Utrecht University

FACULTY OF LAW ECONOMICS AND GOVERNANCE

LL.M. EUROPEAN LAW

Elisabeth Prants

**Student number**: 5379369

# Enhancing Cross-border Collaboration in Combatting Child Sexual Abuse:

*A Study on Europol's Role and the Dynamics of Information Sharing among the European Union Member States*

Master thesis

2023/2024

**First supervisor:** Dr. Olia Kanevskaia

**Second supervisor:** Dr. mr. Thomas Verellen

**Word count**: 12 516

June 28 2024

## Table of Contents

# 1. Introduction

## 1.1. Research Problem and Context

The difficulties of transnational crime, particularly in today's digital era, present significant challenges for law enforcement agencies across Europe. As a central figure in the European Union's (EU) to combat such crimes, Europol is pivotal in promoting information sharing and cooperation among Member States.[1] These challenges arise from several factors, including the variations in national laws across different countries and the swift pace of technological advancements.[2] As police forces globally struggle to solve problems arising from these challenges to collaborate effectively, criminal activities thrive by exploiting these gaps to their advantage.[3]

Child sexual abuse is an alarming issue with long-lasting impacts on victims. It is often hidden and undetected, happening within the circle of those the child trusts most, breaking their sense of safety. When the abuse is also recorded and shared online, the violation continues as long as perpetrators share these images and videos online, often for years. Victims know that the pictures and videos of their abuse are out there, possibly seen by people they know. This knowledge is an ongoing trauma, making them relive those terrible moments over and over.[4]

The context is set against the backdrop of the exponential development of the digital world. As time passes, cybercrime has progressively infiltrated nearly every area of criminal activity.[5] This makes the crime truly a global one and has unfortunately facilitated the creation of a worldwide market for child sexual abuse material (CSAM).[6] Child sexual abuse is a pervasive

[1] Claudio Collovà and Nele Lüker, 'Pre-legislative Synthesis: Combating Child Sexual Abuse' (European Parliamentary Research Service, January 2024) PE 757.611, p 9.

[2] Giulio Calcara, 'The Role of INTERPOL and EUROPOL in the Fight Against Cybercrime, With Particular Reference to the Sexual Exploitation of Children Online and Child Pornography' (2013) 7(1) Masaryk University Journal of Law and Technology 19, p 20.

[3] Calcara, 2013, p 20.

[4] European Commission, 'EU Strategy for a more effective fight against child sexual abuse' https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en accessed 24 February 2024.

[5] Wouter van Ballegooij, 'Revision of the Europol Regulation' (European Parliamentary Research Service, January 2021) PE 654.214, p 1.

[6] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU strategy for a more effective fight against child sexual abuse' COM(2020) 607 final (24 July 2020), p 1.

and deeply concerning issue that transcends national borders.[7] Reports[8] indicate that the EU has become the largest host of CSAM globally.[9] Year on year, there are increases in reports of online child sexual abuse content.[10] The number of reports of child sexual abuse online concerning the EU grew from 23,000 in 2010 to more than 1,5 million in 2022, which included more than 5 million images and videos.[11] It has never been easier for child sex offenders to contact their potential victims, share imagery and encourage others to commit offences.[12]

This situation needs a robust and coordinated response from law enforcement agencies across the EU. The EU combats these crimes through various methods, including joint international police operations and information systems.[13] However, difficulties with advanced technologies like end-to-end encryption and anonymity can result in under-performance across the EU in preventing, investigating and prosecuting offences related to child sexual abuse and exploitation.[14]

The societal and legal implications of child sexual abuse necessitate a competent and comprehensive response, both at the national and European levels.[15]. By focusing on these issues, this research aims to explore the mechanisms through which Europol supports Member States, the challenges faced in this collaborative endeavour, and potential improvements to enhance collective efforts against child sexual abuse.

[7] European Commission, 'EU Strategy for a more effective fight against child sexual abuse' https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en accessed 24 February 2024.

[8] Internet Watch Foundation, Face the Facts: Internet Watch Foundation Annual Report 2020 (2021) https://www.iwf.org.uk/about-us/who-we-are/annual-report-2020/ accessed 24 February 2024.

[9] European Commission, 2020a, p 2.

[10] United Nations Children's Fund (UNICEF), 'Ending Online Child Sexual Exploitation and Abuse: Lessons Learned and Promising Practices in Low- and Middle-Income Countries' (UNICEF, December 2021), p 2.

[11] European Commission, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast)' (COM(2024) 60 final, 2024/0035(COD) (6 February 2024), p 82.

[12] UNICEF, 'Protecting Children Online' (UNICEF, last updated 23 June 2022) https://www.unicef.org/protection/violence-against-children-online accessed 24 February 2024.

[13] European Commission, 'EU Strategy for a more effective fight against child sexual abuse' https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en accessed 24 February 2024.

[14] National Center for Missing & Exploited Children, 'End-to-End Encryption' https://www.missingkids.org/theissues/end-to-end-encryption accessed 17 May 2024.

[15] European Commission, 2020a, p 7.

## 1.2. Research Question

This thesis will answer the following research question: How can the EU improve cooperation and information exchange between Member States through Europol to enhance the effective prosecution and prevention of child sexual abuse, considering existing data protection challenges?

Additionally, these sub-questions will also be answered:

1. How does the legal framework employed by the EU facilitate and govern information sharing and data protection among EU Member States in the investigation of child sexual abuse cases?
2. How do Europol's mechanisms and strategies enhance coordination and information exchange among EU Member States in child sexual abuse investigations?
3. What challenges, primarily related to privacy and data protection, impact the effectiveness of cross-border cooperation and information exchange in child sexual abuse cases among EU Member States?
4. What recommendations can be made to address these challenges to improve Europol's role in facilitating more effective cross-border collaboration and information sharing among EU Member States in addressing child sexual abuse?

## 1.3. Academic Relevance of the Research

The issue of child sexual exploitation and abuse is a societal concern, as children's dependency on adults makes them particularly vulnerable to trust betrayal and significant harm. The enduring consequences on victims' well-being, such as trauma, substance abuse, self-harm or suicide, and difficulties in establishing healthy relationships later in life.[16] Survivors of CSAM are increasingly talking about the lasting harm caused by their images and videos being shared online. Not being able to control whether these files exist or stop them from spreading makes it very difficult for survivors to recover.[17] Overcoming societal attitudes and fostering an environment where victims feel supported is crucial. It is important to provide them with effective support and protection to prevent them from becoming victims of crime again. This

[16] UNICEF, 'Protecting Children Online' (UNICEF, last updated 23 June 2022) https://www.unicef.org/protection/violence-against-children-online accessed 24 February 2024.

[17] National Center for Missing & Exploited Children, 'Child Sexual Abuse Material' https://www.missingkids.org/theissues/csam accessed 25 February 2024.

topic is relevant today because children are increasingly lured to using communication and information technology.

Child abuse cases frequently involve international and cross-border dimensions, demanding intervention by the EU.[18] This complexity sets child abuse apart from other criminal areas. Effective information exchange and collaboration among the EU and the Member States are important for addressing transnational crimes in an interconnected Europe. The central inquiry revolves around examining Europol's mechanisms and strategies and its pivotal role in facilitating international cooperation and enhancing the investigative capacities of EU Member States. The focus is particularly pertinent given the digital age's challenges, where the abuse's nature and scale have evolved, requiring increased, rapid and well-functioning international cooperation in criminal matters, including child sexual abuse.[19]

Furthermore, the research delves into the vital balance between law enforcement and protecting privacy and data rights, a very relevant debate. The introduction of end-to-end encryption, while beneficial on the one side to ensure the privacy of communications, also enables child abusers to share and trade images and videos with impunity and incite each other to provide new abuse.[20] This aspect underscores the complexity of combatting online child sexual abuse within the framework of existing regulations and societal values.

Lastly, the study stands to raise awareness and foster a deeper understanding of cross-border challenges in combatting child sexual abuse, encouraging further research and action. By aiming to improve the effectiveness of collaborative efforts, the research directly contributes to the overarching goal of creating safer environments for children.

### 1.4. Research Approach and Methods

This thesis will employ a qualitative research methodology, using doctrinal, comparative, evaluative and normative approaches to comprehensively analyse the international and EU

[18] European Commission, 2024, p 102.

[19] Council of Europe, Convention on Cybercrime ETS No. 185 (23 November 2001) https://rm.coe.int/1680081561, preamble.

[20] European Commission, 'EU Strategy for a more effective fight against child sexual abuse' https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en accessed 24 February 2024.

legal frameworks that govern and balance child protection with data privacy. This analysis will delve into the complexities of these frameworks, examining how they intersect and interact to safeguard vulnerable children and personal data rights.

This research will analyse a range of legal documents, directives and regulations that are relevant to Europol’s operations and its cross-border efforts against child sexual abuse. It will also examine proposals and impact assessments (IAs) from the European Commission related to this issue. Europol’s practical tools to combat these crimes are searched through their case studies and document analysis. Additionally, the study will explore the impact of various EU regulations on privacy rights and examine their implications for Europol’s investigative processes.

Acknowledging the study's limitations, including potential biases and constraints in generalisability, this research will provide a focused exploration of the selected legal frameworks within the specified scope. While numerous challenges hinder cross-border efforts against child sexual abuse, this research primarily concentrates on the challenges related to data privacy and protection.

This research uses artificial intelligence (AI) tools to enhance the text's clarity, coherence and grammatical integrity. Specifically, Grammarly has been employed to identify and correct grammatical errors and improve phrasing. Additionally, ChatGPT has been used to refine research questions and assist in structuring the thesis chapters. While these AI tools have provided valuable initial feedback and suggestions, their outputs have been critically evaluated and adapted to ensure alignment with the university guidelines and the study's specific requirements. This approach has effectively helped the analytical and compositional aspects of the research process.

## 2. Legal Frameworks Facilitating Europol's Information Sharing

Europol collaborates extensively with law enforcement agencies, government departments and the private sector to enhance security and cross-border cooperation.[21] This chapter delves into the legal frameworks that underpin Europol's operations, focusing on data protection regulations that guide its practices. It details the legislative basis and operational mandates that enable Europol to process personal data while balancing individual rights and security needs. It provides an overview of the evolution, structure and powers of Europol. The discussion sets a base for understanding Europol's capabilities and challenges in subsequent chapters.

### 2.1. Overview of Europol's Legal Framework and Operational Mandate

Europol, the EU's law enforcement agency, established in 1999 and headquartered in The Hague, the Netherlands, assists its Member States in improving safety across Europe.[22] Europol's closest partners are the Member States.[23] As the EU's central agency for law enforcement cooperation, Europol embodies the collective effort of Member States to ensure public safety through collaboration.[24]

Officially becoming an EU agency in 2010, Europol supports Member States and analyses crime trends in the EU. The work usually involves addressing crimes that require international collaboration and cooperation between several countries, both within and outside the EU.[25] Member States leverage their liaison officers stationed at Europol and utilise the agency's information exchange channels to share intelligence and collaborate on criminal investigations.[26] Additionally, non-Member States also station liaison officers at Europol to facilitate cooperation.[27] The liaison officer network at Europol guarantees that the interests of the law enforcement agencies from EU Member States are represented at Europol's

[21] Europol, 'Partners & Collaboration' (last updated 14 February 2024) https://www.europol.europa.eu/partners-collaboration accessed 13 May 2024.
[22] European Union, 'Europol'https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/europol_en accessed 6 May 2024; Europol, 'How and where did it all start' (last updated 10 Jul 2019) https://www.europol.europa.eu/faq/how-and-where-did-it-all-start accessed 6 May 2024.
[23] Europol, 'Member States' (last updated 9 December 2021) https://www.europol.europa.eu/partners-collaboration/member-states accessed 13 May 2024.
[24] European Commission, 2020b, p 5.
[25] Europol, 'About Europol' https://www.europol.europa.eu/about-europol accessed 6 May 2024.
[26] *Ibid.*
[27] Europol, 2024b.

headquarters.[28] The Member States also pool resources, entrusting Europol to manage their data within its databases and provide joint analysis.[29] The agency's accumulating expertise in various policing areas has established Europol as a crucial and highly effective component of EU support for national law enforcement authorities.[30]

Central to Europol's operational effectiveness is the principle of sincere cooperation outlined in Article 4(3) of the Treaty on European Union (TEU).[31] This principle obligates Member States to assist each other in carrying out tasks that flow from the Treaties, ensuring the fulfilment of obligations under the Treaties, and refraining from any measure which could jeopardise the attainment of the Union's objectives. In the context of Europol, Member States must actively cooperate and share relevant information to combat cross-border crime effectively, aligning their national policies with EU strategies and directives to enhance security and law enforcement efforts.

Building on this foundation of cooperation, the legislative mandate for Europol is further specified in Article 88 of the Treaty of the Functioning of the European Union (TFEU).[32] This Article details that Europol's role is to support and enhance the efforts of police authorities and other Law enforcement services from the Member States, fostering their collaboration in the prevention and fight against serious crimes impacting two or more Member States, terrorism, and crimes that threaten a shared interest under a Union policy.[33] Additionally, it specifies that Europol shall be regulated by a Regulation adopted through the ordinary legislative procedure.[34]

The Europol Regulation[35] outlines Europol's powers, structure, and data handling procedures. It was adopted by the European Parliament and the Council of the EU on 11 May 2016.[36] It

[28] Europol, 2021b.

[29] European Commission, 2020b p 5.

[30] *Ibid.*

[31] Treaty on European Union (TEU) [2012] OJ C 326/13.

[32] Treaty on the Functioning of the European Union (TFEU) [2012] OJ C 326/47.

[33] European Commission, 'Proposal for a Regulation of the European Parliament and the Council Amending Regulation (EU) 2016/794' COM(2020) 796 final 2020/0349(COD) (9 December 2020), p 5.

[34] *Ibid.*

[35] European Parliament and Council Regulation 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) [2016] OJ L 135/53.

[36] Europol, 'About Europol' https://www.europol.europa.eu/about-europol accessed 6 May 2024.

strengthens Europol's role in supporting cooperation among law enforcement authorities in the EU.[37]

The primary objective of Europol follows from Article 3(1) of the Regulation. It states that Europol shall support and strengthen its Member States in preventing and combatting all forms of serious international and organised crime, cybercrime and terrorism.[38]

Article 4(1) of the Regulation specifies Europol's tasks necessary to achieve the objectives outlined in Article 3. Most of them focus on collaboration with Member States.

Article 4(1)(c) mandates Europol to coordinate, organise, and implement investigative and operational actions. These efforts are designed to support and strengthen the activities of the competent authorities from the Member States when these actions are carried out jointly. This provision ensures that Europol plays a pivotal role in enhancing the effectiveness of national law enforcement agencies by providing critical support and coordination in joint operations, thus strengthening the collective capacity to combat crime across the EU.

Under Article 4(1)(e), Europol provides information and analytical support to Member States during major international events, ensuring comprehensive preparation and response strategies for potential security. Article 4(1)(g) highlights Europol's role in advancing crime prevention through developing, sharing and promoting specialised knowledge of crime prevention methods, investigative procedures and technical and forensic methods. Additionally, it involves offering advice to Member States to enhance their law enforcement capabilities. As stated in Article 4(1)(h), Europol supports cross-border information exchanges, operations, and investigations, including joint investigation teams (JITs). This includes providing operational, technical and financial assistance to enhance collaborative efforts among Member States.

Article 4(1)(m) emphasises Europol's commitment to fighting internet-facilitated crimes, as listed in Annex I. This includes combatting sexual abuse and exploitation, also targeting child abuse material and solicitation of children for sexual purposes. This involves assisting Member States in responding to cyberattacks of suspected criminal origin, cooperating on the

[37] *Ibid.*
[38] *Ibid.*

enforcement of removal orders as per Regulation 2021/784[39], and facilitating the referral of online content to service providers for review against their terms of service. According to Article 4(1)(t), Europol assists Member States in processing data related to individuals involved in terrorism or serious crime, provided by third countries or international organisations. Europol also supports the potential inclusion of information alerts on third-country nationals in the Schengen Information System (SIS), aligning with Regulation 2018/1862[40]. Lastly, Article 4(1) y outlines Europol's supportive role in addressing the online dissemination of child sexual abuse material, reinforcing the agency's commitment to tackling severe online crimes and enhancing child protection measures.

Key amendments to the Europol Regulation entered into force on 28 June 2022.[41] These amendments introduced changes in several areas such as support for criminal investigation.[42] Under the conditions specified in the amended Regulation, Europol is authorised to process personal data without Data Subject Categorisation (DSC) as long as it is necessary for aiding a specific ongoing criminal investigation.[43] Additionally, the revised Europol Regulation enhances cooperation with private parties, who often possess data crucial for criminal investigations.[44] The updated legal framework allows Europol to receive data directly from these parties. Furthermore, the amendment introduces specific rules that govern cooperation with private entities in cases involving the online dissemination of child sexual abuse material.[45]

As action at the national level alone does not suffice to address these transnational security challenges, Member States' law enforcement authorities have increasingly used Europol's support and expertise to counter serious crime and terrorism.[46]

[39] European Parliament and Council Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79.
[40] European Parliament and Council Regulation 2018/1862 of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters [2018] OJ L 312/7.
[41] Europol, 'Europol's amended Regulation enters into force' (published 28 June 2022) https://www.europol.europa.eu/media-press/newsroom/news/europols-amended-regulation-enters-force accessed 7 May 2024.
[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.*
[45] *Ibid.*
[46] European Commission, 2020b, p 5.

Europol enhances the effectiveness of law enforcement activities across EU Member States through several key initiatives.[47] One of them is facilitating the exchange of information between national agencies and Europol's liaison officers.[48] That promotes better coordination and efficiency in operations. Additionally, Europol provides operational analysis and support to Member States.[49]

In addition to operational support, Europol offers expertise and technical support for investigations, under the supervision and legal responsibility of the respective Member States.[50] This role is crucial in maintaining the integrity and effectiveness of local law enforcement within the EU framework. Moreover, Europol produces strategic reports and crime analyses based on intelligence from Member States or other sources.[51]

Furthermore, Europol is vital in harmonising investigative techniques across Member States and actively organises events to raise awareness among law enforcement officers about its services.[52] This helps to improve their knowledge and effectiveness in handling international cases, thus strengthening overall security and law enforcement collaboration within the EU.[53]

### 2.2. Child Sexual Abuse Directive

The EU's key instrument for addressing child sexual abuse is Directive 2011/93/EU[54], also known as the Child Sexual Abuse Directive.[55] It was enacted on 13 December 2011.[56] This directive is also fundamental in setting the legal framework for addressing such crimes across the EU, which directly ties into Europol's operational mandate and activities. It forms a core part of the legislative environment that Europol operates within.

The Child Sexual Abuse Directive aims to standardise the legal framework across Member States by harmonising definitions of criminal offences such as child sexual abuse, sexual

[47] Europol, 2021b.
[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*
[51] *Ibid.*
[52] *Ibid.*
[53] *Ibid.*
[54] European Parliament and Council Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L 335/1.
[55] Collovà and Lüker, 2024, p 2.
[56] *Ibid.*

exploitation, child pornography and grooming, while also increasing minimum penalties for these crimes.[57] The directive outlines preventative measures, including strategies for identifying and managing potential offenders or recidivists.[58] It also prohibits individuals with histories of offences from holding jobs that entail regular contact with children.[59] It also includes provisions to safeguard child victims during investigations and legal proceedings.[60] Additionally, the directive promotes strengthened collaboration between Member States and non-Member States to combat child sex tourism.[61]

### 2.3. Data Privacy Measures in Information Sharing

Data protection is a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union (EU Charter).[62] It is also established as a principle in Article 16 TFEU.[63] The EU has implemented several measures to combat child sexual exploitation while ensuring data protection and privacy.

#### 2.3.1. Data Protection in the Europol Regulation

Under Article 36 of the Europol Regulation, Europol must confirm whether they process personal data concerning an individual.[64] Europol must grant access to this data if such data is being processed.[65] The individual is entitled to know the purpose and legal basis for the processing, the types of personal data being processed and who has received the data, particularly if it involves third countries or international organisations.[66] Additionally, Europol must inform the individual of the expected duration of data storage, their rights to amend or delete their data and how to contact and lodge a complaint with the European Data Protection Supervisor.[67]

[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid.*
[60] *Ibid.*
[61] *Ibid.*
[62] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391; Van Ballegooij, 2021, p 6.
[63] Mariusz Maciejewski, 'Personal data protection' (Fact Sheets on the European Union, November 2023) https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection accessed 2 June 2024; Van Ballegooij, 2021, p 6.
[64] Europol, 'Right of access' (last updated 27 March 2024) https://www.europol.europa.eu/right-of-access accessed 14 May 2024.
[65] *Ibid.*
[66] *Ibid.*
[67] *Ibid.*

According to Article 81 of Regulation 2018/1725[68], which is also referenced in Article 27a of the Amended Europol Regulation, there are circumstances where Europol may restrict access to personal data.[69] These restrictions are necessary to prevent interference with legal processes, protect public and national security or safeguard the rights of others, like victims and witnesses.[70] These measures are taken to balance individual rights with the need to maintain security and justice.[71]

### 2.3.2. General Data Protection Regulation

Regulation 2016/679[72], also known as the General Data Protection Regulation (GDPR), ensures the protection of individual data privacy during processing by most private and public sector entities, as detailed in Recital 6. It affirms the fundamental right to data protection.[73] Recital 7 further emphasises that the GDPR grants individuals greater control over their personal data while modernising and harmonising the rules.

The GDPR is highly relevant in the context of combatting child sexual abuse. Although it does not contain provisions specific to combatting child sexual abuse, it applies to all personal data processing activities, except for criminal justice activities governed by Directive 2016/680/EU.[74] Also, the Child Sexual Abuse Directive aligns with the GDPR and Directive 2016/680/EU, maintaining strong data protection safeguards.[75] Member States are responsible for enforcing these rules through their data protection authorities and courts.[76]

[68] Europol Parliament and Council Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data [2018] OJ L 295/39.

[69] Europol, 2024c.

[70] *Ibid.*

[71] *Ibid.*

[72] European Parliament and Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

[73] European Commission, 2024, p 8.

[74] European Commission, 2024, p 9; European Parliament and Council Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

[75] European Commission, 2024, p 9.

[76] *Ibid.*

A significant challenge arises from the use of end-to-end encryption (E2EE). While E2EE protects individuals' privacy, it also limits Europol's and Member States' law enforcement agencies' ability to access crucial data during investigations. This tension between safeguarding personal data and enabling effective law enforcement illustrates the complexities Europol faces under the GDPR framework. These specific challenges posed by the E2EE are discussed in further detail in the Challenges Chapter.

### 2.3.3. The Digital Services Act

The Regulation 2022/2065[77], generally known as the Digital Services Act (DSA), establishes a comprehensive framework of due diligence obligations for content moderation by intermediary service providers.[78] Article 1(1) of the DSA states that its purpose is to foster a safer and more accountable online environment that promotes innovation and enhances the protection of fundamental rights. Furthermore, Recital 9 of the Regulation specifies that the DSA fully harmonises the rules governing intermediary services within the internal market. It eliminates several disincentives that hinder providers' voluntary initiatives to detect, remove or restrict success to illegal content, such as CSAM. [79]

Moreover, the DSA represents a significant step forward in holding digital companies accountable for their platforms' content, including child-related content.[80] For example, the DSA mandates the swift removal of illegal online content such as CSAM, hate speech, terrorist content and illegal products with platforms like TikTok and Facebook increasingly training moderators to identify these types of content.[81]

Recital 61 of the DSA notes that the effectiveness of combatting illegal content, particularly CSAM, increases when online platforms prioritise notices from trusted flaggers. Trusted flagger status, granted by the Digital Services Coordinator of the Member State where they are established, is given to entities like Europol and members of the INHOPE network, who are

[77] European Parliament and Council Regulation 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1.
[78] European Commission, 2024, p 9.
[79] *Ibid.*, p 9-10.
[80] Negreiro, 2023, p 3.
[81] *Ibid.*

recognised for their expertise in managing such content. That way the DSA enhances Europol's capabilities by collaborating with online platforms. Europol can work closely together with online platforms to identify and investigate instances of child sexual abuse. The DSA's requirements for transparency and cooperation facilitate Europol's access to data and its ability to respond quickly to threats

Additionally, Article 18(2) of the DSA specifies that if the hosting service provider cannot reasonably determine the concerned Member State, it must notify the Member State's law enforcement authorities where it was established or where its legal representative resides. Alternatively, the provider may inform Europol.

### 2.3.4. The Interim Regulation

Currently, Regulation 2021/1232 (the Interim Regulation)[82] provides a temporary exception from certain requirements of Directive 2002/58/EC (the e-Privacy Directive)[83] which protects the confidentiality of communications.[84] According to Article 1 of the Interim Regulation, its purpose is to enable providers of number-independent interpersonal communications services ('providers') to use specific technologies for processing personal data. This exception allows providers of certain communication services to maintain their voluntary efforts in detecting, reporting and removing online CSAM.[85]

Recitals 1 and 2 of Regulation 2024/1307 clarify that although the Interim Regulation was initially set to expire on 3 August 2024, uncertainties regarding establishing a suitable framework by the end date necessitated a temporary extension.[86] Consequently, the co-legislators adopted Regulation 2024/1307, which takes effect on 4 August 2024, introducing amendments to the Interim Regulation. Additionally, Recital 3 highlights the legislators'

[82] European Parliament and Council Regulation 2021/1232 of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 274/41.

[83] European Parliament and the Council Directive 2002/58/EC of 13 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37.

[84] Negreiro, 2023, p 3.

[85] *Ibid.*

[86] European Parliament and Council Regulation 2024/1307 of 29 April 2024 on amending Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2024] OJ L series.

commitment to establishing a long-term legal framework to prevent any future extensions of the Interim Regulation.

According to Recital 6 of the Interim Regulation, it is in line with Directive 2011/93/EU. It does not dictate Member States' policies concerning consensual sexual activities involving children, which may be considered normal exploration of sexuality during human development. It respects the diverse cultural and legal traditions and acknowledges new ways children and adolescents establish and maintain relationships, including through information and communication technologies.

### 2.4. Integration with External Agencies and Third Parties

Article 4(1)(c)(ii) of the Europol Regulation states that Europol works together with Eurojust where appropriate. Article 26 of the Europol Regulation outlines the conditions under which Europol can exchange data with private parties.[87] Europol can receive (bulk) personal data from private parties if it is only processed to identify the relevant Member State, third country or international organisation.[88] These entities can then decide to resubmit the data to Europol within four months of the initial transfer.[89] Thus, data exchanges between Europol and private parties typically occur indirectly through National Units (ENUs) or contact points in third countries or international organisations.[90] However, in specific cases where it is necessary and in the data subject's interest, Europol may directly send personal data to private parties.[91] This is allowed to prevent imminent crime or, in cases where the crime is publicly known, combat cybercrime.[92]

The legal frameworks governing Europol's operations, particularly regarding data protection, play an important role in balancing individual privacy with the demands of law enforcement. These regulations ensure that Europol's data processing activities are transparent, accountable and secure. Amendments to the regulation have expanded these capabilities, aiming to enhance Europol's effectiveness in crime prevention and investigation while also maintaining peace and

[87] Van Ballegooij, 2021, p 5.
[88] *Ibid.*
[89] *Ibid.*
[90] *Ibid.*
[91] *Ibid.*
[92] *Ibid.*

security within the EU.[93] The next chapter will explore Europol's information sharing and investigative strategies. It will analyse how these strategies leverage the established legal frameworks to facilitate cross-border cooperation and improve intelligence sharing, reinforcing Europol's critical role in ensuring safety and justice across the EU.

[93] Adam J. McKee, 'European Police Office' (Doc McKee, last modified 19 May 2023) https://docmckee.com/cj/docs-criminal-justice-glossary/european-police-office-definition/ accessed 6 May 2024.

## 3. Europol's Information Sharing and Investigative Strategies

In the digital age, child sexual abuse is a constantly evolving phenomenon, which is heavily influenced by technical advancements.[94] Europol strategically uses technological tools and collaborative initiatives to address child sexual abuse in the digital age. The agency employs advanced technology, strategic partnerships and innovative platforms to track and analyse the digital footprints left by offenders.

### 3.1. The Europol Cybercrime Centre

The Europol Cyber Crime Centre (EC3), established within Europol, plays a significant role in fighting cybercrime, including the issue of child sexual abuse.[95] EC3's main focus is strengthening the law enforcement response to cybercrime across the EU and helping protect EU citizens, businesses and governments from online crime.[96]

EC3 offers operational analysis, coordination and expertise to assist national law enforcement agencies in investigating online child sexual abuse.[97] This includes providing specialised technical and digital forensic support to investigations and operations.[98] The centre acts as a hub for sharing information and intelligence related to cyber threats, including those linked to child sexual abuse networks.[99] It facilitates the exchange of information between Member States and coordinates cross-border collaborative efforts to tackle these pervasive crimes.[100]

EC3 assists competent authorities in Member States with the prevention and detection of all forms of criminal activity related to the sexual exploitation of children.[101] The centre offers support and expertise in fighting the distribution of child abuse material across various online platforms.[102] It addresses all forms of criminal online behaviour against children, such as

[94] Europol, 'Child Sexual Exploitation' https://www.europol.europa.eu/crime-areas/child-sexual-exploitation accessed 13 May 2024.

[95] Europol, 'Europol Cybercrime Centre (EC3)' https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 accessed 8 May 2024.

[96] *Ibid.*

[97] *Ibid.*

[98] *Ibid.*

[99] *Ibid.*

[100] *Ibid.*

[101] Europol, 'Child Sexual Exploitation' https://www.europol.europa.eu/crime-areas/child-sexual-exploitation accessed 13 May 2024.

[102] *Ibid.*

grooming, self-generated indecent material, sexual extortion and live-streaming on the web.[103] It works closely with various countries' law enforcement to track offenders, dismantle networks and rescue victims.

Since 2014, Europol has regularly gathered victim identification specialists from around the world to focus on unsolved child sexual abuse cases.[104] Six children were identified and rescued from abuse as a result of the 12th Victim Identification Taskforce held by Europol's EC3.[105] Over 30 specialists around the world, along with Europol experts, gathered both at Europol's headquarters and online to analyse over 460 sets of images and videos of child sexual abuse, involving victims as young as a few days old.[106] This collaborative effort led to the arrest of one offender.[107] While it may seem that only one arrest is too few, identifying these perpetrators is extremely challenging, and every arrest is a crucial step forward. Thus, apprehending even a single offender represents a success in the ongoing battle against child sexual abuse. The task also narrowed down the likely country of origin for the abuse material in 236 cases, with further national-level investigations now underway to identify more victims.[108]

EC3's support does not end there. It has a dedicated team of specialists which assists countries in combatting child sexual abuse and exploitation online.[109] This team, known as AP Twins, supports the prevention and combatting of child sexual exploitation and abuse.[110] It targets the production and distribution of child abuse material across online environments, alongside other internet-facilitated crimes against children such as grooming and sexual extortion.[111] In 2022, this team assisted in 93 investigations against this crime.[112]

[103] *Ibid.*
[104] Europol, 'Six sexually-abused children rescued as a result of Europol Victim Identification Taskforce' (published 26 May 2023) https://www.europol.europa.eu/media-press/newsroom/news/six-sexually-abused-children-rescued-result-of-europol-victim-identification-taskforce accessed 20 June 2024.
[105] *Ibid.*
[106] *Ibid.*
[107] *Ibid.*
[108] *Ibid.*
[109] *Ibid.*
[110] Europol, 'Europol Analysis Projects' (last updated 24 April 2023) https://www.europol.europa.eu/operations-services-innovation/europol-analysis-projects accessed 9 May 2024.
[111] *Ibid.*
[112] Europol, 2023d.

### 3.2. Schengen Information System

The Schengen Information System (SIS) is Europe's largest and most used security and border management information-sharing system.[113] It enhances cooperation among the Schengen countries' border, immigration, police, customs and judicial authorities.[114] This enables effective information sharing that is vital in aiding Europol and other law enforcement agencies across Europe in combatting child sexual abuse.

The SIS allows a country to enter an alert that immediately becomes available to all participating countries in real time, enabling all relevant authorities to access and act upon these alerts across the EU promptly.[115] This instant access is crucial for addressing transnational crimes like child sexual abuse, which involve perpetrators and victims from multiple countries. It is particularly vital for the timely interception of suspects at borders and for preventing potential cross-border crimes, like trafficking or abduction of children.

In March 2023, the SIS was upgraded granting Europol access to all alert categories.[116] As mentioned in the Legal Frameworks chapter, the changes now permit the agency to recommend that EU countries issue information alerts in the SIS for suspected terrorists and criminals, based on data received from non-EU countries.[117] This allows for enhanced information exchange with Member States on serious crime areas, such as child sexual abuse.

The SIS proved its effectiveness in a case where a 10-year-old kidnapped in Poland was located in Germany in less than 24 hours.[118] This quick resolution was made possible by the Polish police swiftly issuing a missing person alert through the SIS, highlighting its importance in handling cross-border emergencies.[119]

[113] European Commission, 'Schengen Information System' https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en accessed 17 June 2024.

[114] *Ibid.*

[115] European Commission, 'What is SIS and how does it work?' https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en accessed 17 June 2024.

[116] *Ibid.*

[117] *Ibid.*

[118] European Commission, 'EU Schengen Information System saves lives' (News article, 19 September 2023) https://home-affairs.ec.europa.eu/news/eu-schengen-information-system-saves-lives-2023-09-19_en accessed 17 June 2024.

[119] *Ibid*.

### 3.3. European Multidisciplinary Platform Against Criminal Threats

In 2010, the Council launched the European Multidisciplinary Platform Against Criminal Threats (EMPACT), a new four-year security initiative led by EU Member States to identify, prioritise and tackle threats from organised and serious international crime.[120] It has become a key EU tool for multidisciplinary and multiagency efforts to combat organised crime, focusing on addressing the most pressing criminal threats to the EU.[121] On 8 March 2021, the Council approved the ongoing implementation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022+.[122]

EMPACT employs a structured methodology to systematically and coherently address the most significant threats, including organised and serious international crimes, such as child sexual exploitation.[123] It aims to strengthen cooperation among EU Member States, institutions, agencies, third-party countries and organisations.[124] EMPACT operates through a four-step cycle: 1) Policy development using the EU Serious and Organised Crime Threat Assessment (SOCTA) by Europol to identify threats; 2) The Council sets priorities, each with a Multi-Annual Strategic Plan (MASP); 3) Development, implementation and monitorisation of annual Operational Action Plans (OAP) in line with MASP's goals; 4) Evaluation at cycle's end for future improvements.[125] This integrated approach integrates various measures, including law enforcement, police and judicial cooperation, information management and innovation.[126]

[120] European Commission, 'EMPACT fighting crime together' https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/empact-fighting-crime-together_en accessed 20 June 2024.
[121] Europol, 'EU Policy Cycle – EMPACT' https://www.europol.europa.eu/crime-areas-and-statistics/empact accessed 19 June 2024.
[122] Council of the European Union, 'Permanent Continuation of the EU Policy Cycle for Organised and Serious International Crime: EMPACT 2022+' (Council Document, ST-9921-2021-INIT, 8 March 2021) https://data.consilium.europa.eu/doc/document/ST-9921-2021-INIT/en/pdf accessed 20 June 2024, p 4.
[123] Europol, 'EU Policy Cycle – EMPACT' https://www.europol.europa.eu/crime-areas-and-statistics/empact accessed 19 June 2024.
[124] *Ibid.*
[125] Council of the European Union, 2021, p 5; Slađana Mladenović, 'Strategic Response of EU Institutions on Cybercrime in the post-Lisbon Period'(International Scientific Conference "Archibald Reiss Days", Belgrade, 3-4 March 2015) https://www.researchgate.net/publication/380630893_Strategic_Response_of_EU_Institutions_on_Cybercrime_in_the_post-Lisbon_Period accessed 20 June 2024, p 237.
[126] Europol, 'EU Policy Cycle – EMPACT' https://www.europol.europa.eu/crime-areas-and-statistics/empact accessed 19 June 2024.

As part of the EMPACT 2022-2025, tackling online and offline child sexual exploitation as a form of cybercrime is one of the top priorities.[127] In September 2023, a training seminar supported by Europol was organised within the EMPACT framework, gathering law enforcement officers from 27 European countries.[128] This seminar focused on investigative techniques for tackling the distribution of child sexual abuse images via file-sharing networks.[129] Expert investigators delivered the training, emphasising the detection and analysis of illegal files and the identification of perpetrators who use these networks to distribute such material.[130]

Using the skills acquired from the seminar, a subsequent law enforcement action led to the arrest of 57 men suspected of possessing and sharing CSAM.[131] The suspects, ranging in age from 23 to 72, came from all walks of life, including four school teachers and one person who worked with disabled children.[132] The operation also resulted in the seizure of over 100 000 illegal files, with forensic examinations ongoing and estimates that over one million images and videos will ultimately be confiscated.[133] Europol identified suspects who also possessed materials such as paedophile manuals as High Value Targets, indicating a higher likelihood of direct abuse.[134] This classification guides further investigations and prioritises actions against those posing the greatest risk to children.[135]

The primary strategic objective of operations like this is to eliminate the risk of children being sexually abused.[136] During this operation, at least one child was rescued from ongoing physical abuse, and several others were safeguarded from potential harm.[137] These outcomes, though seemingly small, are crucial and represent progress in protecting vulnerable children from abuse.

[127] Europol, ‘Child Sexual Exploitation’ https://www.europol.europa.eu/crime-areas/child-sexual-exploitation accessed 13 May 2024.
[128] Europol, ’57 men arrested for possessing and sharing over 100 000 depictions of child sexual abuse’ (published 8 March 2024) https://www.europol.europa.eu/media-press/newsroom/news/57-men-arrested-for-possessing-and-sharing-over-100-000-depictions-of-child-sexual-abuse accessed 31 May 2024.
[129] *Ibid.*
[130] *Ibid.*
[131] *Ibid.*
[132] *Ibid.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Ibid.*
[136] *Ibid.*
[137] *Ibid.*

### 3.4. Secure Information Exchange Network Application

In an organisation like Europol, which depends on the exchange of information, ensuring the secure and rapid transmission of sensitive and restricted data is crucial.[138] The Secure Information Exchange Network Application (SIENA) is a platform designed to meet the communication requirements of EU law enforcement.[139] It facilitates the swift and user-friendly exchange of operational and strategic crime-related information, including data on child sexual abuse cases.[140] This data is shared among Europol's liaison officers, analysts and experts, Member States, and Third Parties with whom Europol has cooperation agreements or working arrangements.[141]

In recent years, SIENA has become the main information exchange channel for specialised law enforcement units and various initiatives.[142] The third step of the previously discussed EMPACT cycle involves developing, implementing and monitoring OAPs, which are crucial for managing crime priorities from 2022 to 2025.[143] SIENA plays a pivotal role in the secure exchange of criminal investigation data.[144]

SIENA facilitates the efficient transfer and analysis of data to Europol, supporting the intelligence cycle essential for adjusting strategic goals and priorities, particularly in response to new or evolving threats identified during mid-term reviews.[145] The execution and effectiveness of the OAPs rely heavily on the robust capabilities of SIENA to ensure that accurate and timely information strengthens all operational actions within EMPACT.[146]

[138] Europol, 'Secure Information Exchange Network Application (SIENA)' (last updated 10 June 2022) https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena accessed 24 May 2024.
[139] *Ibid.*
[140] *Ibid.*
[141] *Ibid.*
[142] *Ibid.*
[143] Europol, 'EU Policy Cycle – EMPACT' https://www.europol.europa.eu/crime-areas-and-statistics/empact accessed 19 June 2024.
[144] *Ibid.*
[145] *Ibid.*
[146] *Ibid.*

Europol's Strategy 2020+[147] aims to expand and enhance SIENA by advancing Europol's information management architecture and swiftly adopting new methods and technologies as they emerge.[148] SIENA is essential to making Europol the EU's central information hub, connecting Europol more closely to front-line law enforcement.[149]

Europol recently shared that over 3000 law enforcement authorities from more than 70 countries and international entities are now connected via SIENA.[150] In 2023, a record 1,79 million messages were exchanged through SIENA, emphasising its importance as Europe's primary law enforcement communication channel.[151] Expanding SIENA's network to include more countries enhances the collective intelligence on crimes, including child sexual abuse, allowing for quicker identification and response to such threats across borders.[152]

### 3.5. Stop Child Abuse – Trace an Object

Europol's Stop Child Abuse – Trace an Object (SCATO) initiative is one of the best examples of how law enforcement uses crowdsourcing to fight online child sexual exploitation (OCSE).[153] According to Howe, crowdsourcing is an open-call task performed by a large volunteer group of individuals with varying knowledge and skills.[154] This platform engages the public in providing tips about objects related to child sexual abuse images to help identify the context and potentially the location of the abuse.[155]

Ilbiz and Kaunert evaluated the platform's effectiveness using three key factors: public accessibility, the transaction costs associated with gathering information, and trust building between the public and law enforcement agencies. Their analysis, which included reviewing

[147] Europol, 'Europol Strategy 2020+' (13 December 2018) https://www.europol.europa.eu/sites/default/files/documents/europol_strategy_2020.pdf accessed 21 June 2024.
[148] Europol, 2022b.
[149] *Ibid.*
[150] Europol, 'More than 3000 law enforcement authorities now connected to Europol' (published 12 April 2024) https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol accessed 21 June 2024.
[151] *Ibid.*
[152] *Ibid.*
[153] Ethem Ilbiz and Christian Kaunert, 'Crowdsourcing to Tackle Online Child Sexual Exploitation: Europol's 'Stop Child Abuse – Trace an Object' Platform' (2023) Policing: A Journal of Policy and Practice https://academic.oup.com/policing/article/doi/10.1093/police/paad009/7084824 accessed 17 June 2024, p 2.
[154] Jeff Howe, 'The Rise of Crowdsourcing' (Wired, 1 June 2006) https://www.wired.com/2006/06/crowds/ accessed 17 June 2024; Ilbiz and Kaunert, 2023, p 3.
[155] Europol, 'Stop Child Abuse – Trace an Object' https://www.europol.europa.eu/stopchildabuse accessed 17 June 2024; Ilbiz and Kaunert, 2023, p 2.

Europol documents and interviewing law enforcement and NGO representatives, concluded that the SCATO platform is user-friendly and easily accessible to the public.[156]

However, senior law enforcement officials note that crowdsourcing is not always the optimal method for such investigations due to higher transaction costs for gathering intelligence.[157] Effective crowdsourcing requires high-value tips to offset these costs.[158] One of the challenges is the limited public recognition of partially obscured images on the SCATO platform, intended to protect victims' identities and investigation integrity.[159] Consequently, low-value tips increase workloads and costs for law enforcement, driving a shift towards investing in AI and advanced photo analysis technologies.[160]

Handling OCSE cases is sensitive and public hesitancy to report these cases is common[161]. Thus, establishing trust between the public and law enforcement is crucial for effective information collection on crowdsourcing platforms.[162] Furthermore, Europol's SCATO platform lacks clear guidelines on managing public tips, including their collection, processing, storage and eventual termination.[163] Effective communication, including clear guidelines and positive success stories, might improve crowd engagement and trust.[164] Although Europol shares success statistics, these often reveal the limited utility of most tips, suggesting a need for more meaningful feedback to the public.[165]

Europol's efforts to combat OCSE use these tools for operational support, rapid information sharing and public engagement. While effective, there are still privacy and data protection concerns that halter Europol's efforts. The next chapter will explore these challenges, focusing on balancing law enforcement needs with privacy rights in cross-border cooperation.

[156] Ilbiz and Kaunert, 2023, p 1.
[157] *Ibid.*, p 6.
[158] *Ibid.*
[159] *Ibid.*
[160] *Ibid.*
[161] *Ibid.*, p 7.
[162] *Ibid.*
[163] *Ibid.*
[164] *Ibid.*
[165] *Ibid.*, p 8.

# 4. Privacy Challenges in Cross-Border Cooperation and Data Protection

Navigating the delicate balance between robust law enforcement and stringent data protection presents a formidable challenge in the fight against child sexual abuse within the EU. This chapter delves into the complexities of cross-border cooperation, highlighting how privacy concerns and the diverse implementation of EU laws complicate the efficient exchange of crucial information.

## 4.1. Jurisdictional and Legal Challenges with the Child Sexual Abuse Directive

Effective cooperation between police forces of different Member States in addressing child sexual abuse requires a solid common legal framework.[166] Detailed international agreements and conventions are crucial, enabling police forces from various countries to cooperate more synergistically and effectively on a transnational level.[167]

However, the lack of a common legal framework often leads to obstacles in developing a strong and coordinated response.[168] Despite the universal condemnation of child pornography and child sexual abuse in general, the legal landscape remains fragmented.[169] Substantial variations in national laws across Member States create challenges in aligning enforcement efforts.[170] International regulations and conventions often fail to establish a strong common legal framework.[171]

This allows criminal activities to exploit these legal gaps and continue to thrive, undermining the efforts that police forces worldwide attempt to overcome these heinous crimes.[172] This sub-chapter delves into the institutional framework surrounding these data protection and anonymity challenges within Europol's operations.

The Child Sexual Abuse Directive, previously addressed in the legal frameworks chapter, faces significant challenges that hinder effective cooperation among Member States, consequently impeding Europol's work. Officially enacted on 13 December 2011, Member States were

[166] Calcara, 2013, p 20.
[167] *Ibid.*
[168] *Ibid.*
[169] *Ibid.*
[170] *Ibid.*
[171] *Ibid.*
[172] *Ibid.*

required to implement the necessary legal, regulatory and administrative measures by 18 December 2013 to comply with the directive.[173] The implementation of the Child Sexual Abuse Directive has not had the expected result.[174] The national laws have revealed several shortcomings and fragmentation among Member States.[175]

Although some Member States have transposed the contents of the directive into their national laws, recognising acts of child sexual abuse and exploitation as criminal offences, the directive's potential has yet to be realised.[176] The complete implementation of all its provisions by Member States is essential for achieving its intended impact.[177] Additionally, the obstacles to the complete implementation of the directive include the use of vague or ambiguous terminology in some of its provisions, which complicates the enforcement and harmonisation of the directive across the EU.[178]

In 2019, the Commission opened infringement procedures against 23 Member States to address their ongoing failure to implement the directive fully.[179] On the EUR-Lex National transposition page for Directive 2011/93/EU, which receives weekly updates, it is clear that several Member States have not yet fully transposed the directive. Also, various reports, such as the one by Missing Children Europe, ECPAT and eNACSO, highlight that while legislative measures are in place, the practical implementation and compliance still differ across the EU.[180]

In 2018 and 2019, the Commission held six specialised workshops to assist Member States in incorporating various provisions and to gain a deeper understanding of the challenges involved.[181] These workshops and further bilateral discussions between the Commission and Member States, highlighted the need for more structured and ongoing support.[182] This is

[173] Collovà and Lüker, 2024, p 2.
[174] Carmina-Elena Tolbaru, 'Fight Against Sexual Abuse and Online Exploitation of Children – Key Priority at the European Union Level' (2022) 1 International Journal of Legal and Social Order 347, p 348.
[175] Mar Negreiro, 'Combating child sexual abuse online' (European Parliamentary Research Service, June 2023) PE 738.224, p 3.
[176] Tolbaru, 2022, p 348; European Commission, 2020a, p 3.
[177] *Ibid.*
[178] European Commission, 2024, p 102.
[179] European Commission, 2020a, p 3.
[180] Missing Children Europe, ECPAT and eNACSO, 'A Survey on the Transposition of Directive 2011/93/EU on Combatting Sexual Abuse and Sexual Exploitation of Children and Child Pornography' (2016) http://www.enacso.eu/news/survey-on-the-transposition-of-directive-201193eu-on-combating-sexual-abuse-and-sexual-exploitation-of-children-and-child-pornography/ accessed 22 June 2024.
[181] European Commission, 2024, p 36.
[182] *Ibid.*

particularly evident in prevention and victim assistance, areas not traditionally emphasised in Member States' strategies against child sexual abuse.[183] The primary issues often stem from a lack of expertise in relevant fields and challenges in communication and coordination among key stakeholders, such as different government ministries.[184] Notably, there is still considerable scope for enhancement in the area of interventions targeting potential offenders.[185]

### 4.2. End-to-end Encryption

The rapid development of technology has not only led to increased crime but has also raised significant questions about data protection and privacy. A key issue is E2EE, which prevents any third party from viewing, reading or intercepting information exchanged between individuals.[186] In response to growing concerns about online data security, many technology companies are adopting E2EE.[187] However, this strategy has potential drawbacks. E2EE can prevent companies and third parties from detecting illegal activities on their platforms, including those who use the internet to demand graphic sexual abuse material from children.[188]

Without exceptions to E2EE, child abuse will continue undetected, leaving victims as collateral damage while protecting abusers and those who trade the images and videos of the abuse.[189] This ongoing circulation of abusive images and videos online causes prolonged trauma and feelings of revictimisation among survivors.[190] EU commissioner for home affairs, Ylva Johansson has also emphasised the urgent need for "detection, reporting and removal of child sexual abuse online is urgently needed to prevent the sharing of images and videos of the sexual abuse of children, which retraumatises the victims often years after the sexual abuse has ended."[191] The National Centre for Missing & Exploited Children (NCMEC) estimates that more than half of its CyberTipline reports could disappear with E2EE, allowing the abuse to

[183] *Ibid.*
[184] *Ibid.*
[185] *Ibid.*
[186] National Center for Missing & Exploited Children, 'End-to-End Encryption' https://www.missingkids.org/theissues/end-to-end-encryption accessed 17 May 2024.
[187] *Ibid.*
[188] *Ibid.*
[189] *Ibid.*
[190] *Ibid.*
[191] Alex Hern, 'Planned EU rules to protect children online are attack on privacy, warn critics' (The Guardian, 12 May 2022) https://www.theguardian.com/society/2022/may/12/planned-eu-rules-to-protect-children-online-are-attack-on-privacy-warn-critics accessed 23 May 2024.

go undetected.[192] E2EE without any provision for detecting CSAM is dangerous and many victims fear that this eliminates their only hope of having their images removed from the internet.[193]

An investigation in Germany illustrated the challenges posed by E2EE, where more than 30 000 suspects reportedly used encrypted group chats and messenger services to share and create abusive material, making it nearly impossible to identify perpetrators.[194] This investigation only managed to identify 72 suspects and 44 victims, demonstrating the significant hurdles in tackling child sexual abuse under current encryption protocols.[195]

There are ongoing discussions about various methods to address the challenges posed by E2EE. One approach could be to limit the use of E2EE. In their joint declaration, the European Police Chiefs emphasise the critical role of cooperation between law enforcement and the technology industry in ensuring public safety, particularly for children.[196] They expressed deep concern that E2EE threatens essential functions such as lawful access to data and the proactive detection of illegal activities, including child sexual exploitation.[197] They stressed that without these capabilities, it would be significantly harder to prevent severe crimes and ensure public safety.[198] The chiefs highlighted the general intolerance of societies for spaces beyond law enforcement's reach and urged that this standard be maintained despite technological advancements and anonymity.[199]

While some support Europol's perspective, others view it as a crucial tool for ensuring data privacy.[200] Critics like Patrick Breyer, German MEP for the Pirate Party, have voiced strong opposition, suggesting that scanning cloud storage and mandatory age verification could lead

[192] National Center for Missing & Exploited Children, 'End-to-End Encryption' https://www.missingkids.org/theissues/end-to-end-encryption accessed 17 May 2024.
[193] *Ibid.*
[194] European Commission, 2020a, p 2.
[195] *Ibid.*
[196] Europol, 'Joint Declaration of the European Police Cheifs' (published 21 April 2024) https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF accessed 17 May 2024.
[197] *Ibid.*
[198] *Ibid.*
[199] *Ibid.*
[200] Julia Tar, 'Europol's declaration against end-to-end encryption reignites debate, sparks privacy concerns' (Euractiv, updated 10 May 2024) https://www.euractiv.com/section/law-enforcement/news/europols-declaration-against-end-to-end-encryption-reignites-debate-sparks-privacy-concerns/ accessed 17 May 2024.

to mass surveillance of private messages and photos. He also called the proposals "fundamental rights terrorism against the trust, self-determination and security on the internet".[201] Additionally, the proposal does not include provisions for law enforcement to report and remove known abusive material online nor set Europe-wide measures for effective prevention, victim support, counselling and criminal investigations.[202]

Further highlighting privacy concerns, Erik Neuenschwander, Apple's director of user privacy and child safety, warned that scanning for specific content types could lead to bulk surveillance and extend to other encrypted systems.[203] Echoing his concerns, Chloé Berthélémy from the European Digital Rights (EDRi) and privacy specialist Carmela Troncoso pointed out the risks and technical challenges of selectively removing encryption.[204] Troncoso noted that weakening encryption could compromise overall societal security and potentially enable criminals to develop their secure platforms and protections.[205]

Although the proposed regulation does not require the complete deactivation of E2EE, it allows providers to use automated techniques to scan users' devices for abusive material – a compromise that some believe balances privacy concerns while also helping deter child abuse.[206]

The debate around E2EE also raises another critical question: could Europol use a 'backdoor' in E2EE systems to balance privacy with the necessity of combatting child sexual abuse? A backdoor refers to a method by which typically unauthorised parties, in this case, a law enforcement agency, can bypass encryption and access encrypted communications and data.[207] The rationale behind implementing a backdoor is to provide Europol access to encrypted information, allowing it to detect and prevent illegal activities that would otherwise remain

[201] Hern, 2022.

[202] *Ibid.*

[203] Lily Hay Newman, 'Apple's Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy' (Wired, 31 August 2023) https://www.wired.com/story/apple-csam-scanning-heat-initiative-letter/ accessed 17 May 2024; Tar 2024.

[204] Tar, 2024.

[205] *Ibid.*

[206] Hern, 2022.

[207] Yathaarth Swaroop, 'Does your organization have an Encryption Backdoor?' (Encryption Consulting, last updated 3 May 2024) https://www.encryptionconsulting.com/what-is-an-encryption-backdoor-is-it-a-boon-or-a-bane/ accessed 24 June 2024.

hidden.[208] This could be particularly crucial in cases involving child sexual abuse, terrorism and other severe crimes where timely access to information can save lives and prevent harm.[209]

However, implementing a backdoor in E2EE systems presents significant challenges and legal implications. Such an initiative would require substantial changes in legislation in various countries. In the EU, any measures introduced must align with the GDPR, the EU Charter and other existing privacy protections.[210] Specifically, Article 8(1) of the EU Charter guarantees every individual's right to personal data protection, while Article 8(2) requires that such data must be processed fairly, collected only for specified purposes and based on the individual's consent or another legal basis. Implementing a backdoor would be a breach of this right. Any measure infringing on fundamental rights must be lawful and meet the criteria of legitimacy, legality, necessity, proportionality, and consistency with democracy. Justifying a backdoor under these stringent conditions is highly challenging. Consequently, the Court of Justice of the European Union (CJEU) would examine any such laws, given their potential conflict with the fundamental right to privacy stipulated in these articles.

Even if backdoors are implemented, criminals might shift to other methods of communication, using unregulated platforms or developing their own encryption tools as mentioned before. That would diminish the effectiveness of the backdoor.

Unfortunately, the effectiveness of a backdoor protocol managed by law enforcement or government authorities highly depends on its implementation.[211] There are several documented instances where backdoors have been exploited by evil entities or even by the government bodies tasked with managing them.[212] Additionally, implementing a backdoor involves a range of legal challenges and requires stringent oversight.[213]

[208] Josh Nadeau, 'Understanding the backdoor debate in cybersecurity' (Security Intelligence, 11 May 2023) https://securityintelligence.com/articles/understanding-the-backdoor-debate-in-cybersecurity/ 24 June 2024.
[209] *Ibid.*
[210] Giovanni Sartor and Andrea Loreggia, 'The impact of Pegasus on fundamental rights and democratic processes' (European Parliament Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, January 2023) PE 740.514, p 8.
[211] Nadeau, 2023.
[212] *Ibid.*
[213] *Ibid.*

The proposed methods to tackle encrypted CSAM present significant drawbacks. Limiting the use of E2EEE introduces technical hurdles that could hamper legitimate privacy and security measures, while implementing backdoors raises serious privacy concerns, potentially violating fundamental rights. Both approaches risk undermining trust in digital communication technologies without sufficiently addressing the root problems of OCSE.

### 4.3. Dark Web

While restricting E2EE or implementing backdoors may address some issues, they could also lead to new challenges. Criminals increasingly use the dark web, where they can maintain their anonymity and are harder to trace, thus complicating enforcement efforts.[214] The dark web is a part of the internet hidden from search engines and can only be accessed through an anonymising browser known as Tor.[215] The Tor browser makes your online activity anonymous by routing your web page requests through a network of proxy servers managed by thousands of volunteers worldwide.[216] This process conceals your IP address, making it unidentifiable and untraceable.[217]

Europol monitors the dark web with a dedicated Dark Web Team that collaborates with EU partners and law enforcement globally to reduce the scope of the underground illegal economy.[218] This team is part of the EC3 and plays a crucial role in fostering a coordinated law enforcement approach aimed at tackling child sexual abuse online.[219]

Still, a pressing need remains to harmonise the monitoring of criminal activities and the lawful collection of crucial evidence from the dark web.[220] The importance of this issue is escalating

[214] Marie-Astrid Huemer, 'Revision of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography' (European Parliamentary Research Service, February 2024) PE 757.790, p 10.

[215] Darren Guccione, 'What is the dark web? How to access it and what you'll find' (CSO, published 2 April 2024) https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html accessed 27 June 2024.

[216] *Ibid.*

[217] *Ibid.*

[218] Europol, 'Crime on the dark web: law enforcement coordination is the only cure' (published 29 May 2018) https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure accessed 27 June 2024.

[219] *Ibid.*

[220] Europol and Eurojust, 'Common challenges in combating cybercrime as identified by Eurojust and Europol' (Joint report, June 2019) https://www.eurojust.europa.eu/publication/common-challenges-combating-cybercrime-identified-eurojust-and-europol accessed 27 June 2024, p 14.

due to advanced security measures adopted by criminals on the dark web, such as two-factor authentication, encrypted messaging, and multi-signature escrow, especially following high-profile operations like the takedown of Hansa, AlphaBay and PAMP in 2017.[221] The absence of a unified international legal framework for the rapid sharing of evidence means that there can be significant delays in obtaining preserved evidence for use in criminal investigations or judicial proceedings in the requesting country.[222] Practitioners commonly view the current Mutual Legal Assistance (MLA) process as too slow to collect and distribute electronic evidence efficiently.[223]

The balance between stringent data protection and effective law enforcement presents a nuanced challenge in the EU's efforts against child sexual abuse. The variability in legal frameworks and directive implementation complicates transnational collaboration. The next chapter proposes strategies that bolster cooperation while respecting privacy rights. This reflection is crucial for developing policies that protect individuals and uphold the EU's fundamental values of privacy

[221] *Ibid.*
[222] *Ibid.*, p 15.
[223] *Ibid.*, p 15.

## 5. Recommendations for Enhancing Member States' Collaboration

As discussions progress about establishing a future EU Joint Cyber Unit and potential European centre to prevent and counter child sexual abuse, Europol must ensure it remains the primary criminal intelligence hub for the EU.[224] This chapter outlines strategic recommendations for improving Europol's capacity to facilitate effective cross-border collaboration and information sharing among EU Member States. Building on the previous chapter's exploration of privacy challenges and legal fragmentation, this chapter addresses the need for strengthened legal frameworks, improved technological capabilities, and increased funding and resources. These enhancements are essential for overcoming jurisdictional and operational issues identified earlier.

### 5.1. Strengthening Legal Frameworks

As previously discussed in the chapter on the Child Sexual Abuse Directive, the primary issues with the directive are its implementation challenges and ambiguous language. Given these crimes' complex and cross-border nature, there is an urgent need for a coordinated response that surpasses the individual Member State laws and policies.

Less than a year after the European Commission introduced a new proposal to tackle child sexual abuse, a report from the Joint Research Centre (JRC) demonstrates how 14 established classification criteria and tags could facilitate an EU-wide strategy by adopting a unified taxonomy.[225] Currently, no comprehensive framework is in place to systematically catalogue the progress made by Member States in this area.[226] This absence of a structured approach limits the potential for an EU-wide prevention strategy.[227]

Establishing a universally accepted set of terms specific to child sexual abuse is proposed to mitigate ambiguities in legal and operational contexts. This taxonomy would standardise the language used in data exchange, reporting and enforcement, thus enhancing clarity and

[224] Europol, 'Europol Programming Document 2022 – 2024' (2021) https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2022-2024.pdf accessed 24 June 2024, p 6.

[225] Joint Research Centre, 'Helping Member States to apply EU rules on combatting child sexual abuse' (News Article, 3 March 2023) https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/helping-member-states-apply-eu-rules-combatting-child-sexual-abuse-2023-03-03_en accessed 25 June 2024.

[226] *Ibid.*

[227] *Ibid.*

uniformity across different jurisdictions. This is important in cross-border cases where differing national laws complicate cooperative efforts.
For instance, EU Member States generally adhere to the definition of a “child” as anyone under the age of 18.[228] This aligns with the United Nations Convention on the Rights of the Child[229], which all EU countries have ratified.[230] This uniform definition facilitates a consistent approach across the EU for the protection of minors against sexual abuse and exploitation.

However, the specific age of consent, which is the age at which a person is considered legally competent to consent to sexual acts, can vary between Member States and may influence how child sexual abuse is defined and prosecuted. The Child Sexual Abuse Directive Article 2(b) describes the ‘age of sexual consent’ as “the age below which, in accordance with national law, it is prohibited to engage in sexual activities with a child.” The age of consent typically ranges from 14 to 18 years across different EU countries.[231] This variation can affect cross-border legal issues and enforcement, requiring careful consideration in implementing protective measures and legal actions against offenders.

Unifying the legal definition of a “child” and other vague terms would facilitate a better understanding and smoother legal proceedings across borders. It would reduce complexities and conflicts in legal systems when pursuing cases that span multiple jurisdictions.

Furthermore, the Commission is dedicated to actively collaborating with Member States to prioritise and resolve all outstanding issues, ensuring thorough implementation and full compliance with the Child Sexual Abuse Directive through the EU.[232] As previously discussed, this directive is a key piece of EU legislation aimed at combatting the sexual abuse and exploitation of children.[233]

[228] European Commission, ‘Child’ https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/child_en accessed 26 June 2024.
[229] United Nations, ‘Convention on the Rights of the Child’ [1989] 1577 UNTS 3 (CRC).
[230] United Nations Human Rights Office of the High Commissioner, ‘Status of Ratification Interactive Dashboard – Convention on the Rights of the Child’ https://indicators.ohchr.org accessed 26 June 2024.
[231] European Union Agency for Fundamental Rights, ‘Consent for sexual activity with an adult’ https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/consent-sexual-activity-adult accessed 25 June 2024.
[232] European Commission, 2020a, p 3.
[233] Collovà and Lüker, 2024, p 2.

As mentioned in the Challenges Chapter, the Commission has been organising specialised workshops to assist Member States in implementing the Child Sexual Abuse Directive.[234] While the Member States continue to face challenges in transposing the directive, enhancing the efficiency of the workshops could be beneficial. Increasing their frequency would ensure the issues remain at the forefront of policy discussions. Holding these sessions regularly would provide ongoing support and enable timely adjustments to strategies as needed.

Moreover, developing an EU-wide legal framework specifically tailored for conducting online investigations on the deep and dark web could substantially enhance law enforcement efforts in these areas.[235]

Uniform and comprehensive enforcement of the Child Sexual Abuse Directive is essential. Standardising legal instruments across the EU minimises discrepancies in legal procedures among Member States. Additionally, a unified legal framework enhances the ability to prosecute offenders and prevent future cases of child sexual abuse by establishing clear, strong legal provisions across the EU.

### 5.2. Enhancing Technological Capabilities

In response to the evolving landscape of online child sexual abuse, Europol must bolster its capabilities to support Member States in their investigations better. While the Challenges Chapter previously examined two methods for addressing E2EE, it became evident that those solutions introduced additional complications. This section will explore potential strategies to enhance child sexual abuse investigations effectively.

#### 5.2.1. Europol Decryption Platform

Europol is committed to continuously monitoring emerging trends and actively supports Member States in addressing technical challenges related to their cyber and cyber-facilitated investigations.[236] This support includes identifying effective tactics, developing specialised

[234] European Commission, 2024, p 36.
[235] Europol and Eurojust, 2019, p 15.
[236] Europol, 'Europol's Programming Document 2024-2026' (2023) https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2024-2026.pdf accessed 24 June 2024, p 67-69.

tools and disseminating best practices to meet evolving operational needs.[237] Europol offers decryption services through the Europol Decryption Platform, which is crucial in decrypting data from criminal IT infrastructure and devices confiscated during criminal investigations.[238]

In both Europol's Programming Documents, 2022-2024 and 2024-2026, they pinpointed several areas within the cybercrime field that require enhancement to support better the investigations conducted by Member States.[239] These areas include the forensic capacities of the EC3 Forensics Lab for hardware analysis.[240] Amplifying the research and development efforts of the Lab in decryption and creating advanced specialised decryption solutions is expected to improve the enhanced Decryption Platform.[241]

Europol has also recognised the need to enhance its capabilities in dealing with encrypted communications and other emerging technological methods organised crime groups use to safeguard their activities and conceal related communications.[242] CSAM and other evidence related to exploitation can often be stored in encrypted formats to avoid detection by law enforcement. An efficient decryption platform enables Europol to access encrypted data, which is crucial for identifying offenders and rescuing victims. As discussed before in the challenges chapter, many perpetrators use encrypted communication channels, like WhatsApp, to share illegal content or coordinate their activities. Decryption tools allow Europol and Member States law enforcement to intercept and read these communications.

### 5.2.2. Enhanced Metadata Analysis

While the content of communications can be encrypted, metadata is not. Metadata (data about data) consists of standardised, structured and searchable information that describes a dataset or data file.[243] Metadata provides detailed information that adds context and clarity to data. It includes a title and description that briefly summarises the data's contents.[244] Additionally, tags

[237] *Ibid*.
[238] *Ibid.*, p 70.
[239] Europol, 2023b, p 67-69; Europol, 2021a, p 6.
[240] Europol, 2023b, p 70; Europol, 2021a, p 6.
[241] *Ibid.*
[242] Europol, 2023b, p 59.
[243] University of St Andrews, 'Documentation and metadata' https://www.st-andrews.ac.uk/research/support/open-research/research-data-management/working-with-data/documentation-and-metadata/ accessed 26 June 2024.
[244] Piotr Kononow, 'What is Metadata (with examples)' (Dataedo, 16 September 2018) https://dataedo.com/kb/data-glossary/what-is-metadata 26 June 2024.

and categories aid in the classification of the data, while details on the creation and modification provide insights into who originated the data and when it was last updated. [245] Access control information specifies who can view or edit the data.[246]

For files, metadata reveals the name, type, size, and timing details of creation and modification.[247] It can include camera settings and geolocation in the context of pictures. In contrast, emails encompass the subject, sender and recipient information, timing, the servers involved in sending and receiving the email, its format (plain text or HTML) and anti-spam measures.[248]

Using metadata does not require breaking encryption but it must still follow data protection laws. All Europol's data processing in support of a criminal investigation must follow Article 18a of the Europol Regulation. Europol's function is distinct because it provides the only EU-wide platform for the multilateral exchange and analysis of personal data concerning organised crime.[249]

Europol can utilise metadata analysis to detect user patterns and anomalies that might suggest criminal activity.[250] By examining metadata, investigators can reveal hidden details, establish timelines, and pinpoint individuals involved in incidents or activities.[251] This adds more depth to their analysis, enabling them to connect the information and draw conclusions.[252] Additionally, automating the collection and analysis of metadata enhances the efficiency and accuracy of these investigative processes.[253]

[245] *Ibid.*
[246] *Ibid.*
[247] *Ibid.*
[248] *Ibid.*
[249] Oldřich Bureš, 'Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol' (2016) 15(1) European view 57,p 59.
[250] Tower Forensics, 'What is Metadata Analysis?' (posted 7 June 2024) https://www.towerforensics.co.uk/latest-news/what-is-metadata-analysis/ accessed 26 June 2024.
[251] *Ibid.*
[252] *Ibid.*
[253] *Ibid.*

### 5.3. Increasing Funding and Resources

To effectively combat OCSE, it is imperative to enhance both technological capabilities and the skillsets of law enforcement personnel. This requires investment in innovative technologies and comprehensive training programmes.

#### 5.3.1. Technology Development Fund

The Technology Development Fund could be a strategic initiative aimed at bolstering the resources required to develop and implement tools designed for detecting and investigating OCSE. This fund is envisioned as an incentive for innovation, enabling Europol and Member States law enforcement agencies to leverage advanced technological solutions to enhance their operational capabilities.

At the end of 2019, Justice and Home Affairs ministers from all EU Member States tasked Europol with establishing an Innovation Lab.[254] This initiative aims to support the law enforcement community by driving advancements in innovation.[255] The Lab's goal is to identify, promote and develop innovative solutions to support the operational efforts of EU Member States.[256] These solutions will enable investigators and analysts to leverage new technologies, avoid duplication of work, create synergies and optimise resource utilisation.[257]

Europol's Innovation Lab could prioritise efforts to combat child sexual abuse by investing in the development of advanced machine learning algorithms designed to identify patterns and anomalies indicative of OCSE activities. The EU should invest in research to develop new technologies that can help detect and prevent illegal activities without breaking encryption. For instance, developing secure ways to share cryptographic hashes of illicit images or other digital footprints could allow platforms to detect and block CSAM without accessing the underlying data.[258]

[254] Europol, 'Innovation lab' (last updated 27 September 2023) https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab 27 June 2024.

[255] *Ibid.*

[256] *Ibid.*

[257] *Ibid.*

[258] Uwe Breidenbach, Martin Steinebach and Huajian Liu, 'Privacy-Enhanced Robust Image Hashing with Bloom Filters' (2021) 10(1) Journal of Cyber Security and Mobility 97, p 98.

### 5.3.2. Training and Education Programmes

Addressing the complex nature of child sexual abuse requires not only advanced technological tools but also well-trained personnel. Europol has also acknowledged the need to continue providing and supporting training courses on Victim Identification and Combatting Child Sexual Exploitation of Children.[259]

Although Europol already provides training courses for its staff and Member States' JITs, increasing the frequency and expanding the reach of these programmes are essential for maximising their effectiveness. By offering more regular and inclusive training sessions, more law enforcement personnel can be equipped with the latest skills and knowledge needed to tackle emerging threats. However, additional funding is necessary to achieve this expansion and improve the training quality. With increased financial support, Europol could maintain a highly skilled and knowledgeable workforce, thereby strengthening the security capabilities of EU Member States.

Therefore, increased funding should be allocated to training and educational programmes that equip law enforcement officials with the necessary skills to handle online child sexual abuse. These programmes should cover legal aspects, digital forensics and psychological factors involved in child sexual abuse cases.

By strengthening legal frameworks, enhancing technological capabilities, and increasing funding and resources, Europol can better support Member States in addressing the complexities of cross-border investigations. Implementing these recommendations will secure Europol's position as a central hub for intelligence sharing and law enforcement cooperation, thereby boosting the EU's ability to protect children from sexual abuse. These recommendations aim to address the gaps identified in previous analyses, such as jurisdictional challenges, privacy concerns and operational inefficiencies. Implementing these strategies will ensure a more unified and effective approach, safeguarding children across Europe and reinforcing the EU's commitment to justice and security.

[259] Europol, 2023b, p 74.

# 6. Conclusion

## 6.1. Research Outcome

This research showed how Europol facilitates information sharing and cooperation among EU Member States. Through a detailed examination of the legal frameworks and operational strategies, the study identified both strengths and areas requiring enhancements to better address the complexities of child sexual abuse in the digital era.

The primary research question for this thesis was 'How can the EU improve cooperation and information exchange between Member States through Europol to enhance the effective prosecution and prevention of child sexual abuse, considering existing data protection challenges?'. The thesis addressed the question by exploring various strategies and mechanisms through which the EU can improve cooperation and information exchange among Member States via Europol to enhance the prevention and prosecution of child sexual abuse, while also considering data protection challenges.

The thesis also answered each of its sub-questions by delving into the operations, challenges and strategic needs of Europol's role in combating such crimes. The thesis discussed legal frameworks such as the Europol Regulation and the GDPR that underpin data handling and information sharing practices. Additionally, it outlines how Europol's mechanisms and platforms facilitate real-time information sharing and operational collaboration among Member States.

Furthermore, the thesis identifies several challenges related to privacy and data protection that impact cross-border cooperation. These include difficulties with different national data protection laws and the technical challenges of E2EE and the dark web, which can prevent access to crucial data during investigations. To address these challenges, the thesis offers specific recommendations to enhance Europol's effectiveness. These include legislative amendments to streamline data protection protocols within Europol's operations without compromising the fundamental rights of privacy and data protection.

Overall, the thesis provides an analysis of Europol's current capabilities and limitations within the EU's legal and operational framework, offering practical solutions to improve its role in addressing child sexual abuse while respecting necessary data protection and privacy standards.

### 6.2. Implications and Further Research

Although Europol possesses significant capabilities, the challenges it faces in combatting child sexual abuse often surpass its direct control, pointing to inherent limitations within its current framework. A broader response from the EU is imperative to enhance Europol's effectiveness. By expanding the scope of support and resources available to Europol, the EU can ensure that the agency is not only well-equipped but also authorised to address the complex dynamics of transnational child exploitation. This holistic approach is essential for adapting to the evolving landscape of digital crime and safeguarding vulnerable children across Europe.

As mentioned in the Challenges Chapter, E2EE demonstrates a dilemma in modern digital communications and law enforcement. The encryption technology that ensures privacy for users worldwide simultaneously creates a shield for perpetrators, hindering the ability of Europol to access crucial data during investigations. This ongoing situation reflects a broader issue in the digital age – the tension between upholding individual privacy and ensuring children's safety. This duality underscores the need for a balanced approach that respects individual rights while providing law enforcement with the tools necessary to protect the most vulnerable.

Given the complexities, further research is imperative in several areas: developing advanced technologies that detect illegal activities without breaching E2EE; exploring the legal and ethical implications of encryption circumvention tools such as 'backdoors'; enhancing policy frameworks to balance privacy rights with law enforcement needs. Addressing these research areas is crucial for refining strategies that maintain the internet as a safe space without compromising fundamental privacy.

# 7. Bibliography

## 7.1. Primary Sources:

**Council of Europe**

- Council of Europe, Convention on Cybercrime ETS No. 185 (23 November 2001) https://rm.coe.int/1680081561.

**European Union**

*Charter and Treaties*

- Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
- Treaty on European Union (TEU) [2012] OJ C 326/13.
- Treaty on the Functioning of the European Union (TFEU) [2012] OJ C 326/47.

*Directives*

- European Parliament and the Council Directive 2002/58/EC of 13 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37.
- European Parliament and Council Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L 335/1.
- European Parliament and Council Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

*Regulations*

- European Parliament and Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.
- European Parliament and Council Regulation 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) [2016] OJ L 135/53.

- Europol Parliament and Council Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data [2018] OJ L 295/39.
- European Parliament and Council Regulation 2018/1862 of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters [2018] OJ L 312/7.
- European Parliament and Council Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79.
- European Parliament and Council Regulation 2021/1232 of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 274/41.
- European Parliament and Council Regulation 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1.
- European Parliament and Council Regulation 2024/1307 of 29 April 2024 on amending Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2024] OJ L series.

**United Nations**

- United Nations, ‘Convention on the Rights of the Child’ [1989] 1577 UNTS 3 (CRC).

### 7.2. Secondary Sources:

**Breidenbach, Steinebach and Liu, 2021**

- Uwe Breidenbach, Martin Steinebach and Huajian Liu, ‘Privacy-Enhanced Robust Image Hashing with Bloom Filters’ (2021) 10(1) Journal of Cyber Security and Mobility 97, p 98.

**Bureš, 2016**

- Oldřich Bureš, 'Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol' (2016) 15(1) European view 57.

**Calcara, 2013**

- Giulio Calcara, 'The Role of INTERPOL and EUROPOL in the Fight Against Cybercrime, With Particular Reference to the Sexual Exploitation of Children Online and Child Pornography' (2013) 7(1) Masaryk University Journal of Law and Technology 19.

**Collovà and Lüker, 2024**

- Claudio Collovà and Nele Lüker, 'Pre-legislative Synthesis: Combating Child Sexual Abuse' (European Parliamentary Research Service, January 2024) PE 757.611.

**Council of the European Union, 2021**

- Council of the European Union, 'Permanent Continuation of the EU Policy Cycle for Organised and Serious International Crime: EMPACT 2022+' (Council Document, ST-9921-2021-INIT, 8 March 2021) https://data.consilium.europa.eu/doc/document/ST-9921-2021-INIT/en/pdf accessed 20 June 2024.

**European Agency for Fundamental Rights**

- European Union Agency for Fundamental Rights, 'Consent for sexual activity with an adult' https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/consent-sexual-activity-adult accessed 25 June 2024.

**European Commission**

- European Commission, 'Child' https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/child_en accessed 26 June 2024.
- European Commission, 'EMPACT fighting crime together' https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/empact-fighting-crime-together_en accessed 20 June 2024.
- European Commission, 'EU Strategy for a more effective fight against child sexual abuse' https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-

abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en accessed 24 February 2024.

- European Commission, 'Schengen Information System' https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en accessed 17 June 2024.
- European Commission, 'What is SIS and how does it work?' https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en accessed 17 June 2024.

**European Commission, 2020a**

- European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU strategy for a more effective fight against child sexual abuse' COM(2020) 607 final (24 July 2020).

**European Commission, 2020b**

- European Commission, 'Proposal for a Regulation of the European Parliament and the Council Amending Regulation (EU) 2016/794' COM(2020) 796 final 2020/0349(COD) (9 December 2020).

**European Commission, 2023**

- European Commission, 'EU Schengen Information System saves lives' (News article, 19 September 2023) https://home-affairs.ec.europa.eu/news/eu-schengen-information-system-saves-lives-2023-09-19_en accessed 17 June 2024.

**European Commission, 2024**

- European Commission, 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast)' (COM(2024) 60 final, 2024/0035(COD) (6 February 2024).

**Europol**

- Europol, 'About Europol' https://www.europol.europa.eu/about-europol accessed 6 May 2024.
- Europol, 'Child Sexual Exploitation' https://www.europol.europa.eu/crime-areas/child-sexual-exploitation accessed 13 May 2024.
- Europol, 'EU Policy Cycle – EMPACT' https://www.europol.europa.eu/crime-areas-and-statistics/empact accessed 19 June 2024.
- Europol, 'Europol Cybercrime Centre (EC3)' https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 accessed 8 May 2024.
- Europol, 'Stop Child Abuse – Trace an Object' https://www.europol.europa.eu/stopchildabuse accessed 17 June 2024.

**Europol, 2018a**

- Europol, 'Crime on the dark web: law enforcement coordination is the only cure' (published 29 May 2018) https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure accessed 27 June 2024.

**Europol, 2018b**

- Europol, 'Europol Strategy 2020+' (13 December 2018) https://www.europol.europa.eu/sites/default/files/documents/europol_strategy_2020.pdf accessed 21 June 2024.

**Europol, 2021a**

- Europol, 'Europol Programming Document 2022 – 2024' (2021) https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2022-2024.pdf accessed 24 June 2024.

**Europol, 2021b**

- Europol, 'Member States' (last updated 9 December 2021) https://www.europol.europa.eu/partners-collaboration/member-states accessed 13 May 2024.

**Europol, 2022a**

- Europol, ‘Europol’s amended Regulation enters into force’ (published 28 June 2022) https://www.europol.europa.eu/media-press/newsroom/news/europols-amended-regulation-enters-force accessed 7 May 2024.

**Europol, 2022b**

- Europol, ‘Secure Information Exchange Network Application (SIENA)’ (last updated 10 June 2022) https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena accessed 24 May 2024.

**Europol, 2023a**

- Europol, ‘Europol Analysis Projects’ (last updated 24 April 2023) https://www.europol.europa.eu/operations-services-innovation/europol-analysis-projects accessed 9 May 2024.

**Europol, 2023b**

- Europol, ‘Europol’s Programming Document 2024-2026’ (2023) https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2024-2026.pdf accessed 24 June 2024.

**Europol, 2023c**

- Europol, ‘Innovation lab’ (last updated 27 September 2023) https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab 27 June 2024.

**Europol, 2023d**

- Europol, ‘Six sexually-abused children rescued as a result of Europol Victim Identification Taskforce’ (published 26 May 2023) https://www.europol.europa.eu/media-press/newsroom/news/six-sexually-abused-children-rescued-result-of-europol-victim-identification-taskforce accessed 20 June 2024.

**Europol, 2024a**

- Europol, '57 men arrested for possessing and sharing over 100 000 depictions of child sexual abuse' (published 8 March 2024) https://www.europol.europa.eu/media-press/newsroom/news/57-men-arrested-for-possessing-and-sharing-over-100-000-depictions-of-child-sexual-abuse accessed 31 May 2024.

**Europol, 2024b**

- Europol, 'Partners & Collaboration' (last updated 14 February 2024) https://www.europol.europa.eu/partners-collaboration accessed 13 May 2024.

**Europol, 2024c**

- Europol, 'Right of access' (last updated 27 March 2024) https://www.europol.europa.eu/right-of-access accessed 14 May 2024.

**Europol and Eurojust, 2019**

- Europol and Eurojust, 'Common challenges in combating cybercrime as identified by Eurojust and Europol' (Joint report, 1 June 2019) https://www.eurojust.europa.eu/publication/common-challenges-combating-cybercrime-identified-eurojust-and-europol accessed 27 June 2024.

**Guccione, 2024**

- Darren Guccione, 'What is the dark web? How to access it and what you'll find' (CSO, published 2 April 2024) https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html accessed 27 June 2024.

**Hern, 2022**

- Alex Hern, 'Planned EU rules to protect children online are attack on privacy, warn critics' (The Guardian, 12 May 2022) https://www.theguardian.com/society/2022/may/12/planned-eu-rules-to-protect-children-online-are-attack-on-privacy-warn-critics accessed 23 May 2024.

**Howe, 2006**

- Jeff Howe, 'The Rise of Crowdsourcing' (Wired, 1 June 2006) https://www.wired.com/2006/06/crowds/ accessed 17 June 2024.

**Huemer, 2024**

- Marie-Astrid Huemer, 'Revision of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography' (European Parliamentary Research Service, February 2024) PE 757.790.

**Ilbiz and Kaunert, 2023**

- Ethem Ilbiz and Christian Kaunert, 'Crowdsourcing to Tackle Online Child Sexual Exploitation: Europol's 'Stop Child Abuse – Trace an Object' Platform' (2023) Policing: A Journal of Policy and Practice https://academic.oup.com/policing/article/doi/10.1093/police/paad009/7084824 accessed 17 June 2024.

**Internet Watch Foundation, 2021**

- Internet Watch Foundation, *Face the Facts: Internet Watch Foundation Annual Report 2020* (2021) https://www.iwf.org.uk/about-us/who-we-are/annual-report-2020/ accessed 24 February 2024.

**Joint Research Centre, 2023**

- Joint Research Centre, 'Helping Member States to apply EU rules on combatting child sexual abuse' (News Article, 3 March 2023) https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/helping-member-states-apply-eu-rules-combatting-child-sexual-abuse-2023-03-03_en accessed 25 June 2024.

**Kononow, 2018**

- Piotr Kononow, 'What is Metadata (with examples)' (Dataedo, 16 September 2018) https://dataedo.com/kb/data-glossary/what-is-metadata 26 June 2024.

**Maciejewski, 2023**

- Mariusz Maciejewski, 'Personal data protection' (Fact Sheets on the European Union, November 2023) https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection accessed 2 June 2024

**McKee, 2023**

- Adam J. McKee, ‘European Police Office’ (Doc McKee, last modified 19 May 2023) https://docmckee.com/cj/docs-criminal-justice-glossary/european-police-office-definition/ accessed 6 May 2024.

**Missing Children Europe, ECPAT and eNACSO, 2016**

- Missing Children Europe, ECPAT and eNACSO, ‘A Survey on the Transposition of Directive 2011/93/EU on Combatting Sexual Abuse and Sexual Exploitation of Children and Child Pornography’ (2016) http://www.enacso.eu/news/survey-on-the-transposition-of-directive-201193eu-on-combating-sexual-abuse-and-sexual-exploitation-of-children-and-child-pornography/ accessed 22 June 2024.

**Mladenović, 2015**

- Slađana Mladenović, ‘Strategic Response of EU Institutions on Cybercrime in the post-Lisbon Period’(International Scientific Conference “Archibald Reiss Days”, Belgrade, 3-4 March 2015) https://www.researchgate.net/publication/380630893_Strategic_Response_of_EU_Institutions_on_Cybercrime_in_the_post-Lisbon_Period accessed 20 June 2024, p 237.

**Nadeau, 2023**

- Josh Nadeau, ‘Understanding the backdoor debate in cybersecurity’ (Security Intelligence, 11 May 2023) https://securityintelligence.com/articles/understanding-the-backdoor-debate-in-cybersecurity/ 24 June 2024.

**National Center for Missing & Exploited Children**

- National Center for Missing & Exploited Children, ‘End-to-End Encryption’ https://www.missingkids.org/theissues/end-to-end-encryption accessed 17 May 2024.

**Negreiro, 2023**

- Mar Negreiro, ‘Combating child sexual abuse online’ (European Parliamentary Research Service, June 2023) PE 738.224.

**Newman, 2023**

- Lily Hay Newman, ‘Apple’s Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy’ (Wired, 31 August 2023) https://www.wired.com/story/apple-csam-scanning-heat-initiative-letter/ accessed 17 May 2024.

**Sartor and Loreggia, 2023**

- Giovanni Sartor and Andrea Loreggia, ‘The impact of Pegasus on fundamental rights and democratic processes’ (European Parliament Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies, January 2023) PE 740.514.

**Swaroop, 2024**

- Yathaarth Swaroop, ‘Does your organization have an Encryption Backdoor?’ (Encryption Consulting, last updated 3 May 2024) https://www.encryptionconsulting.com/what-is-an-encryption-backdoor-is-it-a-boon-or-a-bane/ accessed 24 June 2024.

**Tar, 2024**

- Julia Tar, ‘Europol’s declaration against end-to-end encryption reignites debate, sparks privacy concerns’ (Euractiv, updated 10 May 2024) https://www.euractiv.com/section/law-enforcement/news/europols-declaration-against-end-to-end-encryption-reignites-debate-sparks-privacy-concerns/ accessed 17 May 2024.

**Tolbaru, 2022**

- Carmina-Elena Tolbaru, ‘Fight Against Sexual Abuse and Online Exploitation of Children – Key Priority at the European Union Level’ (2022) 1 International Journal of Legal and Social Order 347.

**Tower Forensics, 2024**

- Tower Forensics, ‘What is Metadata Analysis?’ (posted 7 June 2024) https://www.towerforensics.co.uk/latest-news/what-is-metadata-analysis/ accessed 26 June 2024.

**UNICEF**

- UNICEF, ‘Protecting Children Online’ (UNICEF, last updated 23 June 2022) https://www.unicef.org/protection/violence-against-children-online accessed 24 February 2024.

**UNICEF, 2021**

- United Nations Children’s Fund (UNICEF), ‘Ending Online Child Sexual Exploitation and Abuse: Lessons Learned and Promising Practices in Low- and Middle-Income Countries’ (UNICEF, December 2021).

**United Nations Human Rights Office of the High Commissioner**

- United Nations Human Rights Office of the High Commissioner, ‘Status of Ratification Interactive Dashboard – Convention on the Rights of the Child’ https://indicators.ohchr.org accessed 26 June 2024.

**University of St Andrews**

- University of St Andrews, ‘Documentation and metadata’ https://www.st-andrews.ac.uk/research/support/open-research/research-data-management/working-with-data/documentation-and-metadata/ accessed 26 June 2024.

**Van Ballegooij, 2021**

- Wouter van Ballegooij, ‘Revision of the Europol Regulation’ (European Parliamentary Research Service, January 2021) PE 654.214.