E-ISSN: 2963-4946
Vol. 3 No. 9 June 2025
ASEAN Journal of Social and Humanities
https://ajosh.org/

BEYOND DIGITAL BORDERS: A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS FOR DIGITAL EVIDENCE IN CHILD-RELATED CRIME INVESTIGATIONS

Siti Chusnul Nurlaela[1], Subianta Mandala[2]
Universitas Borobudur, Indonesia
Email: elasheylla@gmail.com, subianta_mandala@borobudur.ac.id

ARTICLE INFO

Keywords: digital evidence; child protection; comparative law; criminal procedure

ABSTRACT

Digital evidence in child-related crime investigations presents unique challenges for legal systems worldwide, particularly as such crimes increasingly transcend national borders. The intangible, volatile, and jurisdictionally complex nature of digital evidence raises fundamental questions about how different legal frameworks address collection, preservation, and admissibility in these sensitive cases. Objectives. This study aims to identify and analyze key differences in legal frameworks governing digital evidence in child-related crime investigations across the European Union, United States, and United Kingdom, with specific focus on authority requirements, procedural standards, and cross-border evidence exchange mechanisms. Methods. Through comparative legal analysis of primary legal texts, case law, and secondary literature, this research examines the procedural requirements, technical standards, and jurisdictional approaches to digital evidence across the selected jurisdictions. Research Findings. The analysis reveals distinct regulatory models: the EU employs a structured judicial oversight model through instruments like the European Investigation Order and the emerging e-evidence package; the US CLOUD Act facilitates direct public-private cooperation through streamlined court orders and bilateral agreements; and the UK relies on Criminal Procedure Rules and traditional Mutual Legal Assistance Treaty processes with emphasis on maintaining strict chain of custody. Significant variations exist in authority requirements, technical standards for evidence authentication, and mechanisms for cross-jurisdictional cooperation. These jurisdictional differences create practical challenges for cross-border investigations, particularly concerning cloud-stored data and child sexual abuse material. The study proposes a harmonized approach that balances investigative efficiency with privacy protections and addresses the unique vulnerabilities of child victims, while respecting different legal traditions.

Introduction

The digital era has transformed how crimes against children are perpetrated, investigated, and prosecuted. As child exploitation increasingly transcends national borders through digital channels, the legal frameworks governing digital evidence collection and admissibility face unprecedented challenges (Eggestein & Knapp, 2014). These challenges are particularly acute in cases involving children, where the sensitivity of evidence, victim vulnerability, and the rapidly evolving technological landscape demand specialized approaches from law enforcement and judiciary alike.

The intangible, volatile, and jurisdictionally complex nature of digital evidence complicates investigations in ways traditional evidence does not. Digital evidence in child exploitation cases may be stored across multiple jurisdictions, encrypted, or accessible only through private technology companies operating globally (Rappert et al., 2022). This reality has prompted various legal responses from major jurisdictions, with significantly different approaches emerging across the European Union, United States, and United Kingdom.

The inadequacy of traditional investigatory powers in addressing digital evidence challenges has been well-documented (Hörnle, 2021). Traditional legal frameworks built on territorial jurisdiction principles conflict fundamentally with the non-territorial nature of digital data (Busser, 2018). This has led to competing regulatory approaches, with the EU developing comprehensive legal instruments like the European Investigation Order and the e-evidence package, while the US has enacted the CLOUD Act to facilitate direct cooperation between law enforcement and service providers.

This paper examines the key differences in legal frameworks governing the collection, preservation, and admissibility of digital evidence in child-related crime investigations across these major jurisdictions. It specifically addresses three critical questions: (1) How do authority requirements for digital evidence collection differ across jurisdictions? (2) What are the procedural and technical standards for preserving digital evidence integrity? (3) What mechanisms exist for cross-border evidence exchange in child exploitation cases?

By analyzing these differing approaches, this paper aims to identify best practices and potential paths toward greater international harmonization of digital evidence standards in child-related cases. Such harmonization is increasingly vital as digital crimes against children continue to grow in scope and sophistication, requiring coordinated transnational responses.

Several comparative legal studies have begun to explore these issues. For instance, Hörnle (2021) discusses the difficulties of cross-border enforcement in cloud-based investigations, particularly in the absence of uniform standards. Similarly, Stefan and Fuster (2018) examine the evolution of the European Investigation Order and its limitations in the digital context. While these studies provide valuable insights, they often address digital evidence from a general cybercrime perspective without focusing on child-related crimes, which present unique legal and procedural complexities due to victim vulnerability, the urgency of preservation, and heightened ethical sensitivities.

This article fills that gap by offering a targeted comparative analysis of how the European Union, United States, and United Kingdom regulate the collection, preservation, and cross-border transfer of digital evidence specifically in child exploitation investigations. Unlike prior works, this study focuses on the interplay between investigative authority, procedural safeguards, and international cooperation mechanisms in high-sensitivity cases involving children.

The novelty of this research lies in its effort to synthesize child-specific digital evidence protocols across jurisdictions, identify best practices, and propose a harmonized framework that balances investigative efficiency with fundamental rights protection. By doing so, the paper contributes both to comparative criminal procedure scholarship and to ongoing international efforts in strengthening legal responses to online child sexual exploitation.

Research method

This study employs a comparative legal analysis methodology to examine digital evidence frameworks across the EU, US, and UK jurisdictions. The research combines doctrinal analysis of primary legal texts with evaluation of secondary legal literature and case studies to identify key differences in legal approaches.

The analysis focuses on three key dimensions of digital evidence handling:

1. Legal Authority Framework. Analysis of statutes, regulations, and court decisions establishing the legal basis for digital evidence handling in each jurisdiction.
2. Procedural Requirements. Examination of the formal processes required for collection, preservation, and admissibility of digital evidence, with particular focus on child-related cases.
3. Cross-Border Mechanisms. Assessment of the legal instruments facilitating transnational evidence exchange and their effectiveness in child exploitation investigations.

To enhance the comparative depth, legal cases were selected based on relevance to child exploitation investigations and involvement of digital evidence procedures. The time frame of analysis spans from 2015 to 2023, allowing for a focus on contemporary legal challenges and reforms, including the implementation of instruments like the EU e-Evidence Package, US CLOUD Act, and UK post-Brexit regulations.

Data sources include:

1. Primary legal texts (statutes, directives, regulations)
2. Case law from relevant jurisdictions
3. Academic legal literature
4. Policy documents and official guidance from law enforcement agencies
5. Reports from international bodies and non-governmental organizations

The selection of jurisdictions (EU, US, UK) allows for comparison between civil and common law traditions, while representing major approaches to digital evidence regulation. Additionally, these jurisdictions have been particularly active in developing legal frameworks specifically addressing digital evidence in child exploitation cases.

Results and Discussion

European Union Framework

The European Union has developed several key instruments governing digital evidence in criminal investigations, with significant implications for child-related cases. The EU's approach to digital evidence is characterized by structured judicial oversight and procedural standardization across member states. Directive 2014/41/EU established the European Investigation Order (EIO), which provides a comprehensive framework for obtaining evidence across EU borders (Blažič & Klobučar, 2020). This directive standardized the process for requesting and obtaining evidence between member states, including digital evidence relevant to child exploitation cases.

The authority requirements under the EU framework typically require judicial authorization, reflecting the EU's emphasis on judicial oversight as a safeguard against potential overreach. As noted by Stefan and Fuster (2018), this contrasts with the more executive-centered approach seen in some other jurisdictions.

The EU is further developing its legal framework through the proposed e-evidence package, which includes a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. This initiative aims to address specific challenges posed by digital evidence by introducing standardized procedures for obtaining electronic evidence directly from service providers (Chavleski & Galev, 2019).

The EU framework places significant emphasis on both procedural standardization and fundamental rights protection in digital evidence collection. The e-evidence package proposes preservation orders that would require service providers to preserve specific data for up to 60 days, addressing concerns about the volatile nature of digital evidence (Chavleski & Galev, 2019).

Technical standards for evidence collection vary across member states, but the EU has attempted to harmonize approaches through instruments like the European Network of Forensic Science Institutes (ENFSI) guidelines, which provide best practices for digital forensics procedures applicable to child exploitation cases (Casey, 2011).

A notable aspect of the EU approach is the interaction between evidence collection and data protection requirements. The General Data Protection Regulation (GDPR) imposes significant constraints on data processing, with specific provisions for law enforcement activities. This creates a complex balancing act between investigative needs and privacy protections that investigators must navigate when collecting digital evidence in child-related cases (Busser, 2018).

For cross-border evidence exchange, the European Investigation Order has streamlined processes within the EU, establishing clear timelines and procedures. However, exchanges with non-EU countries remain more complex and typically rely on Mutual Legal Assistance Treaties (MLATs).

The proposed e-evidence package aims to further streamline this process by allowing direct requests to service providers across borders, potentially reducing delays in accessing crucial digital evidence in time-sensitive child exploitation cases. This

represents a significant shift from the traditional approach that required formal judicial cooperation (Blažič & Klobučar, 2020).

United States Framework

The United States has developed distinct approaches to digital evidence in criminal investigations, particularly through recent legislative innovations addressing jurisdictional challenges. The US framework for digital evidence in child exploitation cases is primarily governed by federal statutes, including the Electronic Communications Privacy Act, the Stored Communications Act, and more recently, the CLOUD Act of 2018. These frameworks generally require court orders or warrants, though the specific standards vary depending on the type of data sought (Eggestein & Knapp, 2014).

The CLOUD Act represents a significant development in US digital evidence law, explicitly addressing the territorial challenges of cloud-stored data. It clarifies that US service providers must comply with legal orders for data regardless of where that data is stored, effectively extending US jurisdiction overseas (Hörnle, 2021). This approach contrasts with the EU's more sovereignty-conscious framework.

In child exploitation investigations specifically, the US framework provides enhanced authorities through statutes like the PROTECT Act and the Child Protection and Safety Act, which modify procedural requirements and expand investigative powers in cases involving child sexual exploitation (Eggestein & Knapp, 2014).

US courts have established significant precedent regarding digital evidence collection and authentication. The Federal Rules of Evidence, particularly Rules 901 and 902, govern the authentication of digital evidence, requiring sufficient proof that the evidence is what it claims to be (Casey, 2011).

For preservation, US service providers typically have obligations under 18 U.S.C. § 2703(f) to preserve records for up to 90 days (renewable) upon request from authorities, providing investigators with time to obtain formal legal process. This provision is particularly valuable in volatile digital evidence contexts, including child exploitation investigations (Kerr, 2018).

Technical standards for digital evidence handling in the US are largely guided by organizations like the Scientific Working Group on Digital Evidence (SWGDE) and the National Institute of Standards and Technology (NIST). These bodies provide detailed guidance on forensically sound evidence collection and preservation methods applicable to child exploitation investigations (Casey, 2011).

The CLOUD Act fundamentally altered the US approach to cross-border digital evidence by creating a framework for bilateral executive agreements that allow foreign partners to request data directly from US service providers, bypassing the traditionally slow MLAT process (Daskal, 2018). This innovation is particularly significant for time-sensitive child exploitation investigations.

The first such agreement was established between the US and UK in 2019, creating an expedited process for data sharing in serious criminal investigations, including child exploitation cases. Similar agreements are being negotiated with other countries,

potentially creating a network of streamlined evidence-sharing relationships outside the traditional MLAT system (Mulligan, 2018).

However, these bilateral arrangements raise concerns about forum-shopping and potential circumvention of privacy protections, as noted by several legal scholars (Busser, 2018). These concerns are particularly relevant in child exploitation cases, where the urgency of child protection must be balanced against privacy and due process considerations.

United Kingdom Framework

The United Kingdom has developed its own approach to digital evidence, influenced by but distinct from both EU and US frameworks, especially following Brexit.

Legal Basis and Authority Requirements

The UK's approach to digital evidence in child-related investigations is governed primarily by the Police and Criminal Evidence Act 1984 (PACE), the Criminal Procedure and Investigations Act 1996, and the Regulation of Investigatory Powers Act 2000. These frameworks establish the legal basis for seizure, search, and examination of digital devices (Walden, 2007).

Authority requirements in the UK typically involve warrants for search and seizure, though exceptions exist for urgent circumstances. The UK has also developed specialized procedural guidelines for child exploitation cases, reflecting the sensitive nature of such investigations (Crown Prosecution Service, 2018).

Post-Brexit, the UK is no longer bound by EU instruments like the European Investigation Order, though cooperation mechanisms continue to evolve. The UK's departure from the EU legal framework creates new challenges and opportunities for its digital evidence regime in cross-border cases (Mitsilegas, 2021).

The UK's Criminal Procedure Rules provide detailed guidelines for the handling of digital evidence, emphasizing documentation of the chain of custody and the maintenance of evidence integrity. These requirements are particularly stringent in child exploitation cases, where the integrity of digital evidence is often central to prosecution (Rappert et al., 2022).

Digital forensics practices in UK child exploitation investigations emphasize the importance of human validation in evidence processing, particularly when identifying child sexual abuse imagery. Rappert et al. (2022) highlight the UK approach of combining automated processing with human verification to ensure both efficiency and accuracy in sensitive cases.

The UK has also developed specialized technical guidance through organizations like the Association of Chief Police Officers (ACPO) and the National Crime Agency (NCA), providing standardized approaches to digital evidence collection particularly relevant to child exploitation cases (Casey, 2011).

The UK traditionally relied on MLATs for cross-border evidence exchange but has been developing more efficient alternatives. Most notably, the UK-US CLOUD Act Agreement allows UK authorities to request data directly from US service providers in serious criminal investigations, including child exploitation cases (Mulligan, 2018).

Post-Brexit, the UK is developing new bilateral arrangements to replace EU cooperation mechanisms. These include the UK-EU Trade and Cooperation Agreement, which contains provisions for law enforcement cooperation, though with less depth than previous EU membership provided (Mitsilegas, 2021).

The UK also participates in international initiatives like the WePROTECT Global Alliance, which facilitates cross-border cooperation specifically for combating online child sexual exploitation (WeProtect Global Alliance, 2021).

International Standards and Harmonization Efforts

Beyond the specific jurisdictional approaches, several international initiatives aim to harmonize approaches to digital evidence in child exploitation cases. The Budapest Convention on Cybercrime provides a framework for international cooperation on cybercrime investigations, including provisions specifically addressing child pornography offenses. The Convention establishes minimum standards for criminalization, procedural powers, and international cooperation (Council of Europe, 2001).

The Virtual Global Taskforce and INTERPOL's International Child Sexual Exploitation (ICSE) database represent operational cooperation mechanisms specifically focused on child exploitation investigations. These initiatives facilitate information sharing and coordinate investigations across jurisdictions (INTERPOL, 2022).

However, significant challenges to harmonization persist. These include differing legal traditions, varying constitutional protections for privacy, and divergent approaches to issues like data retention and encryption. These differences are particularly acute in child exploitation cases, where investigative urgency must be balanced against fundamental rights considerations (Svantesson, 2018).

Challenges and Gaps in Current Frameworks

The comparison of EU, US, and UK frameworks reveals fundamental tensions between territorial jurisdiction and the non-territorial nature of digital data. These tensions are particularly evident in:

1. Conflicting Legal Obligations. Service providers may face contradictory legal requirements when operating across jurisdictions, especially regarding data disclosure in child exploitation investigations (Busser, 2018).
2. Extraterritorial Claims. The US CLOUD Act's assertion of authority over data stored abroad contrasts with the EU's emphasis on data sovereignty, creating potential conflicts in cross-border child exploitation investigations (Hörnle, 2021).
3. Jurisdictional Determination. When digital evidence exists in cloud environments with data stored across multiple jurisdictions, determining which legal framework applies becomes increasingly complex (Svantesson, 2018).

These conflicts can significantly impede investigations of child exploitation, where delays caused by jurisdictional disputes may directly impact child safety.

Across all jurisdictions, several technical challenges complicate digital evidence handling in child-related cases:

1. Encryption. End-to-end encryption increasingly limits investigative access to digital communications, creating tensions between security, privacy, and investigative needs in child exploitation cases (Eggestein & Knapp, 2014).
2. Volume and Filtering. The enormous volume of potential digital evidence requires sophisticated filtering techniques, especially in child exploitation cases involving large collections of images or videos (Rappert et al., 2022).
3. Volatile Data. The ephemeral nature of certain digital evidence (like messaging app content with automatic deletion) creates preservation challenges requiring rapid response across jurisdictions (Casey, 2011).
4. Authentication. Proving the authenticity and integrity of digital evidence becomes increasingly complex in cross-platform, cross-border contexts (Casey, 2011).

These technical challenges intersect with legal frameworks in ways that can either facilitate or hinder effective investigation, highlighting the need for legal regimes that accommodate technological realities. Each jurisdiction takes a distinct approach to balancing investigative imperatives with privacy and rights protection:

1. EU Approach: The EU framework emphasizes judicial oversight and data protection principles, potentially increasing procedural protections but sometimes at the cost of investigative efficiency (Blažič & Klobučar, 2020).
2. US Approach: The US CLOUD Act model prioritizes investigative access, raising concerns about potential privacy infringements when applied across jurisdictions with different protection standards (Daskal, 2018).
3. UK Approach: The UK system attempts to balance these concerns through procedural safeguards while maintaining investigative flexibility, particularly in urgent child protection scenarios (Rappert et al., 2022).

These different balancing approaches reflect broader societal and constitutional values in each jurisdiction, making full harmonization particularly challenging.

Future Directions And Recommendations

Based on comparative analysis, several approaches could enhance harmonization while respecting jurisdictional differences:

1. Tiered Consent Model. Developing an international framework where certain categories of particularly serious offenses (including child exploitation) receive expedited processing across jurisdictions (Svantesson, 2018).
2. Standardized Technical Protocols. Establishing internationally recognized technical standards for digital evidence collection and preservation that courts across jurisdictions would recognize as meeting admissibility requirements (Casey, 2011).
3. Protected Categories Framework. Creating special procedural rules for digital evidence in cases involving children that balance investigative urgency with appropriate safeguards (Demarco et al., 2016).

4. Multilateral Agreements. Expanding beyond bilateral arrangements like those under the CLOUD Act to create multilateral frameworks that reduce the complexity of cross-jurisdictional cases (Mulligan, 2018).

These approaches could help bridge the gaps between different jurisdictional frameworks while maintaining necessary protection.

The unique vulnerability of children in digital exploitation cases suggests the need for specialized procedural safeguards:

1. Accelerated Processing. Implementing fast-track procedures for digital evidence requests in cases involving imminent harm to children (WeProtect Global Alliance, 2021).
2. Specialization Requirements. Ensuring that digital evidence in child exploitation cases is handled by specially trained personnel familiar with both technical and child protection considerations (Rappert et al., 2022).
3. Victim-Centered Approaches. Developing evidence collection and preservation methods that minimize additional trauma to child victims while maintaining evidential integrity (Crown Prosecution Service, 2018).
4. Age-Appropriate Privacy Balancing. Creating frameworks that consider the age of victims when determining appropriate privacy protections and investigative authorities (Demarco et al., 2016).

These safeguards could be incorporated into existing frameworks to better address the specific needs of child-related investigations.

The central role of private companies in storing and controlling digital evidence suggests the need for enhanced cooperation models:

1. Standardized Preservation Requests. Developing internationally recognized formats for evidence preservation requests that companies can process efficiently across jurisdictions (Kent, 2014).
2. Proactive Detection Obligations. Clarifying legal obligations for service providers to proactively detect and preserve evidence of child exploitation, harmonized across jurisdictions (Eggestein & Knapp, 2014).
3. Trusted Channel Programs. Establishing verified communication channels between law enforcement and major service providers to expedite requests in child exploitation cases (INTERPOL, 2022).
4. Joint Training Initiatives. Implementing cross-training programs between law enforcement and technology companies to enhance mutual understanding of technical and legal requirements (WeProtect Global Alliance, 2021).

These cooperation models could significantly enhance the efficiency of digital evidence collection while maintaining appropriate oversight.

Conclusion

This comparative analysis reveals significant divergences in how the EU, US, and UK approach digital evidence in child-related crime investigations. The EU's structured judicial oversight model emphasizes procedural safeguards and data sovereignty. The US

CLOUD Act framework prioritizes investigative efficiency through direct public-private cooperation. The UK system attempts to balance these approaches while maintaining a strong chain of custody requirements and emphasizing human validation in child exploitation cases. These differences reflect broader legal traditions and societal values but also create practical challenges for cross-border investigations. The non-territorial nature of digital evidence increasingly conflicts with territorial based legal frameworks, creating particular difficulties in time-sensitive child exploitation cases.

Despite these challenges, opportunities exist for greater harmonization. Standardized technical protocols, specialized procedural frameworks for child-related cases, and enhanced public-private cooperation models could all contribute to more effective cross-jurisdictional investigations while maintaining appropriate safeguards. As digital technologies continue to evolve, legal frameworks for digital evidence must likewise adapt. This adaptation requires ongoing dialogue between jurisdictions, technical experts, and child protection specialists to ensure that legal responses remain both effective and protective of fundamental rights. The unique vulnerability of children in digital exploitation contexts demands no less than our most thoughtful and coordinated legal response.

References

Blažič, B. J., & Klobučar, T. (2020). Investigating crime in an interconnected society: Will the new and updated EU judicial environment remove the barriers to justice? In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1183-1188). https://doi.org/10.23919/MIPRO48935.2020.9245133

Busser, E. (2018). EU-US digital data exchange to combat financial crime: Fast is the new slow. *German Law Journal, 19*(5), 1307-1332. https://doi.org/10.1017/S2071832200023117

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Chavleski, A., & Galev, G. (2019). Gathering e-evidence in cross-border cases: Recent developments in EU law. *Knowledge International Journal, 32*(1), 189-193.

Council of Europe. (2001). *Convention on Cybercrime*. European Treaty Series - No. 185. https://rm.coe.int/1680081561

Crown Prosecution Service. (2018). Child sexual abuse: Guidelines on prosecuting cases of child sexual abuse. https://www.cps.gov.uk/legal-guidance/child-sexual-abuse-guidelines-prosecuting-cases-child-sexual-abuse

Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and international lawmaking 2.0. *Stanford Law Review Online, 71*, 9-16.

Demarco, J., Davidson, J., Bifulco, A., Scally, M., Cheevers, C., Schimmenti, A., Caretti, V., Puccia, A., Corbari, E., Schilder, J., & Bogaerts, S. (2016). EU online child safety: What does the literature say? Luxembourg: Publications Office of the European Union. https://doi.org/10.2788/972621

Eggestein, J. V., & Knapp, K. (2014). Fighting child pornography: A review of legal and technological developments. *Journal of Digital Forensics, Security and Law, 9*(3). https://doi.org/10.15394/jdfsl.2014.1191

Hörnle, J. (2021). Digital investigations in the cloud—Criminal enforcement cooperation. In *Internet Jurisdiction Law and Practice*. https://doi.org/10.1093/oso/9780198806929.003.0006

INTERPOL. (2022). International Child Sexual Exploitation database. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Kent, G. (2014). Sharing investigation specific data with law enforcement - An international approach. *Stanford Public Law Working Paper*. http://dx.doi.org/10.2139/ssrn.2472413

Kerr, O. S. (2018). Implementing Carpenter. In *The digital Fourth Amendment*. Oxford University Press.

Mitsilegas, V. (2021). European criminal law after Brexit. *Criminal Law Forum, 32*, 219-252. https://doi.org/10.1007/s10609-020-09407-9

Mulligan, S. P. (2018). Cross-border data sharing under the CLOUD Act. *Congressional Research Service Report R45173*.

Rappert, B., Wilson-Kovacs, D., Wheat, H., & Leonelli, S. (2022). Evincing offence: How digital forensics turns big data into evidence for policing sexual abuse. *Engaging Science, Technology, and Society, 8*(3). https://doi.org/10.17351/ests2022.1049

Stefan, M., & Fuster, G. G. (2018). Cross-border access to electronic data through judicial cooperation in criminal matters: State of the art and latest developments in the EU and the US. *CEPS Liberty and Security in Europe Papers No. 2018-07*.

Svantesson, D. J. B. (2018). Law enforcement cross-border access to data. In N. Witzleb, D. Lindsay, M. Paterson, & S. Rodrick (Eds.), *Big Data, Political Campaigning and the Law* (pp. 196-215). Routledge.

Walden, I. (2007). *Computer crimes and digital investigations*. Oxford University Press.

WeProtect Global Alliance. (2021). Global threat assessment 2021: Working together to end child sexual exploitation and abuse online. https://www.weprotect.org/global-threat-assessment-21/