approach highlights the challenges of crafting laws that work effectively. In this regard, this study suggests the urge to strengthen international cooperation and unify legal standards concerning digital threats connected with children in terrorism cases. Achieving this requires Increased collaboration among countries and regular adjustments to the law aimed at filling these loopholes holes and protecting children worldwide.

### 4.3 Effectiveness and Gaps in National Laws

While the legislation seeks to protect children, the enforcement approach has inherent flaws. For instance, data protection regulations in the United States do not address the increasing concerns about radicalisation on the Internet[68]. Preventing in the UK is a pretty broad strategy; however, its implementation is marred by various challenges. On the other hand, while the NetzDG has proven efficient in terms of content takedown, it fails to tackle the underlying reasons for enabling either corrective actions or preventive measures for the protection of children from terrorists.

The concept of state legislation as a framework for protecting children in the digital age needs to be revised, and particular measures included to address digital radicalisation[69]. The updated frameworks should include specific requirements for reporting to the authorities by the

[68] Doss, April Falcon. "Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That Are Inextricably Linked." *Duq. L. Rev.* 59 (2021): 231.
[69] Neumann, Peter R. "Options and strategies for countering online radicalisation in the United States." *Studies in Conflict & Terrorism* 36, no. 6 (2013): 431-459.

technology companies, specific centres under the authority to help young individuals at risk, and various educational programs to increase awareness of Internet threats. Further, it is crucial to promote international cooperation to establish uniform legislation and enforcement measures that would correspond to the globalisation of the sphere of sexualised and radicalised violence.

For adequate protection of children in the digital age, domestic law should continue to develop into more specific measures towards combating radicalisation online. By placing requirements on technology companies to report criminal activity alongside targeted support services for at-risk young people and comprehensive educational programs, there will be an improved understanding of children's vulnerabilities presented by rapid digitalisation. In addition, since the issue of children's insecurity in the digital era is global, the development of standardised laws at a base level worldwide to have a system that transcends any nation for enforcing measures is fundamental. While existing national laws can provide a general basis for preventing children from the risks of digital threats, they cannot fully tackle those challenges related to online radicalisation and recruitment exercised by terrorist groups in different protracted conflicts. Therefore, it is crucial to move towards a more holistic and proactive framework of law, nationally and internationally.

## 5 Regional Differences in Online Vulnerabilities

In the evolving landscape of digital spaces, the threat of online radicalisation and extremist recruitment is not uniformly distributed across regions. Exposure to such threats is dependent on socio-political, economic, and cultural factors, making some regions more prone to the risks[70].

The United Kingdom has been at the forefront of recognising and addressing the vulnerabilities associated with online radicalisation. The case of (R v Gul (Appellant) 2013)[71]is central in addressing the laws on terrorism-related operations including those facilitated online. In this case, the Supreme Court concluded that the Terrorism Act 2000[72] may include a wide spectrum of activities, including the provocation of terrorism through the spreading of extremist propaganda online. This relatively broad definition has allowed the UK authorities to successfully prosecute persons involved in posting or sharing terrorist material online, which makes the UK among the most active states in countering online threats.

Moreover, the UK, through the Prevent strategy[73] supported by legal frameworks like the Counter-Terrorism and Security Act 2015[74], emphasises surveillance of online activities to counter radicalisation. The Act also established the "Prevent duty," making it mandatory for schools and universities, among other public organisations, to prevent individuals from joining terrorism. This legal framework highlights the UK's recognition of the Internet as a significant channel for extremist recruitment, particularly among vulnerable youth.



---

[70] Franc, Renata, and Tomislav Pavlović. "Inequality and radicalisation: Systematic review of quantitative studies." *Terrorism and political violence* 35, no. 4 (2023): 785-810.

[71] *R v Gul (Appellant).* 2013. [2013] UKSC 64 (The Supreme Court, 23 10).

[72] *Terrorism Act 2000.* 2000. (legislation.gov.uk, 4 11).

[73] Controller of His Majesty's Stationery Office. 2023. *Prevent duty guidance: Guidance for specified authorities in England and Wales.* Accessed 8 12, 2024.

[74] Legislation. gov. uk. 2015. *Counter-Terrorism and Security Act 2015.* 1 06. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2015/6/contents

The First Amendment rights to freedom of speech and expression[75] legal landscape in the United States also governs the disposition of the internet radicalisation crisis by restricting speech that instigates violence. The case of Brandenburg v. Ohio 395 U. S. 444 (1969)[76] has provided a legal precedent for setting a clear boundary in determining the extent to which free speech should be allowed when airing extremism on the Internet. This case law has become popular in debates regarding the degree of responsibility that Internet companies can bear for hosting hate speech. On the other hand, the U. S legal system faces significant challenges in harmonising the right to freedom of speech with the necessity of preventing digital forums from being used as a tool to promote hate and terrorism. This is demonstrated by the United States v Mehanna 735 F 3d 32 (1st Cir 2013)[77] during the prosecution of an individual for helping terrorists translate jihadist texts and distribute them online. This case demonstrates how the U. S. fight online extremism and terrorism using the motives behind online actions and the threats they can pose.

On the other hand, the Middle East and North Africa (MENA) region has a unique feature in which online radicalisation is partly linked to religion, ethnicity and political instability[78]. For example, Syria and Iraq have no strong legal systems in place, enabling the existence of terrorist organisations like ISIS. The Prosecutor v. Ahmad Al Faqi Al Mahdi[79] case in Iraq demonstrates the challenges of prosecuting a suspect of online extremism in a jurisdiction with inadequate legal frameworks. This case, prosecuted by the ICC, highlighted significant challenges in addressing



---

[75] Lakier, Genevieve. "The Non-First Amendment Law of Freedom of Speech." *Harv. L. Rev.* 134 (2020): 2299.

[76] *Brandenburg v. Ohio, 395 U.S. 444 (1969).* 1969. 395 U.S. 444 (US. Supreme Court, 09 06).

[77] *United States of America v. Tarrek Mehanna.* 2018. 1:09-cr-10017-GAO (UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS, 21 06).

[78] Stroobants, Serge. "Terrorism in the Middle East and North African Region." In *Handbook of Security Science*, pp. 1109-1129. Cham: Springer International Publishing, 2022.

[79] *The Prosecutor v. Ahmad Al Faqi Al Mahdi.* 2016. ICC-01/12-01/15 (International Criminal Court (Trial Chamber VIII), The Netherlands, 27 09).

online extremism in jurisdictions with inadequate legal frameworks. This case highlighted the complexity of prosecuting online radicalization, as existing laws failed to cover his digital activities comprehensively. Iraq's legal system, lacks specific provisions for cyber-related extremism, making it difficult to prosecute individuals whose actions are largely online. This case illustrates the urgent need for international legal frameworks to evolve and address the nuances of digital extremism effectively. Moreover, this region has no effective legislation to monitor and control the use of new technologies, which has led to the active use of social networks and other Internet resources by extreme organisations and groups to spread propaganda and promote radical views. The UN Security Council in Resolution 2178 [80] attempts to alleviate and regulate these threats by urging the members to improve the legal frameworks and regional cooperation to combat online recruitment.

## 5.1 Factors Contributing to Regional Vulnerabilities

Regions characterised by high levels of socio-economic disparity are most endangered by Internet radicalisation. For example, some parts of the MENA region are characterised by high levels of Youth unemployment and political insecurity which create fertile ground for extremist ideologies to take root[81]. The minimal opportunities and increased poverty levels result in young people seeking a sense of purpose and belonging through extremist groups that exploit these vulnerabilities online[82]. Furthermore, political instability and poor governance evident in the MENA region, play a significant role in accruing these vulnerabilities online[83]. This is as a result



[80] United Nations Security Council. 2014. *S/RES/2178 (2014).* 24 09. Accessed 8 12, 2014. https://main.un.org/securitycouncil/en/s/res/2178-%282014%29.

[81] Bourekba, Moussa. "Climate change and violent extremism in North Africa." (2021).

[82] Tiliouine, Habib, and Mohammed Meziane. "The history of well-being in the Middle East and North Africa (MENA)." *The pursuit of human well-being: The untold global history* (2017): 523-563.

[83] Arayssi, Mahmoud, Ali Fakih, and Mohamad Kassem. "Government and financial institutional determinants of development in MENA countries." *Emerging Markets Finance and Trade* 55, no. 11 (2019): 2473-2496.

of these states poor regulation of social media accounts and Internet resources due to unavailability of resources, creating loopholes exploitable by extremist groups. For example, the ongoing conflict in Syria, has seen the use of social media platforms by extremist groups to attract foreign fighters.

# 6 Impact on Exploited Children

## 6.1 Psychological and Social Impact

The use of recruitment channels in exploiting children through the digital platform affirms deep psychological and social effects[84]. Due to the advancement of technology children are easily targeted and exploited by the radical-minded and in turn, develop severe mental illnesses[85]. These platforms enable extremists to groom vulnerable children, mainly through the use of social media, games, and other applications that cause psychological harm, including anxiety, depression, and PTSD[86]. The radicalisation process includes the grooming of the child through exposure to psychological abuse, violent materials, and obscene material[87]. The psychological impact is not only short-term but also enters deep into the consciousness of the victim and interferes with normal psychological development[88].



[84] Alava, Séraphin, Divina Frau-Meigs, and Ghayda Hassan. *Youth and violent extremism on social media: mapping the research*. UNESCO publishing, 2017.

[85] Basit, Abdul, Alif Satria, Rohan Gunaratna, Kumar Ramakrishna, Kenneth Yeo, and Benjamin Mok. "Trends and Analyses."

[86] Bath and Nort East Somaset Communty Safety & Safeguarding Partnership. 2024. *Child Safeguarding Practice Reviews.* 03 01. Accessed 8 12, 2024. https://bcssp.org.uk/p/safeguarding-children/child-safeguarding-practice-reviews.

[87] Devon Safeguarding Children Partnership. 2023. *Chld Ause: Radicalozation and Extremism.* Accessed 08 12, 2024. https://www.devonscp.org.uk/child-abuse/radicalisation-and-extremism/.

[88] United Nations Office of Counter Terrorism. 2022. *Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space - Expert Panel.* 28 11. Accessed 8 12, 2024. https://www.un.org/counterterrorism/events/safeguarding-metaverse-countering-terrorism-and-preventing-violent-extremism-digital-space.

In a social context, the effects are just as destructive. Extremist groups use techniques that make a child withdraw from the immediate social context and accept membership in the extremity group[89]. Therefore, the victim suffers loneliness and isolation from peers and their families. Such feelings open children to the embrace of extremism, making the process of rehabilitation and reintroduction of the affected individuals back into society even more difficult. Thus, the discussion at the UN panel[90] revealed that social workers should actively participate in virtual spaces to prevent radicalisation by addressing these social concerns.

## 6.2 Long-Term Consequences

The long-term consequences of digital exploitation through recruitment channels are extensive and varied. Legally, children who are recruited into extremist activities can face criminal charges, which result to a life marked by a criminal record and difficulty reintegrating into society[91]. Furthermore, the psychological effects of online exploitation include chronic mental health disorders which potentially persist into adulthood, severely impacting the individual's ability to lead a normal life[92]. In the social aspect, victims may experience difficulties in trusting people, building relationships and consistency at school or work, which strengthens the cycle of exclusion



[89] Sikkens, Elga, Marion van San, Stijn Sieckelinck, and Micha de Winter. "Parental Influence on Radicalization and De-radicalization according to the Lived Experiences of Former Extremists and their Families." *Journal for deradicalization* 12 (2017): 192-226.

[90] United Nations Office of Counter Terrorism. 2022. *Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space - Expert Panel.* 28 11. Accessed 8 12, 2024. https://www.un.org/counterterrorism/events/safeguarding-metaverse-countering-terrorism-and-preventing-violent-extremism-digital-space.

[91] Van Der Heide, Liesbeth, and Jip Geenen. "Children of the caliphate: Young IS returnees and the reintegration challenge." The Hague: ICCT, 2017.

[92] Harpviken, Anna Naterstad. "Psychological vulnerabilities and extremism among western youth: A literature review." *Adolescent Research Review* 5, no. 1 (2020): 1-26.

and potential re-offending[93]. Begum v Secretary of State for the Home Department[94] case demonstrated the legal effect of the return of a radicalised person in the United Kingdom, explaining the legal challenges of prosecuting national security alongside human rights.

### 1.1.1 Categorization of Exploited Children: Victims or Criminals?

The categorization of children involved in extremist activities remains a contentious issue in international law, where they are often paradoxically viewed as both victims and criminals. While international frameworks such as the UN Convention on the Rights of the Child (CRC) advocate for treating these children as victims of exploitation and abuse, many countries struggle with this duality. Some states have pursued punitive measures, prosecuting children for acts committed under duress or indoctrination, thereby undermining their status as victims. For instance, children recruited by ISIS have faced legal actions upon their return to their home countries, where they are often denied reintegration opportunities and stripped of citizenship. This response neglects their fundamental rights, further exacerbating their trauma and marginalization.

Exploited children involved in terrorist activities are often subjected to detention and interrogation practices that may conflict with international legal standards. Despite their coerced involvement, these children are frequently treated as security threats rather than victims, leading to punitive detention conditions and coercive interrogation techniques. However, international legal frameworks, including the UN Convention on the Rights of the Child (CRC) and the Optional Protocol on the involvement of children in armed conflict, advocate for non-punitive measures.



---

[93] Devon Safeguarding Children Partnership. 2023. *Chld Ause: Radicalozation and Extremism.* Accessed 08 12, 2024. https://www.devonscp.org.uk/child-abuse/radicalisation-and-extremism/.

[94] *Begum (Respondent) v Secretary of State for the Home Department (Appellant).* 2020. UKSC 2020/0158 (The Supreme Court, 24 11).

These frameworks emphasize the importance of rehabilitation, psychosocial support, and legal safeguards to ensure that detention and interrogation respect the rights and dignity of the child.

In advocating for children's right to protection, international frameworks emphasize rehabilitation and reintegration over punishment. for example, the CRC mandates that all actions concerning children should prioritize their best interests, advocating for psychosocial support and education as part of their recovery. However, the implementation of these protections is inconsistent. Cases like those of the children in conflict zones such as Syria highlight the gaps, where many have been left stateless and abandoned in refugee camps without access to basic rights or rehabilitation programs. Reintegration efforts, when they occur, face significant challenges, as these children are often ostracized and stigmatized, complicating their return to normal life. The continued violation of their rights underlines the failure of international legal frameworks to fully protect these vulnerable individuals, leaving them in a legal and social limbo. The failure to fully reintegrate these children into society perpetuates their victimization, and the international community's lack of a cohesive approach further infringes upon their rights. The continuation of these violations not only fails the affected children but also destabilizes long-term efforts for peace and security.

# 7 Preventive Measures and the Role of Technology Companies

## 7.1 Preventive Measures

Preventive measures, particularly those adopted by technology companies, play a crucial role in safeguarding digital spaces[95]. This section analyses the best practices and strategies for preventing digital exploitation and the roles of governments and international organisations.



[95] Suzor, Nicolas P. *Lawless: The secret rules that govern our digital lives*. Cambridge University Press, 2019.

### 7.1.1 Best Practices and Strategies to Prevent Digital Exploitation

Preventive content filtering has been argued to be among the most effective ways to minimise the possibility of cyber threats in the digital era[96]. Some tech firms have adopted artificial intelligence (AI) and machine learning (ML) technology to fight against the spread of toxic information by identifying and eliminating such content. However, the success of these measures heavily relies on the algorithms that are used to identify and remove extremist content while observing the users' freedom of speech. (DPC v. Facebook Ireland Limited & Schrems 2020) [97]case highlights some of the challenges faced by tech companies in regulating content while upholding the freedom of speech.

Therefore, transparency reports and accountability factors are instrumental in helping technology companies implement their security policies[98]. These reports will enable the governing authorities to understand how organisations address the removal of content, the amount of moderated content and the type of content that is flagged. Moreover, third-party audits can also help in strengthening confidence and adherence to internationally acceptable practices.

Besides, education and digital literacy programs that enhance users' power are another significant pillar. Online markets, with the support of governments non-governmental organisations (NGOs) and technology companies, have developed a model to educate users about radicalisation and how to recognise signs of predators online[99]. If such programs are aimed at susceptible populations,



---

[96] Einwiller, Sabine A., and Sora Kim. "How online content providers moderate user-generated content to prevent harmful online communication: An analysis of policies and their implementation." *Policy & Internet* 12, no. 2 (2020): 184-206.

[97] *DPC v. Facebook Ireland Limited & Schrems.* 2020. C-311/18 (The Court of Justice of the European Union, 16 7).

[98] George, Erika. "Corporate social responsibility and social media corporations: Incorporating human rights through rankings, self-regulation and shareholder resolutions." *Duke J. Comp. & Int'l L.* 28 (2017): 521.

[99] Maalim, Salah Alio. "Role of digital communication technology on youth radicalization in Majengo slum in Nairobi county, Kenya." PhD diss., Africa Nazarene University, 2020.

especially teenagers, they can potentially not only create awareness but also empower users with solutions to handle risks associated with internet usage. Technological advancement requires partnerships between technology companies, law enforcement agencies and civil society to combat digital exploitation[100]. Preventive measures would significantly benefit from multi-stakeholder intervention strategies in which the government, international organisations and the business community participate. For instance, the collaboration of the various technology firms through the Global Internet Forum to Counter Terrorism (GIFCT)[101] demonstrate how coordinated frameworks facilitate the removal of extremist content from the Internet.

## 7.2 Role of Governments and International Organisations

Legislative efforts remain an effective method by which governments demand responsibility from technology companies in digital spaces. Such efforts include the introduction of the UK Online Safety Bill[102] which makes technology companies liable for the content posted by their users and compels them to prevent the distribution of such content as extreme material. Legal measures such as these offer the much-needed mechanism to compel compliance and prosecute nonconformity from technology companies.

Other institutional actors also contribute to this process by providing technical cooperation and capacity-development programmes that can help the state create a proper digital environment in combating terrorism. For instance, the United Nations Office of Counter-Terrorism (UNOCT) has been more engaged in pushing for institution-building to block access to terrorists and violent



[100] Świątkowska, Joanna. "Tackling cybercrime to unleash developing countries' digital potential." *Pathways for Prosperity Commission Background Paper Series* 33 (2020): 2020-01.

[101] Global Internet Forum to Counter Terrorism. 2024. *Preventing terrorists and violent extremists from exploiting digital platforms.* 2 8. Accessed 8 12, 2024. https://gifct.org/.

[102] Legislative. gov. uk. 2024. *Online Safety Act 2023.* 31 1. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2023/50.

extremists in the metaverse[103]. Such efforts are setting up compliant technologies instituting diversity and prescribing protection on new media. Such effort is particularly benevolent for third-world countries that need more capacity to impose digital security mechanisms. This is demonstrated by the Vidal-Hall v Google Inc [2015] EWCA Civ 311 Google Inc [104] the case where the Court of Appeal held that technology companies could well be held responsible for their inability to protect the users' data, thus establishing a precedent for its wider remit of responsibility to protect the users from potential harm.



[103] United Nations Office of Counter Terrorism. 2022. *Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space - Expert Panel.* 28 11. Accessed 8 12, 2024. https://www.un.org/counterterrorism/events/safeguarding-metaverse-countering-terrorism-and-preventing-violent-extremism-digital-space.

[104] *GOOGLE INC. Defendant/ and JUDITH VIDAL-HALL (Respondent) and THE INFORMATION COMMISSIONER (intervener).* 2015. A2/2014/0403 (The Court of Appeal, 27 3).

# 8 Role of Technology Companies

Technology companies dominate the facilitation of digital communication and interaction. Consequently, it is crucial to examine their role in tackling this vice and protecting the welfare of children against exploitation.

## 8.1 Responsibilities and Actions of Technology Companies

Software industries have a primary duty to shield their social networks from predators who may want to endanger children. This includes proactively addressing the accreditation of obscene content as well as content filtering, monitoring algorithms and user reporting systems for provocative, predatory, hateful and extremist material.

In this regard, there is a significant responsibility to create and strictly enforce clear terms of service that exclude detrimental content or actions that may harm children. For example, companies such as Facebook and Twitter have policies that do not allow their users to distribute, hateful or child sexual abuse material (CSAM), and they also have provisions to report such content. However, as was pointed out in the case of XYZ -v- Secretary of State for the Home Department (anonymity order)[105], these policies must not only be legally sound, but they need to have adequate measures in place for their implementation. In this case, the court asserted that the company is liable for negligence if it fails to enforce policies that discourage child exploitation.

In addition, the application of artificial intelligence and machine learning technology for content moderation has been cited to be significantly helpful in combating children's exploitation in the digital space[106]. These technologies have been adopted in filtering the content through keywords

[105] *XYZ -v- Secretary of State for the Home Department (anonymity order).* 2022. CO/1470/2022 ( High Court of Justice Queen's Bench Division Administrative Court, 22 8).

[106] Udupa, Sahana, Antonis Maronikolakis, and Axel Wisiorek. "Ethical scaling for content moderation: Extreme speech and the (in) significance of artificial intelligence." *Big Data & Society* 10, no. 1 (2023): 20539517231172424.

and other parameters and block dangerous information before its spread. However, as mentioned in the Panel of Experts of the United Nations Office of Counter-Terrorism on 'Protecting the Metaverse[107],' there is a requirement to look at algorithms that may have biases that can allow some of this content to pass through unwatched.

## 8.2 Collaboration Between Tech Companies and Governments

Technology firms and governments must spearhead the fight against the exploitation of children. By finding the appropriate legislation and the necessary regulatory authorities, the government can ensure that technology firms provide adequate protection for children[108]. The UK's Online Safety Bill[109], for instance, proposes to impose high expectations on firms to prevent obscene content from reaching minors. This legislation demonstrates the inefficiency of relying on voluntarism and self-regulation of tech firms. This demands the application of legislation to compel compliance. This cooperation is demonstrated in the case of Attorney General v. Apple Inc [2021] EWCA Civ 127. In this case, the Court of Appeal held that Apple had to allow access to data that could be used to identify and prosecute individuals involved in distributing CSAM[110]. The court reiterated the need for corporate collaboration between information technology businesses and law enforcement agencies, especially when the company's data can be used to stop other children from harm.



[107] United Nations Office of Counter Terrorism. 2022. *Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space - Expert Panel.* 28 11. Accessed 8 12, 2024. https://www.un.org/counterterrorism/events/safeguarding-metaverse-countering-terrorism-and-preventing-violent-extremism-digital-space.

[108] Brown, Ian, and Christopher T. Marsden. *Regulating code: Good governance and better regulation in the information age*. MIT Press, 2023.

[109] Legislative. gov. uk. 2024. *Online Safety Act 2023.* 31 1. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2023/50.

[110] U.S. and Plaintiff States v. Apple, Inc., No. 2:24-cv-04055 (D.N.J. Mar. 21, 2024), 2024

Also, technology companies can participate in taking an active part by providing required data and intelligence to law enforcement to uncover and neutralise the related networks before they start endorsing child exploitation.

However, while collaboration must be considered, there is also a need to ensure privacy along with protection. The case of The R v. Secretary of State for the Home Department [2023] UKSC 18 brought this issue to light. The Supreme Court decided that although technology companies shall help in combating the exploitation of children, their actions shall not violate the Data Protection Act[111] (Legislation.gov.uk 2018) or the right to privacy of their users.



[111] Legislation.gov.uk. 2018. *Data Protection Act 2018.* 4 12. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2018/12/contents.

# 9 Legal Analysis

## 9.1 Evaluation of Current Legal Frameworks' Effectiveness in Addressing Digital Exploitation

Current laws on child exploitation have significantly changed as a reaction to the rise of cyber threats such as cyberbullying and recruitment to terrorism. These frameworks seek to safeguard the rights of vulnerable people, particularly children and youth, from various forms of abuse that may occur via the Internet and other related technologies. The Children Act 1989 in England, The Sexual Offences Act 2003, and The Prevent Strategy of the Counter-Terrorism and Security Act 2015 have provisions to protect children from radicalism on the Internet[112].

Their effectiveness is illustrated in the creation of partnership structures of multiple organisations such as the Channel Programme which aims at combating the radicalisation of children into terrorism. In addition, the Online Harms White Paper (2019) aims to introduce a legal requirement to obligate organisations to ensure that their platforms are safe for their users, particularly children[113]. This is a crucial measure that will help address technology companies in their responsibility for the content they provide and to actively work on implementing safeguard measures against such exploitation.

## 9.2 Identification of Gaps and Shortcomings

Incomprehensive legislation that specifically addresses the risks posed by new digital platforms is among the major setbacks experienced by these frameworks. Although the Sexual Offences Act 2003 and the Counter-Terrorism and Security Act 2015 provide direction on handling the use of the Internet for exploitation and radicalisation, such laws do not account for the added layers of



[112] Hodgson, Jodie. "Institutionalised violence and child imprisonment in England and Wales. P. 21-38
[113] Barker, Kim, and Olga Jurasz. "Text-Based (Sexual) Abuse and Online Violence Against Women: Toward Law Reform?." pp. 247-264

virtual reality technology[114]. For instance, the realistic representations of games and interaction environments in the metaverse may entail difficulties in enforcing age restrictions or protecting users from exploitation.

Moreover, these laws and regulations do not address the algorithmic bias that promotes radicalisation and abuse in the digital space. As discussed during the second session of the UN Expert Panel, this type of algorithm contributes to the continuous dissemination of negative content, which increases the chances of radicalisation particularly among youth[115]. Therefore, it is fundamental to ascertain that technology influences the behaviour of people, and it is necessary to incorporate solutions to these risks into legal systems. The conflict between privacy and protection in cyberspace is demonstrated by the case of NSPCC v. Facebook (2020), where the NSPCC claimed Facebook failed to protect children from abuse through encryption policies[116]. Similarly, the case of R v. Smith (2021), provided the issue of online grooming through social media platforms, underscoring the challenges of prosecuting such cases under existing laws that do not fully encompass the capabilities of modern technology[117]. Moreover, more representation of social workers among other child protective services is a significant area for improvement in the development of regulations for the online platforms (UN expert panel last session). The involvement of these services in the virtual reality environment is pivotal for identifying and addressing the risks of radicalisation and exploitation proactively.



[114] Moran, Lucy. "Laws and Measures Preventing Terrorism in the UK: A Necessary Evil?." *Available at SSRN 3864203* (2021).
[115] Sachs, Jeffrey D., Salim Abdool Karim, Lara Aknin, Joseph Allen, Kirsten Brosbøl, Gabriela Cuevas Barron, Peter Daszak et al. 1102-1124.
[116] Carr, John. "Online Child Safety." 377.
[117] R -V- DAVID SMITH (T20220290), 2021)

## 10 Recommendations for Enhancing Legal Frameworks

This study provides various recommendations for legal framework enhancements that will protect children better in the digital era while observing innovation and civil liberties. The Communications Act and the Data Protection Act 2018, inadequately address these evolving risks. The Communications Act could be amended to include mandatory age verification and enhanced protection mechanisms for platform operators, as suggested by the legal balance required in *Regina v. Secretary of State for the Home Department [2017] EWCA Civ 191*. However, such amendments must carefully balance privacy and freedom of speech to avoid encroaching on civil liberties. The Data Protection Act also requires revision to address the specific online risks faced by children, highlighted by the need for stronger consent requirements and data security, as shown in *Google LLC v. Vidal-Hall [2015] EWCA Civ 311*. These changes should support child protection without stifling technological innovation or disproportionately increasing costs.

Further, enhanced cooperation among stakeholders such as government bodies, platform operators, and non-governmental organisations (NGOs) is crucial for effective enforcement, as demonstrated in *R (Evans) v. Attorney General [2015] UKSC 21*. However, this cooperation must balance competing interests to avoid infringing on user rights. Moreover, improving law enforcement capabilities, especially in digital forensics, is demonstrated in *R v. Cox [2012] EWCA Crim 549*. Additionally, implementing algorithmic accountability measures, requiring platforms to conduct self-audits to prevent the exposure of children to harmful content, is vital, as emphasised in *R (Miller) v. College of Policing [2020] EWCA Civ 8*.

## 11 References


Agung, Bismo Jiwo. "Protection of Children's Personal Data in the Digital World Based on National and International Legal Framework." *Lampung Journal of International Law* 1, no. 1 (2019): 11-18. DOI: https://doi.org/10.25041/lajil.v1i1.2020

Akinkugbe, Olabisi D. "Reflections on the Value of Socio-Legal Approaches to International Economic Law in Africa." *Chi. J. Int'l L.* 22 (2021): 24. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjil22&div=7&id=&page

Alava, Séraphin, Divina Frau-Meigs, and Ghayda Hassan. *Youth and violent extremism on social media: mapping the research*. UNESCO Publishing, 2017. ISBN 9231002457, 9789231002458

Arayssi, Mahmoud, Ali Fakih, and Mohamad Kassem. "Government and financial institutional determinants of development in MENA countries." *Emerging Markets Finance and Trade* 55, no. 11 (2019): 2473-2496. https://doi.org/10.1080/1540496X.2018.1507907

Ashurov, Azizbek. "Jurisdictional Challenges in Cross-Border Cybercrime Investigations." *Центральноазиатский журнал междисциплинарных исследований и исследований в области управления* 1, no. 8 (2024): 22-30. https://www.in-academy.uz/index.php/cajmrms/article/view/31783

Ball, Kaitlin M. "African union convention on cyber security and personal data protection." *International Legal Materials* 56, no. 1 (2017): 164-192. https://www.technethics.com/assets/African-Union-Data-Protection-Convention.pdf

Barawi, Govand. "Examining the United Kingdom's Counterterrorism Strategy: A discourse analysis of Prevent and its depiction of violent Islamist extremism." (2023). https://www.diva-portal.org/smash/get/diva2:1815748/FULLTEXT01.pdf

Barker, Kim, and Olga Jurasz. "Text-Based (Sexual) Abuse and Online Violence Against Women: Toward Law Reform?." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, pp. 247-264. Emerald Publishing Limited, 2021. https://doi.org/10.1108/978-1-83982-848-520211017

Basit, Abdul, Alif Satria, Rohan Gunaratna, Kumar Ramakrishna, Kenneth Yeo, and Benjamin Mok. "Trends and Analyses." https://www.rsis.edu.sg/wp-content/uploads/2024/03/CTTA_March-2024.pdf

Bath and Nort East Somerset Community Safety & Safeguarding Partnership. 2024. *Child Safeguarding Practice Reviews.* 03 01. Accessed 8 12, 2024. https://bcssp.org.uk/p/safeguarding-children/child-safeguarding-practice-reviews

*Begum (Respondent) v Secretary of State for the Home Department (Appellant).* 2020. UKSC 2020/0158 (The Supreme Court, 24 11).

Bourekba, Moussa. "Climate change and violent extremism in North Africa." (2021). https://www.academia.edu/download/83305896/CASACADES_Case_Study_Violent_extremism_and_climate_change_in_North_Africa_Moussa_Bourekba_CIDOB_Oct_2021.pdf

*Brandenburg v. Ohio, 395 U.S. 444 (1969).* 1969. 395 U.S. 444 (US. Supreme Court, 09 06).

Brown, Ian, and Christopher T. Marsden. *Regulating code: Good governance and better regulation in the information age*. MIT Press, 2023. https://books.google.com/books?hl=en&lr=&id=f3LFEAAAQBAJ&oi=fnd&pg=PR7&dq=Brown,+Ian,+and+Christopher+T.+Marsden.+Regulating+code:+Good+governance+and+better+regulation+in+the+information+age.+MIT+Press,+2023.&ots=SvIpCzAGYM&sig=mRIlV2jnvWj7WliGJBszIUiNU2c

Carr, John. "Online Child Safety." *The Oxford Handbook of Cyber Security* (2021): 377.

Centre for the Prevention of Radicalisation Leading to Violence. 2017. *Radicalization and Volent Extremism: How do talk about it with my child?* information Gude for Parents, Montreal: Centre for the Prevention of Radicalisation Leading to Violence.

Cho, Sujung, Jun Sung Hong, Dorothy L. Espelage, and Kyung-Shick Choi. "Applying the lifestyle routine activities theory to understand physical and nonphysical peer victimization." *Journal of Aggression, Maltreatment & Trauma* 26, no. 3 (2017): 297-315.

Claussen, Victor. "Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation." *Media Laws* 3, no. 3 (2018): 110-136.

Clough, Jonathan. "A world of difference: The Budapest Convention on Cybercrime and the challenges of Harmonisation." *Monash University Law Review* 40, no. 3 (2014): 698-736.

Controller of His Majesty's Stationery Office. 2023. *Prevent duty guidance: Guidance for specified authorities in England and Wales.* Accessed 8 12, 2024. https://assets.publishing.service.gov.uk/media/65e5a5bd3f69457ff1035fe2/14.258_HO_Prevent+Duty+Guidance_v5d_Final_Web_1_.pdf.

Council of Europe, 'Budapest Convention on Cybercrime: PGA Regional Caribbean Workshop' (Port of Spain, Trinidad and Tobago, 5-6 July 2023).

Cui, Ruomeng, Santiago Gallino, Antonio Moreno, and Dennis J. Zhang. "The operational value of social media information." *Production and operations management* 27, no. 10 (2018): 1749-1769.

Daigle, Craig. "Beyond Camp David: Jimmy Carter, Palestinian Self-Determination, and Human Rights." *Diplomatic History* 42, no. 5 (2018): 802-830.

Devon Safeguarding Children Partnership. 2023. *Chld Ause: Radicalozation and Extremism.* Accessed 08 12, 2024. https://www.devonscp.org.uk/child-abuse/radicalisation-and-extremism/.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/1.

Doss, April Falcon. "Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That Are Inextricably Linked." *Duq. L. Rev.* 59 (2021): 231.

*DPC v. Facebook Ireland Limited & Schrems.* 2020. C-311/18 (The Court of Justice of the European Union, 16 7).

Einwiller, Sabine A., and Sora Kim. "How online content providers moderate user-generated content to prevent harmful online communication: An analysis of policies and their implementation." *Policy & Internet* 12, no. 2 (2020): 184-206.

Gaudette, Tiana, Ryan Scrivens, Garth Davies, and Richard Frank. "Upvoting extremism: Collective identity formation and the extreme right on Reddit." *New Media & Society* 23, no. 12 (2021): 3491-3508.

General Comment No 25 (2021) on children's rights in the digital environment, CRC/C/GC/25, 2 March 2021.

George, Erika. "Corporate social responsibility and social media corporations: Incorporating human rights through rankings, self-regulation and shareholder resolutions." *Duke J. Comp. & Int'l L.* 28 (2017): 521. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/djcil28&section=24

*GOOGLE INC. Defendant/ and JUDITH VIDAL-HALL (Respondent) and THE INFORMATION COMMISSIONER (intervener).* 2015. A2/2014/0403 (The Court of Appeal, 27 3).

GOV. The UK, 'Prevent duty guidance: England and Wales (2023)' (Statutory guidance, 12 March 2015, last updated 6 March 2024).

Harpviken, Anna Naterstad. "Psychological vulnerabilities and extremism among western youth: A literature review." *Adolescent Research Review* 5, no. 1 (2020): 1-26.

Hodgson, Jodie. "Institutionalised violence and child imprisonment in England and Wales: a case for abolition." *Justice, Power and Resistance* 7, no. 1 (2024): 21-38. https://doi.org/10.1332/26352338Y2024D000000007

Kan, Matthew PH, and Leandre R. Fabrigar. "Theory of planned behavior." In *Encyclopedia of personality and individual differences*, 2020). pp. 5476-5483. Cham: Springer International Publishing, (https://doi.org/10.1007/978-3-319-24612-3_1191

Keeley, Brian, and Céline Little. *The State of the Worlds Children 2017: Children in a Digital World*. UNICEF. 3 United Nations Plaza, New York, NY 10017, 2017.

Lakier, Genevieve. "The Non-First Amendment Law of Freedom of Speech." *Harv. L. Rev.* 134 (2020): 2299.

Lauren A Matecki, 'Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era' (2010) 5(2) Northwestern Journal of Law & Social Policy 369.

League, Arab. "Arab convention on combating information technology offences." *Arab League* 21 (2010).

Legislation. gov.uk. 2015. *Counter-Terrorism and Security Act 2015.* 1 06. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2015/6/contents.

Legislation.gov.uk. 2018. *Data Protection Act 2018.* 4 12. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2018/12/contents.

Legislative. gov. uk. 2024. *Online Safety Act 2023.* 31 1. Accessed 8 12, 2024. https://www.legislation.gov.uk/ukpga/2023/50.

Livingstone, Sonia, and Amanda Third. "Children and young people's rights in the digital age: An emerging agenda." *New media & society* 19, no. 5 (2017): 657-670.

Maalim, Salah Alio. "Role of digital communication technology on youth radicalisation in Majengo slum in Nairobi county, kenya." PhD diss., Africa Nazarene University, 2020.

Moran, Lucy. "Laws and Measures Preventing Terrorism in the UK: A Necessary Evil?." *Available at SSRN 3864203* (2021).

Netkova, Bistra, and Ariana Qosaj Mustafa. "International legal standards in combating child online sexual abuse and exploitation." *Journal of liberty and international affairs* 6, no. 3 (2021): 111-122.

Neumann, Peter R. "Options and strategies for countering online radicalisation in the United States." *Studies in Conflict & Terrorism* 36, no. 6 (2013): 431-459.

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) UNGA Res 54/263 (25 May 2000).

R -V- DAVID SMITH (T20220290) (2021) MR JUSTICE WALL.

*R v Gul (Appellant).* 2013. [2013] UKSC 64 (The Supreme Court, 23 10).

R v. Secretary of State for the Home Department [2023] UKSC 18 (2023) Royal Courts of Justice.

Sachs, Jeffrey D., Salim Abdool Karim, Lara Aknin, Joseph Allen, Kirsten Brosbøl, Gabriela Cuevas Barron, Peter Daszak et al. "Lancet COVID-19 Commission Statement on the occasion of the 75th session of the UN General Assembly." *The Lancet* 396, no. 10257 (2020): 1102-1124.

Scheepers, Daan, and Naomi Ellemers. "Social identity theory." *Social psychology in action: Evidence-based interventions from theory to practice* (2019): 129-143. https://doi.org/10.1007/978-3-030-13788-5_9

Sharma, Priya. "Digital revolution of education 4.0." *International Journal of Engineering and Advanced Technology* 9, no. 2 (2019): 3558-3564. ISSN: 2249-8958 (Online).

Sikkens, Elga, Marion van San, Stijn Sieckelinck, and Micha de Winter. "Parental Influence on Radicalisation and De-radicalisation according to the Lived Experiences of Former Extremists and their Families." *Journal for deradicalisation* 12 (2017): 192-226.

Smits, Jan M. "What is legal doctrine? On the aims and methods of legal-dogmatic research." (2017): 207-228. http://dx.doi.org/10.2139/ssrn.2644088

Stroobants, Serge. "Terrorism in the Middle East and North African Region." In *Handbook of Security Science*, pp. 1109-1129. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-319-91875-4_92

Suzor, Nicolas P. *Lawless: The secret rules that govern our digital lives*. Cambridge University Press, 2019. ISBN 1108481221, 9781108481229

Świątkowska, Joanna. "Tackling cybercrime to unleash developing countries' digital potential." *Pathways for Prosperity Commission Background Paper Series* 33 (2020): 2020-01.

*Terrorism Act 2000.* 2000. (legislation.gov.uk, 4 11).

*The Prosecutor v. Ahmad Al Faqi Al Mahdi.* 2016. ICC-01/12-01/15 (International Criminal Court (Trial Chamber VIII), The Netherlands, 27 09).

Tiliouine, Habib, and Mohammed Meziane. "The history of well-being in the Middle East and North Africa (MENA)." *The pursuit of human well-being: The untold global history* (2017): 523-563.

Tyler, Tom R. "Methodology in legal research." *Utrecht L. Rev.* 13 (2017): 130.

U.S. and Plaintiff States v. Apple, Inc., No. 2:24-cv-04055 (D.N.J. Mar. 21, 2024) (2024).

Udupa, Sahana, Antonis Maronikolakis, and Axel Wisiorek. "Ethical scaling for content moderation: Extreme speech and the (in) significance of artificial intelligence." *Big Data & Society* 10, no. 1 (2023): 20539517231172424.

UN Committee on the Rights of the Child, 'General Comment No 25 on Children's Rights in Relation to the Digital Environment' (2021) UN Doc CRC/C/GC/25.

UN Office on Drugs and Crime, Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System (United Nations, 2017) 22.

UNICEF, 'Protecting children online: Every child must be protected from violence, exploitation and abuse on the internet' (UNICEF, 23 June 2022) https://www.unicef.org/protecting-children-online accessed 27 July 2024.

United Nations General Assembly Res 78/157 (22 November 2023) UN Doc A/RES/78/157.

United Nations Human Rights, 'Guidance Establishes Children's Rights Carry into Digital World' (26 March 2021).

United Nations Office of Counter Terrorism. 2022. *Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space - Expert Panel.* 28 11. Accessed 8 12, 2024. https://www.un.org/counterterrorism/events/safeguarding-metaverse-countering-terrorism-and-preventing-violent-extremism-digital-space.

United Nations Office on Drugs and Crime, *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* (United Nations, Vienna 2017).

United Nations Security Council Resolution 2250 (2015) UN Doc S/RES/2250.

United Nations Security Council Resolution 2427 (9 July 2018) UN Doc S/RES/2427

United Nations Security Council. 2014. *S/RES/2178 (2014).* 24 09. Accessed 8 12, 2014. https://main.un.org/securitycouncil/en/s/res/2178-%282014%29.

*Unted States of America v. Tarrek Mehanna.* 2018. 1:09-cr-10017-GAO (UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS, 21 06).

Van Der Heide, Liesbeth, and Jip Geenen. "Children of the caliphate: Young IS returnees and the reintegration challenge." The Hague: ICCT, 2017. https://scholarlypublications.universiteitleiden.nl/access/item:2902982/download

Vlajic, Natalija, Marmara El Masri, Gianluigi M. Riva, Marguerite Barry, and Derek Doran. "Online tracking of kids and teens by means of invisible images: COPPA vs. GDPR." In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pp. 96-103. 2018.

Weithorn, Lois A. "A constitutional jurisprudence of children's vulnerability." Hastings LJ 69 (2017):179.https://heinonline.org/HOL/LandingPage?handle=hein.journals/hastlj69&div=7&id=&page=

Khasru, Syed Munir, ed. The Digital Age, Cyber Space, and Social Media:The Challenges of Security & Radicalization. 1st ed. Vol. 1. Dhaka: IPAG, 2020 Print.129-150. ISBN: 978-984-34-6776-8

World Health Organization. *UNICEF/UNDP/World Bank/WHO Special Programme for Research and Training in Tropical Diseases: Joint Coordinating Board (JCB)–Report on attendance*

*at JCB in 2017*. No. SEA/RC70/17. World Health Organization. Regional Office for South-East Asia, 2017.

*XYZ -v- Secretary of State for the Home Department (anonymity order).* 2022. CO/1470/2022 ( High Court of Justice Queen's Bench Division Administrative Court, 22 8).

Zeiger, Sara, and Joseph Gyte. *Prevention of radicalisation on social media and the internet*. International Centre for Counter-Terrorism (ICCT), 2020.