COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse

Independent experts' report

Directorate General of Human Rights and Rule of Law - DG I
and Directorate General of Democracy - DG II

June 2021

This report has been prepared by the following independent experts:

Liora Lazarus, Jean-Christophe Le Toquin, Manuel Magriço Aires, Francisco Nunes, Katarzyna Staciwa (acting also as support to the lead expert), Gert Vermeulen and Ian Walden, led by Linos-Alexandre Sicilianos, the former President of the European Court of Human Rights and assisted by the Council of Europe Secretariat.

The opinions expressed in this report are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe.

Table of contents

EXECUTIVE SUMMARY 5

1. INTRODUCTION 7

1.1 Aim of the document 7

1.2 Methodology 9

1.3 Describing the phenomenon 10

2. TECHNICAL OVERVIEW 11

2.1 The three main families of automated detection tools of online child sexual exploitation and abuse 11

2.1.1 File Hashing 12

2.1.2 Computer Vision 12

2.1.3 Artificial Intelligence 14

2.1.4 Implications for this report 15

2.2 Practical examples of the use of automated technology to detect online child sexual exploitation and abuse 16

2.2.1 Content oriented activities 17

2.2.2 Behaviour oriented activities 23

2.2.1 Implications for this report 24

3. LEGAL FRAMEWORK 25

3.1 e-Privacy Directive and the European Electronic Communications Code 25

3.1.1 European Data Protection Supervisor Opinion 26

3.1.2 Report of Committee on Civil Liberties, Justice and Home Affairs Report 27

3.1.3 European Economic and Social Committee Opinion 28

3.1.4 Implications for this report 29

3.2 Service providers conduct 30

3.2.1 The notion of a '*service provider*' 30

3.2.2 Legal framework 30

3.2.3 Proposal for an EU Regulation on the detection, removal and reporting of child sexual abuse online 32

3.2.4 Implications for this report 33

3.3 Positive obligations under International and European Human Rights Law regarding the protection of children from online sexual exploitation and sexual abuse 34

3.3.1 Children's rights and positive obligations under international and European human rights treaty law 34

3.3.2 Jurisprudence on the protection of children from online sexual exploitation and sexual abuse 40

3.3.3 Implications for this report 46
3.4 Data protection conditions and safeguards 47
3.4.1 Relevant ECtHR jurisprudence on Art. 8 ECHR 48
3.4.2 Global Data Protection of the Council of Europe 48
3.4.3 Conditions and safeguards 52
3.4.4 Implications for this report 57
4. KEY CONCLUSIONS AND RECOMMENDATIONS 58
5. GLOSSARY 60
6. ANNEX 62

EXECUTIVE SUMMARY

The scale of online child sexual exploitation and abuse is increasing at an alarming rate. According to the Internet Organised Crime Threat Assessment (Europol, 2020), detection of online child sexual abuse materials (CSAM) was already increasing on a year-to-year basis, but saw a sharp spike during the peak of the COVID-19 crisis.

As an example, in 2020, reports made to the US hotline, CyberTipline included 33.6 million images, of which 10.4 million were unique, and 31.6 million videos, of which 3.7 million were unique. In 2020, the CyberTipline received 21.7 million reports, an increase of 28% from 2019. As reported by INHOPE, 60% of all URLs assessed by INHOPE hotlines in 2020 came from previously assessed material, which means that the same content is spreading and is being repeatedly reported. In the meanwhile, children are revictimized by the continued circulation of the images of their abuse.

This most worrying trend calls for innovative countering techniques. To date, the response to this challenge consists largely of voluntary actions involving the use of automated detection technologies by private sector actors in order to detect, report and remove child sexual abuse material as well as text-based threats, such as grooming.

In order to automatically detect content and/or behaviours, three main families of technologies are applicable: the most elementary is File Hashing, the intermediate category is Computer Vision and the most innovative is Artificial Intelligence, including its most advanced type Deep Learning.

While this is vital to find ways to identify and help rescue child victims, investigate crimes and stop circulation of CSAM, the use of automated technology may impact on the confidentiality of communications' content and related traffic data, which service providers must ensure. It therefore may constitute an interference with the right to private and family life and protection of personal data of those involved.

In September 2020, the European Commission proposed a temporary derogation to provisions in the e-Privacy Directive to allow for the processing of personal and other data for the purpose of combating online child sexual exploitation and abuse (OCSEA). The debate generated by this proposal illustrates well the complexity of the issues at stake.

States have a positive obligation to protect children from sexual abuse and exploitation. To do so, they must however harness a complex and evolving environment both from the technological and legal points of view. In December 2020, the States Parties to the Lanzarote Convention on the protection of children against sexual exploitation and sexual abuse, asked the Council of Europe to bring together the Organisation's expertise to support them in exploring appropriate solutions to reconcile the various human rights at stake while integrating safeguards in actions carried out in the public interest.

This report represents a first step in the Secretary General of the Council of Europe's response to the Lanzarote Committee's call.

The report is based on the individual submissions and the collective effort of a group of independent experts in the fields of human rights, child protection, data protection and the fight against cybercrime. The group was led by Linos-Alexandre Sicilianos, the former President of the European Court of Human Rights and assisted by the Council of Europe Secretariat.

While recognising the benefits a mandatory regime could bring, this report focuses on the practice of voluntary detection and voluntary reporting of OCSEA by service providers mainly based on grounds of public interest as described by existing applicable legal frameworks. As a consequence of this approach, the choice of technological solutions analysed in this document was limited to this context.

After referring to the sheer volume of child abuse content online and the added value of automatically detecting it, the experts describe the technology used, its limitations and potential. Identifying the least restrictive means of detecting OCSEA while effectively protecting its victims remains a critical challenge. Responding to this challenge requires understanding very precisely the objective and the environment for which a particular technology will be selected. To guide the choice, the experts propose to take into account the complexity of the objective, the environment and the technology as well as the maturity of the technology (a well-tested, well-documented and stable technology is a safer choice for the policymakers as it is more challenging to define the appropriate level of safeguards in the case of technology in its early phase of development).

The experts also outline the applicable legal framework describing the relevant key international standards (at global, Council of Europe and EU levels). Of particular importance are:

- the UN Convention on the Rights of the Child and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography;
- the Council of Europe Convention on Human Rights, the European Social Charter and the Conventions on the protection of children against sexual exploitation and abuse, on Cybercrime and on Data protection (also known as Convention 108+);
- the EU Directive 2002/58/EC of the European Parliament and of the Council (e-Privacy Directive) and the European Electronic Communications Code.

The relevance of the European jurisprudence is also highlighted through the analysis of the caselaw of the European Court of Human Rights and the European Union Court of Justice.

The report contains nine recommendations covering issues such as the need to match the pace of technological evolution, to increase transparency and accountability, to coordinate efforts and reinforce the dialogue between the private sector and policy makers/regulators, to embed safeguards at early stages of the development of technology, to give due weight to the positive obligation to protect children from sexual violence and to define a legal framework that provides legal certainty to service providers and addresses future technological developments. The experts also call for the establishment of a public interest-based framework grounded in the Lanzarote Convention, enabling service providers to automatically detect, remove, report and transfer online sexual exploitation and abuse content under the data protection and privacy conditions and safeguards described in the report.

The report is a “must read” for anyone active and interested in the protection of children against sexual violence. The experts put special care in making the content accessible to most readers, despite the complexity of the issue.

The report is also expected to serve as a contribution to the consultation launched by the European Commission in December 2020 regarding a Proposal for Regulation of the European Parliament and the Council on detecting, removing, and reporting child sexual abuse online.

1. INTRODUCTION

1.1 Aim of the document

The scale of online child sexual exploitation and abuse (OCSEA), both in absolute terms and in terms of reports to law enforcement and civil society, is increasing at an alarming rate,[1] calling for new and innovative countering techniques. This call is even stronger in light of the recently published flagship strategic product by Europol,[2] the Internet Organised Crime Threat Assessment (IOCTA) 2020,[3] which points out that although the main threats related to OCSEA remained relatively stable over recent years, the COVID-19 pandemic has shifted this assessment. According to the IOCTA's findings, detection of online child sexual abuse materials (CSAM) was already increasing on a year-to-year basis, but saw a sharp spike during the peak of crisis, reflecting the surge in the exchange of online child abuse materials that occurred during the contact and travel restrictions. It is also expected that developments around the pandemic and related lockdowns and travel restrictions will give rise to an increased number of reports of OCSEA, as abuse that occurred during the COVID-19 pandemic may be reported to law enforcement authorities after the fact. Similarly, a sharp increase in the amount of self-produced indecent material is expected, which is likely to lead to a corresponding increase in online solicitation and exploitation.[4]

To date, the existing response to the challenges posed by OCSEA consists largely of voluntary actions involving the use of automated detection technologies[5] by private sector actors in order to detect, report and remove CSAM as well as text-based threats, such as grooming. One exception to this situation exists in the U.S., where U.S. federal law requires U.S.-based service providers[6] to report instances of apparent '*child pornography*'[7] that they become aware of on their systems to the National Center for Missing & Exploited Children's (NCMEC) CyberTipline[8]. These reports are then shared by

[1] WePROTECT Global Alliance, Global Threat Assessment 2019, *'Working together to end the sexual exploitation of children online'*, p. 2, (available at: https://www.end-violence.org/sites/default/files/paragraphs/download/Global%20Threat%20Assessment%202019.pdf).

[2] The European Union Agency for Law Enforcement Cooperation, better known under the name Europol, formerly the European Police Office and Europol Drugs Unit, is the law enforcement agency of the European Union (EU) formed in 1998 to handle criminal intelligence and combat serious international organised crime and terrorism through cooperation between competent authorities of EU Member States. Based in The Hague.

[3] IOCTA 2020, p. 35, *(available at:* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020).

[4] Ibid, p.41.

[5] See section 2, '*Technical overview*'.

[6] A service 'provider' means "an electronic communication service provider or remote computing service" (18 USC § 2258E(6).

[7] United States federal law defines '*child pornography*' as '*any visual depiction of sexually explicit conduct involving a minor (a person less than 18 years old)*'. Outside of the legal system, NCMEC chooses to refer to these images as Child Sexual Abuse Material (CSAM) to most accurately reflect what is depicted – the sexual abuse and exploitation of children. More information is available at: https://www.missingkids.org/theissues/csam

[8] Run by the National Center for Missing & Exploited Children. The US based National Center for Missing & Exploited Children (NCMEC) is a private, non-profit corporation whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation. See section 2.2.1, *'*Specific role of National Center for Missing & Exploited Children (NCMEC, US)*'.*

NCMEC with law enforcement agencies around the world[9], and constitute a significant portion of cases to be further investigated.

While private sector actors reports are vital to help identify child victims and rescue them from ongoing abuse as well as to stop circulation of CSAM, the current state of affairs has resulted in two related problems. First, there is a significant discrepancy between the use of automated detection technologies and the publicly available level of information on their adoption. This asymmetry of information makes it difficult for policymakers and regulators to develop a coherent approach towards regulating these technologies and ensuring adequate safeguards. Second, the legal framework governing the conduct of SPs can appear unsatisfactory, with a reliance on service providers (SPs) to voluntarily implement technologies to detect OCSEA and even mandatory regimes, such as in the US, do not require them to go looking proactively for OCSEA. In terms of reporting, most countries rely on the voluntary pushing of reports to law enforcement, since the volumes involved effectively preclude mandatory requests from law enforcement. As a consequence, the current absence of a bespoke public interest-based framework, enabling the private sector actors to engage in practices aimed at efficiently responding to the challenges posed by the OCSEA results in a lack of legal certainty for their work and often fragments and duplicates efforts to combat OCSEA.

The aim of this document is therefore to provide guidance to the Council of Europe[10] (CoE) Member States (MS) in ensuring respect for human rights and the rule of law when using automated technology to detect OCSEA. The need for such guidance was expressed during the 30th meeting of the Lanzarote Committee[11] (LCt) and the LCt Secretariat was asked to check the feasibility of a CoE comprehensive human rights-based opinion addressing the above dimensions.[12] It is also expected that providing this guidance will serve as a contribution to the European Commission's (EC) work towards a proposal for a long term solution in summer 2021[13].

Part of the background to this guidance was the discussion within the European Union about a temporary derogation[14] from Articles 5(1) and 6 of the Directive 2002/58/EC (e-Privacy Directive),[15] as regards to the voluntary use of technologies by number-independent interpersonal communications services (NI-ICS), such as voice over Internet Protocol (IP), messaging and web-based e-mail services, for the processing of personal and other data for the purpose of combating child sexual abuse online.

While recognising the benefits a mandatory regime could bring in terms of legal clarity and certainty, inclusive democratic processes and widespread recognition and support, this report focuses on the practice of voluntary detection and voluntary reporting of OCSEA by SPs mainly based on grounds of

[9] Reports 2019 & 2020 by country can be accessed on https://www.missingkids.org/gethelpnow/cybertipline.
[10] https://www.coe.int/en/web/portal/home
[11] https://www.coe.int/en/web/children/lanzarote-committee
[12] List of decisions adopted by the Lanzarote Committee on 10 December 2020, (available at: https://rm.coe.int/list-of-decisions-30th-meeting-lanzarote-committee/1680a0b1eb).
[13] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0568
[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, (Directive on privacy and electronic communications). Official Journal of the European Union, L 201, 31/07/2002 P. 0037–0047, (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN).

public interest as described by existing applicable legal frameworks. As a consequence of this approach, the choice of technological solutions analysed in this document was also limited to this context.

Given the context, it is also important to recall that the terminology used in CoE and European Union (EU) instruments do not always align. In particular, for the purposes of this document, it should be noted that the relevant provisions of the e-Privacy Directive refer to providers of '*electronic communication services*', which is a narrower concept than that of a '*service provider*' used in the Budapest Convention (BC)[16].[17] Likewise, while notions of privacy and data protection are inextricably linked under the European Convention on Human Rights (ECHR),[18] the Charter of Fundamental Rights distinguishes between them as rights. This distinction is then reflected in the fact that the e-Privacy Directive is based on the right to privacy, while the General Data Protection Regulation (GDPR)[19] is grounded in the right to data protection. These distinctions need to be borne in mind when reading this document.

As a final note, it needs to be highlighted that the issue of the extra-territorial scope of positive obligations in relation to combating OCSEA is not comprehensively covered in this document as it is an area of analysis which merits a separate opinion.

1.2 Methodology

The information presented in this document is based on a combination of individual submissions by a group of independent experts invited to this task by the CoE Secretariat: Liora Lazarus, Jean-Christophe Le Toquin, Manuel Aires Magriço, Francisco Nunes, Katarzyna Staciwa (acting also as a support to the lead expert), Gert Vermeulen and Ian Walden, led by Linos-Alexandre Sicilianos, the former President of the European Court of Human Rights. Where appropriate, their respective submissions have been supplemented with public material available at the time of writing such as information, originating from other specialised sources, private sector companies, organisations and institutions.

The document is divided in two parts: the first part focuses on a technical overview and contains an explanation on the current role of automated technology to successfully tackle OCSEA, a simplified analysis of the relevant technological solutions as well as examples of its practical application. In its second part, the document provides an overview of the relevant legal framework: it describes the debate around the EC proposal on a temporary derogation from certain provisions of the e-Privacy Directive, explains the notion and conduct of a '*service provider*' as well as acquainting readers with the proposals of regulations on relevant SPs announced in the public consultation process by the EC. It then focuses on specific positive obligations in relation to OCSEA, in particular the relevant obligations developed under the European Court of Human Rights[20] (ECtHR) as well as the treaty obligations stemming from the CoE Conventions: on the protection of children against sexual

[16] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[17] See section 3.2.1, *The notion of a 'service provider'*.
[18] https://www.echr.coe.int/documents/convention_eng.pdf
[19] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[20] https://www.echr.coe.int/Pages/home.aspx?p=home

exploitation and abuse (also known as the Lanzarote Convention, (LC)),[21] on Cybercrime (also known as the Budapest Convention, (BC) and on Data protection[22] (also known as Convention 108+).

1.3 Describing the phenomenon

The phenomenon of child sexual exploitation and abuse (CSEA) is constantly evolving. Currently there are more than twice as many types of CSEA in comparison to the late 1990's. At that time, materials such as digital copies of older commercial images depicting child victims and evidence of familial production started entering into online circulation as well as some commercial videos which were produced and marketed.

The adoption of information and communication technologies (ICTs) in our daily lives has inseparably linked the offline and online environments in which children may be exposed to many of the same risks, such as being persuaded to engage in sexually explicit conduct (whether real or simulated), being recruited or coerced to participate in pornographic performances, or caused to witness sexual abuse or sexual activities. Many children are victims of sexual exploitation and abuse in multiple ways: they are victims of the offenders carrying out the physical sexual abuse against them, and simultaneously of the offenders who produce, distribute, demand, order, sell or buy, exchange, download, or stream content on child sexual exploitation and abuse, or through any other ICTs which assist in, and contribute to, the sexual exploitation and sexual abuse of those children.[23] Carefully evidenced research shows clearly, that sexual offences against children, including those facilitated through the use of ICTs, have a long-lasting harmful impact on victims. This is especially the case when materials such as images and videos depicting the victim are in circulation long after the physical sexual abuse has been committed.

Children are revictimized by the continued circulation of the images of their abuse. Technology that is used to identify these images, is consequently essential to their protection. As law enforcement authorities worldwide are confronted with an overwhelming amount of online CSAM, implementing technological solutions to combat this phenomenon effectively are essential to an adequate response to the challenge, especially to the swift prioritisation of their cases.

Successful prevention and combating of OCSEA require keeping up to date and reacting to constant developments in this area, facilitated especially by the prevalent use of constantly evolving ICTs. One of the pillars of such an approach, that is critical to the successful protection of children against OCSEA in today's world, is adopting technological solutions to this field, that could – depending on its choice – either support or, while still including human involvement, to some extent replace the human factor in particular areas. However, this choice should be made with appropriate respect to children's fundamental rights such as the right to privacy or freedom of expression.

[21] https://www.coe.int/en/web/children/lanzarote-convention
[22] https://www.coe.int/en/web/data-protection
[23] Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs), adopted by the Lanzarote Committee on 12 May 2017, p. 5, (available at: https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f).

2. TECHNICAL OVERVIEW

2.1 The three main families of automated detection tools of online child sexual exploitation and abuse[24]

A simplified technical overview of the main automated technologies which can be used to detect OCSEA is provided in this section. In order to automatically detect content and/or behaviours, three main families of technologies are applicable: the most elementary is File Hashing (FH), the intermediate category is Computer Vision (CV) and the most innovative is Artificial Intelligence (AI), including Deep Learning (DL), which is the most advanced type of artificial intelligence and can potentially cope with the most complex scenarios.

The table presented below provides an overview of the three main families of automated detection of content and/or behaviours and explains their complexity.

Target	**File ----> Image ----> Specific content in the image -----> Behaviors -----> People**				
(Un)known	**Known content ----------> New content or behaviour**				
Maturity	**Mature technology ----------> Technology in research phase**				
Quality	**Homogenous data from trusted sources ----------> Heterogeneous data**				
Technologies	**File Hashing**	**Computer Vision (images and videos)**		**Artificial Intelligence (Behaviors & Persons)**	
Types		**Global descriptors**	**Local descriptors**	**Machine Learning**	**Deep Learning**

Simple *Complex*

Key questions around the choice of technology are determined by a precise understanding of the objectives and the environment for which the chosen technology is used. These are:

- *target related factor* - what needs to be detected: a file, the content or a person? For example, identifying a known file described as 'csam1.jpg' is trivial compared to identifying a person with facial recognition;
- *(un)known related factor* - what needs to be detected: the known or unknown content and/or behaviour? The most difficult task is not to look for known content, it is to detect previously unseen content and/or behaviours: distribution of CSAM that was never seen before or instances of an adult grooming a child. For example, a hosting or social network provider can decide to detect CSAM reactively upon receiving a notification, or it can act

[24] The additional graphic overview on technologies to detect visual content in images and videos is attached to this document in Annex.

proactively by analysing all content uploaded to its servers. The detection technology in both cases remains the same;

- *maturity factor* - is detection technology mature or in a research phase? A mature technology can be defined as stable, well documented and tested over the years; it is easier to understand and regulate, and its outcomes will be far more predictable;
- *quality factor* - how reliable is the reference database? Automated detection technology often relies on an initial set of data: the more reliable the reference database is, the better understanding of its efficiency is achieved.

2.1.1 File Hashing

A file hashing is based on a mathematical algorithm where one file is reduced to one signature, i.e. 3CBCFDDEC145E3382D592266BE193E5BE53443138EE6AB6CA09FF20DF609E268.[25] This technology helps to detect an identical file and is able to query large datasets of signatures with limited computing resources. A limitation of this technology is that it is not robust to modifications: the modification of one bit or one pixel will result in a different signature, and there is no way to understand if the two files are similar or not. It is sometimes claimed that this type of file hashing does not generate false positives, meaning that two different images cannot have the same signature. If this is true, this would be beneficial in investigations and court cases, mainly when the evidence relies only on hashes without a human review. However, a research shows a minimal possibility that two different files result in one single image, what is called a '*collision vulnerability*'.[26]

Most frequent algorithms are MD5 and SHA-1 adopted by many law enforcement agencies, companies and some hotlines, such as CyberTipline (the U.S.), Internet Watch Foundation (IWF) (UK)[27], Expertisebureau Online Kindermisbruik (EOKM) (NL)[28] and Point de Contact[29] (FR).

2.1.2 Computer Vision

Two exemplary techniques are examined in this category: global descriptors and local descriptors.

Global descriptors

Global descriptor technology is based on the process in which the image is turned into a grid and then, each square of the grid is translated into a signature. It compares identical images and can also detect the same images slightly cropped (up to 20%). This technology does not, however, recognise images significantly modified: rotated, flipped, stretched, zoomed, cropped by 20%, inserted in another picture or a video, etc. The most frequent algorithms are: PhotoDNA (Microsoft),[30] pHash (open

[25] https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.1
[26] https://en.wikipedia.org/wiki/MD5#Collision_vulnerabilities and https://en.wikipedia.org/wiki/SHA-1
[27] https://www.iwf.org.uk/
[28] https://www.eokm.nl/
[29] https://www.pointdecontact.net/
[30] https://www.youtube.com/watch?v=NORlSXfcWlo

source)[31] and TMK PDQF (Facebook).[32] PhotoDNA is used by some hotlines, such as CyberTipline, Cybertip, IWF as well as EOKM and its partners.

Local descriptors

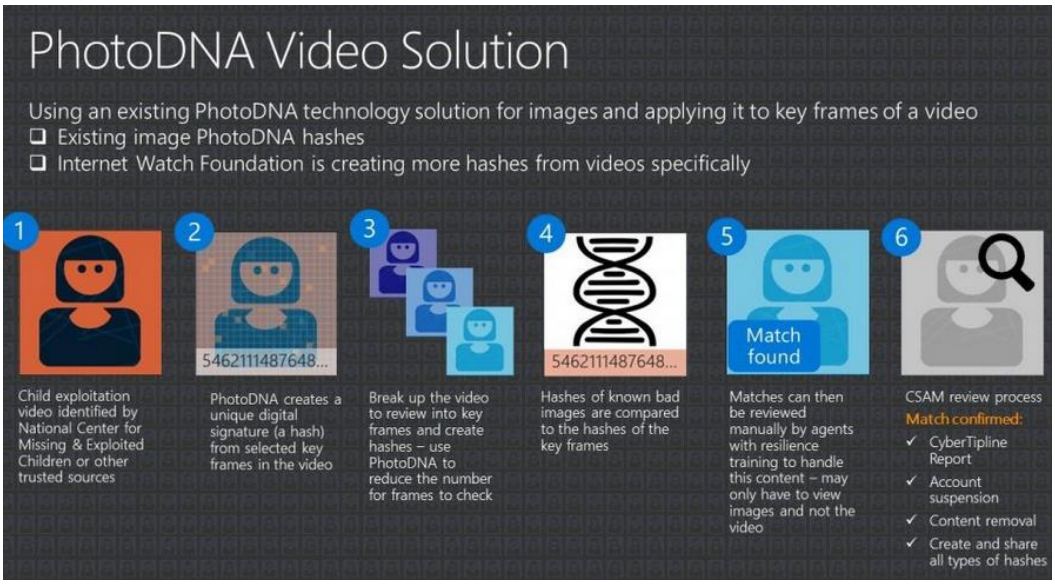
This technology measures the number of shared details between 2 images or videos, identifying strongly similar details. It recognises images even significantly modified: rotated, flipped, stretched, zoomed, cropped by 20% or more, inserted in another picture or video. It is also possible to search for an exact or partial match. As an option, it is possible to recognise content in the image or video: same building, same room, same object, same image inserted in another image or video. What can be considered as its limitation is that it is based on a very rich algorithm that can be complex to process at scale. The most frequent algorithm is SIFT (public domain) processed by Videntifier[33] technology (patented). Among those who use this technology are: INTERPOL,[34] Facebook (for copyright) and some hotlines, such as CyberTipline (for videos) or Point de Contact.

Identifying videos

The above-described principles (FH, CV using global descriptors and CV using local descriptors) apply to identifying videos, however, the main difference between identifying images and videos is that the latter technological approach is hugely demanding on computing resources. If the algorithm and the database system are not designed for maximum efficiency, the detection technology may work at a small scale but will not work in case of large volumes.

The flow chart presented below explains the PhotoDNA video solution by Microsoft based on global descriptors.[35]

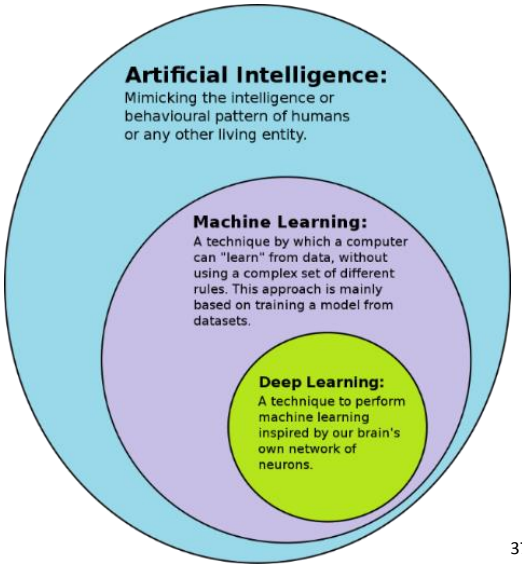
[31] https://www.phash.org/
[32] https://about.fb.com/news/2019/08/open-source-photo-video-matching/
[33] http://www.videntifier.com/
[34] The International Criminal Police Organization (INTERPOL). Run by the Secretary General, it is staffed by both police and civilians and comprises a headquarters in Lyon, a global complex for innovation in Singapore and several satellite offices in different regions.
[35] https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/



2.1.3 Artificial Intelligence

The third and to date the least used technology, which is at the same time the most promising in the fight against OCSEA, is AI. This technology was developed in the 1950s and since then evolved in the 1980s with Machine Learning, where algorithms can be '*trained*' from the data sets. Since the 2010s it has involved another subset which is Deep Learning.[36]

The picture presented below provides a simplified overview of the three families of AI.



[37]

As AI mimics the human brain, it could result in computers being able on their own to detect instances of OCSEA and report it to the relevant authorities. However, regulation of the use of AI is a vast and

[36] https://master-iesc-angers.com/artificial-intelligence-machine-learning-and-deep-learning-same-context-different-concepts/
[37] https://en.wikipedia.org/wiki/Deep_learning#Deep_learning_revolution

complex field of research and it requires different mechanisms than the ones used to control CV technology.[38] Two elements should be considered here:

- *quality of the dataset* - the origin of the dataset in terms of how the dataset has been built, i.e. has this involved collecting public or private conversations, which organisations are involved, have industry or law enforcement gathered and managed this dataset?
- *characteristics of the dataset* - does it contain text conversations only or metadata, such as duration and frequency of communications as well, what language has been chosen for the dataset, is there any other contextual information included, such as the date of creation of the account, the activity of the user account, or the use of a VPN to set up an account?

2.1.4 Implications for this report

A critical challenge lies in identifying the least restrictive means of detecting instances of OCSEA while effectively protecting its victims. Responding to this challenge requires understanding very precisely the objective and the environment for which a particular technology will be selected.

The following elements may be helpful in guiding this process:

- *complexity of the objective* - detecting a known identical image is less complex than searching for similar images. Detecting similar pictures associated with a known image by i.e. depicting the same crime scene is less complex than detecting the same person. The more challenging the objective is, the more complex technology is involved;
- *complexity of the technology* - it is possible to apply complex technologies to straightforward objectives, i.e. deep learning technology can be used to search for identical images whereas less complex solutions could also be applicable in such cases;
- *maturity of the technology* - when it comes to defining safeguards, a well-tested, well-documented and stable technology is a safer choice for the policymakers. It is more challenging to define the appropriate level of safeguards in the case of technology in its early phase of development;
- *complexity of the environment* - the context of the technology deployment significantly matters as the same technology may not be deployed with the same safeguards. The key factors are related to the target audience of the service i.e. for children only, for professionals only, for the public at large, for adults only, whether the technology is deployed in public or private environments, as well as the geographical location and the applicable legal framework in that location.

[38] https://www.forbes.com/sites/cognitiveworld/2020/05/23/towards-a-more-transparent-ai/

2.2 *Practical examples of the use of automated technology to detect online child sexual exploitation and abuse*

As already stated, the use of technology depends to a great extent on what is targeted. With regards to the known forms of OCSEA, the main distinction lies in whether either content, such as CSAM, and/or behaviour, such as grooming is targeted, as well as whether the technology is used as a proactive (prevention) or a reactive (detection) measure.

The table presented below summarises and simplifies the applicability of the previously explained technological solutions to the main forms of OCSEA. It shows that almost the same range of technological solutions are available in the prevention or detection of the main forms of OCSEA. The choice of technological solution should be based on careful assessment as to which of them - in the range - is the most efficient for the purpose considered. As an example, in the case of such form of OCSEA as online availability of CSAM all three families of the automated detection tools are applicable: FH, CV as well as AI. However, their mode of application may differ significantly if the tools are adopted for different purposes.

The form of OCSEA	Prevention	Detection
Online availability of CSAM	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence
Grooming/solicitation of children for sexual purposes	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence, such as Anti-grooming tool (text, metadata, visual content)	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence , such as Anti-grooming tool (text, metadata, visual content)
Child sexually suggestive or explicit images and/or videos generated, shared and received by children	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence, such as Anti-grooming tool (text, metadata, visual content)	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence, such as Anti-grooming tool (text, metadata, visual content)
Sexual coercion and extortion	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence, such as Anti-grooming tool (text, metadata, visual content)	File Hashing Computer Vision, such as PhotoDNA Artificial Intelligence, such as Anti-grooming tool (text, metadata, visual content)

Live-distant child abuse	Computer Vision (based on local descriptors) may help to identify a crime scene (known room or building) Artificial Intelligence (text, metadata, visual content)	File Hashing Computer Vision (based on local descriptors) may help to identify a crime scene (known room or building) Artificial Intelligence (text, metadata, visual content)

2.2.1 Content oriented activities

International Association of Internet Hotlines (INHOPE)

A good example of the use of FH and CV technologies originates from the activities of the International Association of Internet Hotlines (INHOPE), established in 1999. INHOPE is currently made up of 47 hotlines around the world that operate in 43 countries. Each hotline enables the public to anonymously report online material they suspect may be illegal with a focus on CSAM[39].

In order to collect, exchange and classify reports of CSAM the hotlines use a secure platform called '*I see Child Abuse Material*' (ICCAM)[40] which also facilitates image/video hashing/fingerprinting and crawling technologies. Once a hotline receives a public report, the hotline analyst assesses the reported material, and if it is established that there is illegal material on that page, the Uniform Resource Locator[41] (URL) is inserted into ICCAM, the key feature of which is automation. The system then crawls all information found on that URL, assigns a hash value to each image/video and traces its hosting location. Hash value is compared to existing hash lists of baseline CSAM (internationally illegal according to INTERPOL's criteria),[42] national CSAM (according to national legislation in the receiving and hosting country) and identifies unique/already classified material. If content is unique (not found in a hashlist) the analyst can then classify each crawled image/video separately as: baseline, nationally illegal or not illegal.

The flow chart presented below shows the most common scenarios of the process of CSAM removal.

[39] Description of this process is based on the INHOPE 2020 report, (available at: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf).

[40] The ICCAM platform was developed by INHOPE and Ziuz Forensics with funding from the European Commission under the Safer Internet and Connecting Europe Facility programmes. It enables multistakeholder collaboration between hotlines, law enforcement agencies (particularly INTERPOL) and the industry.

[41] URL is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A typical URL could have the form: http://www.example.com/index.html.

[42] The Baseline system allows partners in the public and private sectors to recognize, report and remove known child sexual abuse material from their networks. They can do this by checking images and videos against INTERPOL's Baseline list, which contains the '*digital signatures*' of some of the worst child abuse images and videos. To be included in the Baseline list, child abuse images and videos must be recognized as such by specialist network of investigators, and meet specific criteria in terms of the severity of the image content, for example those believed to feature children aged 13 and under. The strict criteria ensure that the Baseline list refers only to images and videos which would be considered as illegal in any country. More information is available at: https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content.

This automated process reduces both the amount of CSAM that analysts are exposed to as well as duplication of work. As an example, in 2020, reports made to the US hotline, CyberTipline included 33.6 million images, of which 10.4 million were unique (using CV based on global descriptors), and 31.6 million videos, of which 3.7 million were unique (using CV based on local descriptors).[43] As reported by INHOPE, 60% of all URLs assessed by INHOPE hotlines in 2020 came from previously assessed material, which means that the same content is spreading and is being repeatedly reported.[44]

[43] https://www.missingkids.org/gethelpnow/cybertipline
[44] INHOPE 2020 report, p. 28.

In most cases the receiving hotline informs local law enforcement and sends a Notice and Takedown order[45] to the relevant hosting provider if the material is illegal. All images and videos marked as baseline and nationally illegal are made available to INTERPOL through an ICCAM portal specifically designed for them. Consequently, INTERPOL downloads this material and transfers it for inclusion into their International Child Sexual Exploitation Image Database (ICSE Database).[46]

One of the key features of the processes described above is the level of knowledge of a hotline analyst, who assesses illegality of the reported content, decides to enter the report into ICCAM and - if it is unique (not found in a hashlist) - classifies each crawled image/video as baseline, national or not illegal. This task bears heavy responsibility, as if wrongly classified content serves as a reference for future cross check, it can potentially return with a number of false positives. Some of the INHOPE hotlines, i.e. IWF use the '*three pairs of eyes*' verification method through which three trained analysts look at each image and assess it before a hashed image is included on the list.[47]

Specific role of National Center for Missing & Exploited Children (NCMEC, the U.S.)

U.S. federal law requires that U.S.-based SPs report instances of apparent CSAM that they become aware of on their systems to NCMEC's CyberTipline.[48] To date, over 1,400 companies are registered to make reports to NCMEC's CyberTipline[49] and these reports are vital to helping remove children from harmful situations and to stopping further victimization.

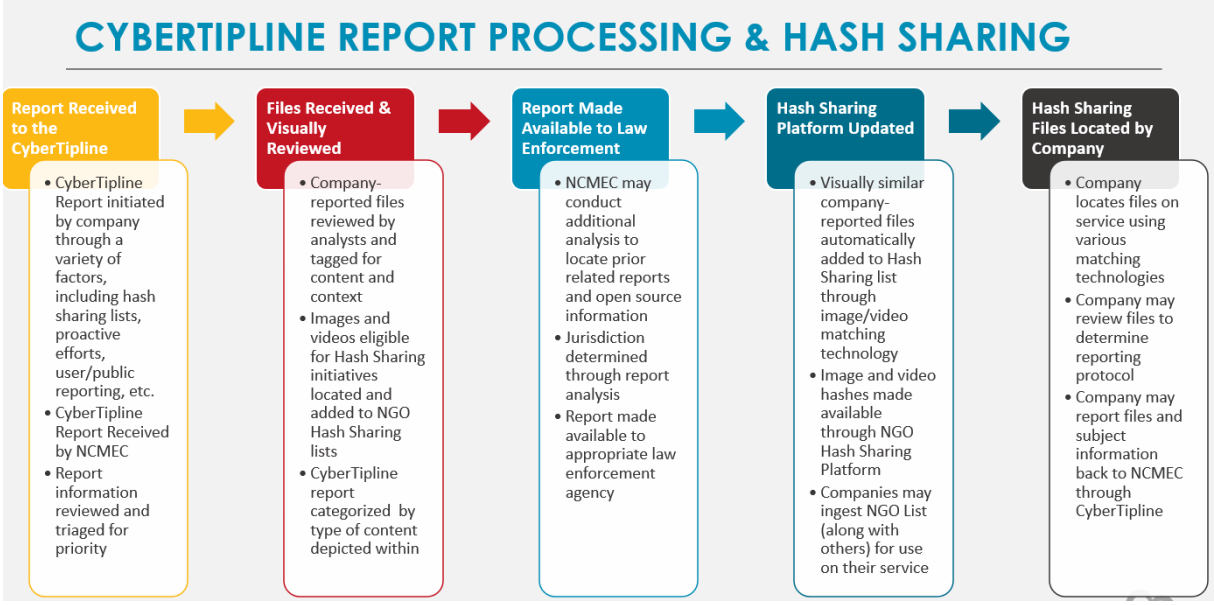
In 2020 the CyberTipline received more than 21.7 million reports, which is an increase of 28% from 2019 (16.9 million in 2019). Whereas the majority (21.4 million) were obtained from ESPs, 303,299 of those reports were from the public, which is more than double that of 2019 (150,667 reports). [50] As suggested by NCMEC, higher numbers of reports can be indicative of a variety of factors, including larger numbers of users on a platform or how robust an ESP's efforts are to identify and remove abusive content.[51]

There are over 30 companies that have access to the NCMEC platform containing more than 7.1 million CSAM hashes at the moment. The IWF[52] and the Canadian Centre for Child Protection also provide a hashlist (via NCMEC's hash platform) to U.S.-based companies. As an example, just the NCMEC's hashlist contains 3.5 million images and 385,000 videos. The companies themselves also create CSAM

[45] A Notice and Takedown order (as explained in the INHOPE's 2020 report) is a procedure for asking a hosting provider (HP) or search engine to immediately remove or disable access to illegal, irrelevant or outdated information hosted on their services. INHOPE hotlines send Notice and Takedown orders to HPs when a member of public sends them a URL containing illegal images and videos depicting child sexual abuse and exploitation.
[46] International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool, which allows specialized investigators from more than 60 countries to share data on cases of child sexual abuse. The database avoids duplication of effort and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images. It holds more than 2.7 million images and videos and has helped identify 23,500 victims worldwide. More information is available at: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.
[47] https://annualreport2020.iwf.org.uk/tech/keyservices/hash
[48] 18 U.S.C. § 2258A
[49] https://www.missingkids.org/theissues/csam#bythenumbers
[50] https://www.missingkids.org/gethelpnow/cybertipline
[51] https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf
[52] https://www.iwf.org.uk/our-services/hash-list

hashlists and share them amongst each other (via a platform that NCMEC offers). This process means that CSAM is often identified and removed before either the public or hotlines ever become aware of it. NCMEC does not use ICCAM in these instances because the content has already been removed from the internet.

The flow chart presented below shows the most common scenarios of the report processing and hash sharing by CyberTipline.



Hash Check Service – Expertise bureau Online Kindermisbruik (EOKM, NL)

Another example of the use of the technology discussed is drawn from the experience of the Dutch hotline, EOKM. Since 2019, the EOKM has offered a Hash Check Service (HCS), the tool comprising a database of millions of hashes of images involving sexual exploitation of children. By means of an API, users can check images against the database to see whether it has a record of them. In 2020, the HCS verified 18.2 billion images, which resulted in close to 7.4 million hits.[53] Thanks to the check, hosting companies were able to delete these from their servers.

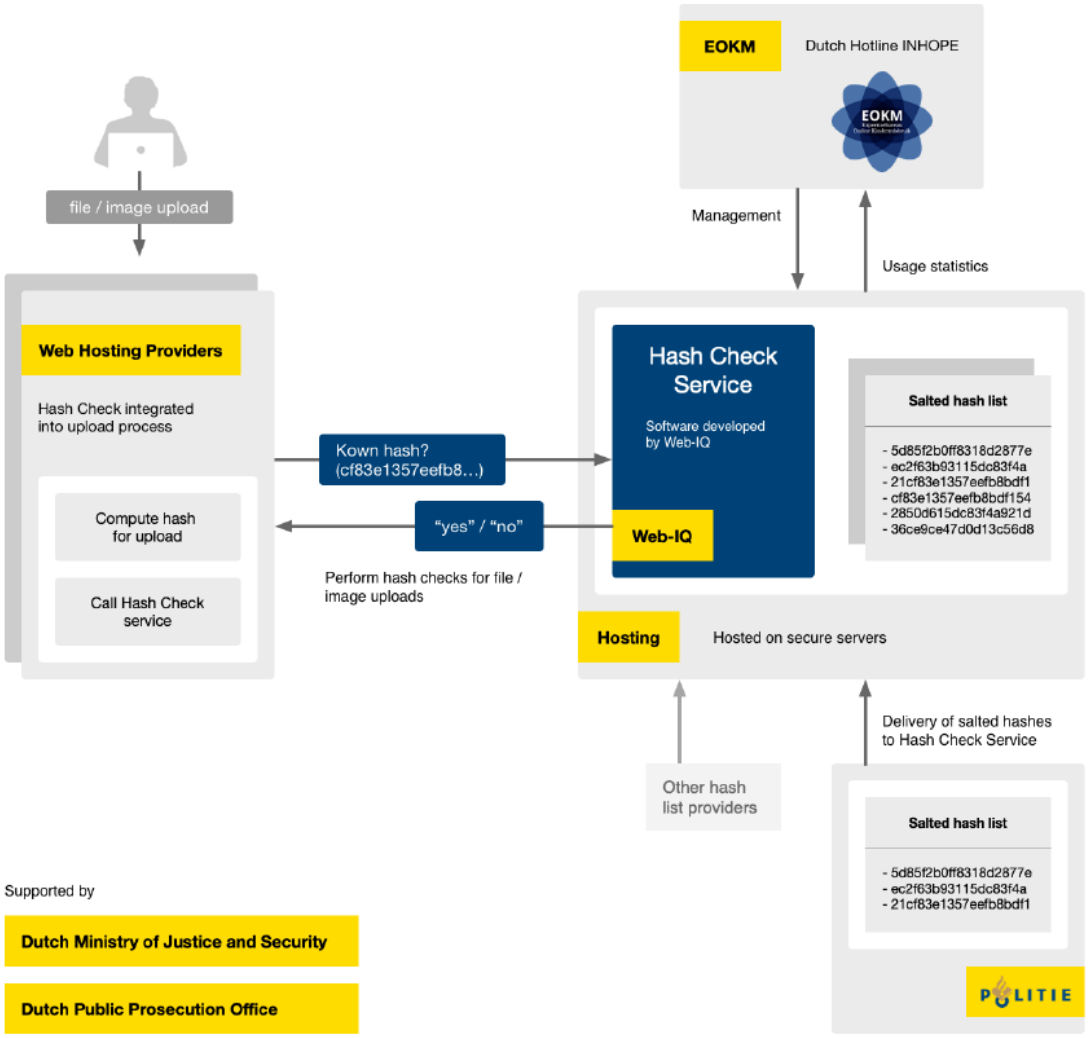
As suggested by EOKM, the numbers are high because many users started out by having all their materials checked for illegal images in one go. Expectations are that the number of images checked will go down in the future., however, because new users keep connecting to the HCS it is difficult to make any definite predictions at this stage. [54]

In the course of 2021, EOKM will be launching two new projects: the first project is aimed at getting more insight into the number of hits they see. As these are hashes rather than actual images, they are currently unable to sufficiently analyse the type of images they find, so more precise data will help

[53] EOKM 2020 report, p. 10, (available at: https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarveslag-2020-DEF-ENG.pdf).
[54] Ibid.

them gain better answers. The second project is a pilot with Web-IQ[55], aimed at analysing how the effect of the hash check server differs between parties that are connected and parties that are not.

The below flow chart explains the HCS functionality:



Internet Watch Foundation (IWF, UK)

Another approach to the use of the technology in question has been taken by IWF, which instead of offering a service to check hashes shares the IWF Hash List under licence with the IWF Members. To make it easy for technology companies to use, each hashed image is graded according to international standards, so companies have confidence in the data that is provided to them. IWF have developed an efficient way to grade and hash millions of child sexual abuse images: an image grading tool, which also de-duplicates multiple hashes as well as images. This means that it can also take hashes or images from other organisations and automatically de-duplicate those against hashes which are already in the system. Such solution again saves time, money and safeguards the welfare of people who would have otherwise needed to view the imagery.[56]

[55] https://web-iq.com/
[56] IWF 2020 report, (available at: https://annualreport2020.iwf.org.uk/tech/keyservices/hash).

Examples of innovation

In recent years, there has been an increase of proactive search efforts taken by hotlines where the national jurisdiction allows it. However, it needs to be noted, that while public reporting leads predominantly to the discovery of previously unknown material, pro-active search predominantly supports removal of already known material, which is reappearing on the internet.[57]

Among INHOPE's network only the IWF was active in the proactive search of CSAM online in 2020.[58] This was made possible by the creation of an intelligent web crawler[59], loaded with over 566,000 hashes of known child sexual abuse images which was deployed to methodically browse targeted areas of the internet. The crawler is used as one operational tactic in a suite of tools designed to find, remove, and disrupt the availability of child sexual abuse material. Apart from running the crawler to generate proactive reports for IWF analysts, it is also used to check the domains of a growing number of domain registry Members who are committed to taking preventative steps to stop their services from being abused. Statistics show that proactive search leads to substantially higher number of identified CSAM. In 2020 it crawled almost 42 million webpages, and over half a billion images. The proactive searching resulted in 154,311 assessed reports which was equal to 52% of the total number of IWF reports.[60]

Another example of innovation in the examined field is Project Arachnid,[61] operated from 2016 by the Canadian Centre. The platform determines that a particular URL contains CSAM by comparing the media displayed on the URL to a database of known digital signatures that have first been assessed by analysts as CSAM. If CSAM is detected, a notice is sent to the hosting provider requesting its removal. Processing tens of thousands of images per second, Project Arachnid detects content at a pace that far exceeds that of traditional methods of identifying and addressing this harmful material.

Project Arachnid is currently detecting over 100,000 unique images per month that require analyst assessment, and this number has been increasing each month. The outcomes of Project Arachnid thus far are self-evident. By 1 June 2021 more than 127 billion images were processed, 39 million images triggered for analyst review, more than 7.5 million notices sent to providers, including 85% of the notices issued relate to victims who are not known to have been identified by police.[62] Such big number of images triggered for analyst review called for collaboration with child protection hotlines around the world. In 2017, the Canadian Centre created the Arachnid Orb - a device that allows other international hotlines to work collaboratively within Project Arachnid. The Arachnid Orb enables analysts worldwide to pool their collective expertise, thus reducing the duplication of assessment and ultimately increasing the number of notices that can be sent through Project Arachnid. The larger the volume of trusted, quality assured hashes, the more effective Project Arachnid will become at

[57] '*Study on framework of best practices to tackle child sexual abuse material online*', carried out for the European Commission by ICF S.A, Wavestone and Grimaldi Studio Legale, p. 5, (available at: https://www.researchgate.net/publication/343813142_Study_on_Framework_of_best_practices_to_tackle_child_sexual_abuse_material_online_EXECUTIVE_SUMMARY_English).
[58] INHOPE 2020 report, p.33.
[59] https://annualreport2020.iwf.org.uk/tech/new/crawlers
[60] Ibid.
[61] https://projectarachnid.ca/en/#what-is-it and https://www.protectchildren.ca/en/press-and-media/news-releases/2021/project-arachnid-csam-online-availability
[62] Ibid.

detecting CSAM and expediting the request to providers to remove these harmful images and/or videos.

The platform was initially designed to crawl links on sites previously reported to Cybertip.ca that contained CSAM and detect where these images and/or videos are being made publicly available. Today Project Arachnid still carries out the crawling activities as described above, but it is continually evolving and adapting to enhance its capabilities in combating CSAM. For example, Shield by Project Arachnid has been developed for use by ESPs to improve upon and accelerate the detection of this harmful material, thus facilitating its speedy removal.

As a final note on the hash sharing-oriented initiatives, it is worth mentioning a recently awarded by DG CONNECT project (CNET/LUX/2020/OP/0059)[63], aiming at facilitating the swift removal of online CSAM. The proof-of-concept solution which will be developed by PwC EU Services[64] together with the EOKM, European Service Network (ESN) and Web-IQ is expected to facilitate the swift voluntary removal of CSAM by improving interoperability, interconnectivity, and quality of data sets. Specifically, it will contribute to proactive identification of hosted media matching known CSAM. The tool also offers a less invasive option for industry via pre-emptive scanning of moment of upload to filter out objectionable material at the source. In effect, this creates a harmonised and holistic foundation for all relevant stakeholders to collect, share and use the invaluable hash databases that catalogue all known CSAM content. This initiative also implies enhancing transparency of the measures aiming at tackling online availability of CSAM.

A last example of innovation, this time by IWF, is the use of AI to enhance analysts' capability by creating a classifier to help triage images[65]. This technology uses machine-learning to signal which reports are most likely to contain child sexual abuse material, and which might not. It will allow analysts to prioritise their work and enable us to focus on those reports which include images of the youngest children being sexually abused. However, it needs to be stressed, that in terms of identifying victims, it is vitally important that there are human eyes making assessments and judgments on the content and AI has not got to the stage where it can make granular distinctions[66]. Similar projects are currently being undertaken by other stakeholders, i.e. project APAKT, led by the Polish hotline, Dyżurnet.pl.[67]

2.2.2 Behaviour oriented activities

Anti-grooming tool

Successful combating of some of the currently existing types of OCSEA requires involvement of other technological solutions beyond the content-oriented technologies described above. The recently announced grooming detection technique is built on AI and aims at targeting behaviours, such as those typical of online predators attempting to lure children for sexual purposes. From the publicly available

[63] https://etendering.ted.europa.eu/cft/cft-display.html?cftId=6634
[64] https://www.pwc.com/gx/en/services/european-union.html
[65] https://annualreport2020.iwf.org.uk/tech/new/classifiers as well as https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/
[66] Ibid.
[67] https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/4100,System-reagujacy-na-zagrozenia-bezpieczenstwa-dzieci-w-cyberprzestrzeni-ze-szcze.html?search=382648399

description as to how the technique works, it can be inferred that this technique does not involve deep learning. The data set seems to be indeed too limited for deep learning, which requires billions of data.

The development of this new technique/tool began in November 2018, and from January 2020 its licensing and adoption has been handled by Thorn.[68] The technique can be used cost-free by technology companies with a chat function who are seeking to protect children from online predation on their platforms as well as law enforcement and non-governmental organizations (NGOs) that are also eligible to apply.[69] Building off the Microsoft patented technology *'Identification and quantification of predatory behaviour across communications systems', 'the technique is applied to historical text-based chat conversations. It evaluates and 'rates' conversation characteristics and assigns an overall probability rating. This rating can then be used as a determiner, set by individual companies implementing the technique, as to when a flagged conversation should be sent to human moderators for review. Human moderators are then capable of identifying imminent threats for referral to law enforcement, as well as incidents of suspected child sexual exploitation to NCMEC'*.[70]

At the time of writing, the availability of public information on the status of deployment of this technology by industry and law enforcement is very limited. It is known that Microsoft has been leveraging the technique in programs on their Xbox platform for several years and is exploring its use in chat services, including Skype. [71]

IWF reThink Chatbot

The last example of technological solutions targeting online behaviours is an interactive chatbot that is being developed by IWF as a part of two-year project financed the End Violence Fund.[72] The chatbot aims to curb the demand for online child sexual abuse material in the way that it will interrupt people trying to access this imagery and prevent them from committing a criminal offence. The IWF reThink Chatbot will interact with internet users who are showing signs that they might be looking for images of child sexual abuse. It will attempt to engage them in a friendly and supportive conversation, and at the right moment, signpost them to the help and intervention support that they need. This project aims to roll-out a pilot by the end of 2021 with a full operational roll-out in 2022. It is believed that this project has massive potential and will help in our proactive fight against online child sexual abuse and exploitation.

2.2.1 Implications for this report

The practical examples of the use of automated technology to detect OCSEA discussed above give rise to an important observation: having a human decision maker is an integral condition of accountability of the technological solutions. Human intervention remains vital in all aspects of the discussed area:

[68] Thorn: Digital Defenders of Children, previously known as DNA Foundation, is an international anti-human trafficking organization that works to address the sexual exploitation of children. The primary programming efforts of the organization focus on Internet technology and the role it plays in facilitating child pornography and sexual slavery of children on a global scale. The organization was founded by American actors Demi Moore and Ashton Kutcher.

[69] https://www.thorn.org/blog/what-is-project-artemis-thorn-microsoft-grooming/

[70] https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/

[71] Ibid.

[72] https://annualreport2020.iwf.org.uk/tech/new/chatbots

from making a choice of datasets used to train algorithms to involving human eyes making assessments and judgments on the reported illegal content.

In particular circumstances, as it is in the case of grooming and its potential risk of proliferation to all platforms providing chat functions, the use of automated technology is essential because it currently provides the only possible means through which to scan large volumes of data and to rescue a child before exploitation occurs.

Whereas there are global concerns relating to the business operations of certain private sector companies it seems that, according to practitioners experienced in combating OCSEA, these concerns should be considered irrelevant to the use of hashing and grooming measures to combat OCSEA. As raised by the representatives of NCMEC in their letters to the Members of EP regarding European Parliament consideration of the proposed Interim Regulation relating to the e-Privacy Directive: *'Hashing technology to combat OCSEA has been utilised for nearly 20 years and based on this experience it can be stated that hashing, and the newer grooming indicators, when used in relation to OCSEA do not monitor or profile unrelated online activity and always involve some level of human or secondary review. When an online service uses hashing technology to detect online child sexual abuse, it does not catalogue or comprehend the content it scans, rather it only searches for specific child sexual abuse imagery it is trained to recognize. All other content passes by without recognition, cognizance, or cataloguing. Grooming indicators operate similarly, except a combination of specific factors produce an alert '.*

While the practitioner voices of those experienced in combating OCSEA are very important in the public discourse, more transparency on the use of automated detection technologies would enhance the development of accountability mechanisms. Mapping the types of existing applications, including a description of the roles and responsibilities of all actors involved, should constitute the first step in enhancing this level of transparency and accountability.

3. LEGAL FRAMEWORK

3.1 e-Privacy Directive and the European Electronic Communications Code

The context of the discussion in the EP towards a temporary derogation from certain provisions of the e-Privacy Directive, mentioned in the introduction of this document, will serve as a starting point of this section in analysing the applicable legal framework.

On 10 September 2020, the EC published a '*Proposal for a Regulation on a temporary derogation from certain provisions of the e-Privacy Directive as regards to the use of technologies by number-independent interpersonal communications services, for the processing of personal and other data for the purpose of combating child sexual abuse online*'[73]. The EC considered that such derogation was necessary as with the entire application of the European Electronic Communications Code (EECC)[74] from 21 December 2020, providers of certain online communication services, including NI-ICS (such as

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0568

[74] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing The European Electronic Communications Code. Official Journal of the European Union, L 321, 17.12.2018, (available at: https://eur-lex.europa.eu/eli/dir/2018/1972/oj).

voice over IP, messaging, and web-based e-mail services), would fall under the scope of the e-Privacy Directive.

One of the key consequences of the EECC was to alter the legal position of certain online communication services. Prior to the EECC, such services were subject to the eCommerce Directive, which operates on a country of origin basis, i.e. SPs established in one Member State are free to supply services into the other Member States without further restriction.[75] While this was subject to certain derogations, including '*the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors'*,[76] in most Member States laws that enabled law enforcement agencies to request data from SPs was tied to their status as providers of '*electronic communication services*' and therefore the powers were not generally exercised against online communication providers.[77] With the coming into force of the EECC, these SPs now fall within a regulatory regime that operates on a country of destination principle, i.e. SPs are subject to the laws of every Member State into which they offer services. This regulatory shift now means that online communication SPs are generally within the scope of national criminal procedure rules concerning interception and related communications data, as well as the provisions of the e-Privacy Directive applicable to providers of '*electronic communication services*'.

The proposal for a temporary derogation was vital to allow voluntary activities involving the use of the automated technologies aiming at detection, reporting and removal of CSAM to be continued after 21 December 2020. Furthermore, the proposal was also necessary to allow time for adoption of sector-specific legislation to tackle OCSEA more effectively, while adequately respecting fundamental rights, including the right to privacy and freedom of expression.

The challenges inherent in balancing privacy with child protection addressed in the EC proposal triggered an important debate among a number of stakeholders, including those actively involved in combating OCSEA. It is worth noting that private sector companies such as Google, LinkedIn, Microsoft, Roblox, and Yubo publicly committed to continuing their proactive efforts in detection and reporting of OCSEA while the EU deliberated next steps.[78]

Three opinions that are relevant for the area in question are examined below: the European Data Protection Supervisor, the Committee on Civil Liberties, and the European Economic and Social Committee.

3.1.1 European Data Protection Supervisor Opinion

The European Data Protection Supervisor (EDPS) published, on 10 November 2020, Opinion 7/2020 on the EC proposal.[79] The EDPS noted that '*confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life and protection of personal data*' and that 'the measures envisaged by the proposal will interfere with the '*rights to respect for private life and data*

[75] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178/1, 17 July 2000.
[76] Ibid., Art. 3(4)(a)(i).
[77] I.e. *Google LLC v Bundesrepublik Deutschland (C-193/18)* [2019] 1 W.L.R. 6044.
[78] https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety
[79] European Data Protection Supervisor, *'Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online'*, (available at: https://edps.europa.eu/sites/default/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf).

protection of the individuals concerned (users, perceived perpetrators and victims)'. Furthermore, the EDPS considered that the '*general, indiscriminate and automated analysis of all text-based communications transmitted through NI-ICS with a view of identifying new potential infringements does not respect the principle of necessity and proportionality. Even if the technology used is limited to using 'relevant key indicators', the EDPS considered that the deployment of such general and indiscriminate analysis is excessive*'. The EDPS also observed that '*automated analysis of speech or text with a view of identifying potential instances of child solicitation is likely to constitute a more significant interference than the matching of images or video based on previously confirmed cases of 'child pornography''*.

In terms of necessity and proportionality, the EDPS stressed that *'due to the absence of an impact assessment accompanying the proposal, the EC has yet to demonstrate that the measures envisaged by the proposal are strictly necessary, effective, and proportionate for achieving their intended objective'.* The EDPS, in the first instance, called upon the EC to provide additional information to enable the co-legislators to consider whether the envisaged measures satisfy the requirements of necessity, effectiveness, and proportionality. According to the EDPS opinion, in order to assess the impact of a measure on the fundamental rights to privacy and to the protection of personal data it was imperative to identify precisely[80]:

- *the scope of the measure*, including the number of people affected and whether it raises '*collateral intrusions*' (i.e., interference with the privacy of persons other than the subjects of the measure);
- *the extent of the measure*, including the amount of information collected; for how long; whether the action under scrutiny requires the collection and processing of special categories of data;
- *the level of intrusiveness*, taking into account: the nature of the activity subjected to the measure - whether it affects actions covered by the duty of confidentiality or not, lawyer-client relationship, medical activity; the context - whether it amounts to the profiling of individuals concerned or not, whether the processing entails the use of (partially or fully) automated decision-making system with a '*margin of error*',
- whether it concerns *vulnerable persons* or not;
- whether it also affects other *fundamental rights*.

The EDPS was also particularly concerned that the proposal did not explain the governance model of ESPs using the derogation, including how they would report or to whom, as well as who would be in charge of maintaining and updating the relevant databases for identifying future instances of OCSEA. Additionally, the EDPS recommended that the validity of any transitional measure should not exceed 2 years.

3.1.2 Report of Committee on Civil Liberties, Justice and Home Affairs Report

The Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the EP published on 11 December 2020 a Report on the EC proposal.[81] The general consideration of the LIBE was that '*the proposed*

[80] Ibid.

[81] Committee on Civil Liberties, Justice and Home Affairs of the European Parliament. '*Report on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by*

regulation did not provide in itself for a legal basis for the scanning of communication by the respective ESPs. Instead, it provided for a restriction of certain rights and obligations laid down in e-Privacy Directive and laid down additional safeguards to be respected by the providers if they wish to rely on this regulation'.[82]

Furthermore, the LIBE clarified the scope of the measure and stated that the EC proposal '*should only apply to videos or images exchanged over messaging or email services. It should not apply to the scanning of text or audio communication, which remains fully subject to the provisions of the e-Privacy Directive'*. In view of its temporary nature, the material scope of the regulation should be limited to the established definition of so called '*child pornography*' and '*pornographic performance*' as defined in Directive 2011/93/EU (CSEA Directive). [83]

According to the LIBE,[84] in order to ensure the proportionality of the restriction to the fundamental rights providers of NI-ICS that wish to reply on this regulation would have to fulfil certain conditions, including:

- a mandatory prior data protection impact assessment pursuant and a mandatory consultation procedure, prior to the use of the technology as required by Articles 35 and 36 of the GDPR);
- using Article 6 (1) d) or e) of GDPR as a legal basis;
- ensuring human overview and intervention for any processing of personal data, and that no positive result is sent to law enforcement authorities or organisations acting in the public interest without prior human review;
- putting in place appropriate procedures and redress mechanisms: no interference with any communication protected by professional secrecy as well as adequate legal basis for transfers outside the EU, in line with Chapter V of the GDPR;
- effective remedies provided by the Member States at national level.

In terms of time limitation of the proposed regulation, the LIBE observed that the period of application of the EC regulation should be limited until 31 December 2022. In case future long-term legislation is adopted and will enter into force before that date, that legislation should repeal the regulation.

3.1.3 European Economic and Social Committee Opinion

In the opinion published on 11 January 2021 the European Economic and Social Committee (EESC)[85] highlighted its general agreement with the proposed regulation for a temporary and strictly limited

number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online', (COM(2020)0568 – C9-0288/2020 – 2020/0259(COD)), (available at: https://www.europarl.europa.eu/doceo/document/A-9-2020-0258_EN.html).

[82] As expressed in the Explanatory Statement, para. a.

[83] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093).

[84] As expressed in the Explanatory Statement, para. c.

[85] Opinion of the European Economic and Social Committee on '*Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online*', (available at:

derogation from Articles 5(1) and 6 of the e-Privacy Directive. The EESC stated that to safeguard privacy and protection of personal data:[86]:

- processing of data must be proportionate and limited to well-established technologies regularly used by NI-ICS for that purpose before entry into force;
- technology used must be in accordance with the state-of-the-art technology used in the industry and must intrude on privacy as little as possible;
- the technology used must in itself be sufficiently reliable and limit error rates to the maximum possible, and rectify any errors without delay, should they occur;
- only *key indicators* technology should be used to detect *child solicitation*;
- processing must be limited to what is strictly necessary for that purpose, and immediate erasure must occur unless there is a detection of online OCSEA;
- the provider is obliged to publish an annual report on its related processing.

However, the EESC was not in favour of the proposed timeframe of derogation (until 31 December 2025) and stated that the EC should ensure that proper privacy safeguards for children are developed and implemented sooner than the five years.

3.1.4 Implications for this report

According to the figures recently reported by NCMEC, the situation discussed above has had an impact on the level of reporting of OCSEA. The centre saw a 58% decrease in reports of EU-related OCSEA cases since 21 December 2020, when the new regulations went into effect.[87]

It is therefore very important to note, that on 29 April 2021, the EU reached a provisional agreement on the temporary legislation discussed above. A number of safeguards were agreed, and the process of developing longer-term legislation started with draft legislation due to be produced by the EC by the summer of 2021. According to the press release by EP[88] *'the agreed changes provide for a derogation to the confidentiality of the communication and traffic data articles of the rules governing the privacy of electronic communications and enable the providers of web-based email, chats and messaging services to voluntarily detect, remove and report child sexual abuse online as well as to use scanning technologies to detect cyber grooming. (…) Parliament's negotiators secured that national data protection authorities will have stronger oversight of the technologies used, an improved complaint and remedy mechanism, and that the processed data should be analysed by a person before being reported further. Service providers will also have to improve their reporting on statistics. This temporary legislation should apply for a maximum of three years, or fewer should new permanent rules on tackling child sexual abuse online be agreed in the meantime'.*

At the time of writing this document, the final and agreed text of the EC proposal, has not been made public.

---

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020AE4192&rid=2).

[86] Ibid, para. 2.5.

[87] https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

[88] Committee on Civil Liberties, Justice and Home Affairs. Press Release. '*Provisional agreement on temporary rules to detect and remove online child abuse*', 30th April 2021, (available at: https://www.europarl.europa.eu/news/en/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse).

3.2 Service providers conduct

This section considers the legal nature of the SP, the jurisdictional complexities arising from cross-border service provision and the lawful basis for monitoring and reporting online availability of CSAM.

3.2.1 The notion of a '*service provider*'

The Budapest Convention defines the notion of a 'service provider' in the following terms:

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any *other entity* that processes or stores computer data on behalf of such communication service or users of such service.[89]

This is very broadly drawn, deliberately so, to extend beyond the traditional provider of telecommunication services to a wide range of online SPs that store content on behalf of users, such as social media providers.[90] The BC extends beyond the EECC and could include entities providing what are referred to under EU law as '*information society services*'[91] and '*audiovisual media services*',[92] provided that the service includes '*communication or related data processing services*'.[93]

It is also important to note, that the definition of a SP under national rules governing the provision of services for regulatory purposes does not necessarily align with the definition of a SP for purposes of criminal procedure. The latter may be drawn wider than the former, as is the case in the United Kingdom[94] and Belgium.[95]

3.2.2 Legal framework

Implementing systems to tackle OCSEA involves SPs in two principal forms of conduct, detection (including removal) and reporting. Detection involves the monitoring and analysis of users' data, commonly distinguished into three main categories:

- *content*, whether in transmission or at rest;
- *traffic data*, detailing the attributes of a user's communication activities;[96]
- *subscriber information*, supplied to the SP when entering into a customer relationship.[97]

---

[89] Article 1c.
[90] Explanatory Report, para. 27.
[91] Directive 2015/1535/EU laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Official Journal of the European Union, J L 241/1, 17 September 2015, (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2015:241:FULL&from=RO).
[92] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, (Audiovisual Media Services Directive) OJ L 95/1, 15 April 2010, as amended by Directive (EU) 2018/1808, (available at: https://eur-lex.europa.eu/eli/dir/2010/13/oj).
[93] Explanatory Report, para. 27.
[94] Investigatory Powers Act 2016, s. 261(11) and (12). (available at: https://www.legislation.gov.uk/ukpga/2016/25/section/261).
[95] Procureur-Generaal Bij Het Hof van Beroep te Gent v Yahoo! Inc., Court of Cassation of Belgium, No. P.10.1347.N, 18 January 2011.
[96] BC, Art. 1d.
[97] BC, Art. 18(3).

The '*lawful*' basis for any processing has both negative and positive connotations. Negative in the sense that the processing should not be in breach of any legal obligation, such as confidentiality obligations and illegal interception. Positive in the sense of having a legal justification, as required under data protection law.[98] The legal basis for processing may also differ depending on the type of data being processed.[99]

In terms of reporting OCSEA, whether to a public law enforcement agency or to a recognised hotline, the potential nature of any disclosure can be broadly distinguished into four scenarios:

1. *voluntary* - a SP may report on a purely voluntary basis. This will usually require authority further to some contractual provision existent between the SP and the user. However, the validity of any such authority could be challenged to the extent that a user's consent to be bound by such terms may be adjudged to be invalid by reason of the status of the user (i.e. as a child), the manner in which the consent was obtained or the term itself may be held in breach of mandatory rules;
2. *qualified voluntary* - voluntary reporting may take place under a statutory framework that expressly permits such disclosure, often specifying the particular circumstances and conditions under which the disclosure may be made and granting the SP an immunity from any liability that could arise;[100]
3. *mandatory through liability* – a SP may proactively report OCSEA that it identifies because it has a statutory duty to report such material and a failure to report may result in non-compliance liability, such as an administrative fine, or liability through association (whether as a primary and secondary offender);[101]
4. *mandatory through request* – a SP may receive an authorised request, from '*a court or an independent administrative authority*',[102] to disclose data in relation to the investigation of the criminal conduct of a user.

In terms of facilitating the deployment of automated OCSEA detection systems by ESPs, neither scenario 1 or 4 would appear to provide a suitable legal basis. Under scenario 1, the legal basis is located primarily in private law, which presents significant risks both to the interests of SPs and the rights of users. While scenario 4 may represent the most robust legal framework, it is reactive in nature, pulling the data from SPs, and would be unsuitable given the volumes that are involved. In terms of scenario 3, there can be concerns about the potential implications of liability-based disclosures on SP conduct, including the possibility of over-reporting and consequent adverse impacts on users, hotlines and law enforcement agencies.

While these scenarios are presented as alternatives, in a cross-border environment jurisdictional concurrency can result in a more complex picture. From a SP's perspective, if they are established in one territory, compliance with a mandatory obligation in another territory into which it offers services

[98] GDPR, Art. 6.
[99] I.e. e-Privacy Directive, Art. 6 in respect of traffic data.
[100] I.e. UK Data Protection Act 2018, Sch. 2, Pt. 1, para. 2.
[101] I.e. US (18 U.S.C. § 2258A) and Italian law.
[102] Tele2 Sverige AB v Post-och Telestyrelsen [2017] 2 C.M.L.R 30. See also Szabó and Vissy v Hungary (2016) 63 E.H.R.R. 3, at para. 77.

may be perceived as '*voluntary*' or, at least, '*unenforceable*'.[103] Whether the SP is correct as a matter of law or practice may require judicial determination, which either party may be unwilling to pursue.

3.2.3 Proposal for an EU Regulation on the detection, removal and reporting of child sexual abuse online

In the context of SP conduct it is also very helpful to present scenarios proposed by the EC in the framework of its initiative aimed at setting out the responsibilities of relevant online SPs, requiring them to detect and report child sexual abuse online and to report that material to public authorities.

In December 2020 the European Commission launched a public invitation for feedback submission, regarding a Proposal for Regulation of the European Parliament and the Council on detecting, removing, and reporting child sexual abuse online. According to the Inception Impact Assessment[104] in relation to this initiative, '*efforts to combat child sexual abuse in the EU are fragmented, duplicated, and/or insufficient in some areas, as shown in particular by the monitoring of the implementation of* CSEA Directive*. In particular, efforts to prevent child sexual abuse online and offline in the EU are insufficient, uncoordinated and of unclear effectiveness, while the efficiency and effectiveness of Member States' efforts to assist victims of child sexual abuse is limited as they do not systematically make use of existing best practices and lessons learned in other Member States or globally (…)'*.

Concerning legislative options, the EC will develop various policy options based on further analysis, focusing in particular on the following possible measures at the EU level:

- *a legal framework* establishing a clear legal basis under which relevant SPs could choose to implement *voluntary* measures for detection, reporting, and removal of child sexual abuse on their services, including both *previously known* and *new material* and *text-based threats*. This framework could also set out the relevant public authority/authorities, at the Union level or national level, to which reports should be made.
- *a legal framework* which, in addition to establishing a clear legal basis as in Option 1, would also create *a binding obligation* for relevant SPs to detect, report and remove *known child sexual abuse material* from their services. Under this Option, appropriate SPs could also choose to implement measures to detect, report, and remove new material and/or text-based threats, but *this would not be mandatory*.
- *a legal framework* that creates *a binding obligation* for relevant SPs to detect, report and remove child sexual abuse from their services, *applicable to both known and new material and to text-based threats* such as grooming. As in Option 1, this framework would also set out the relevant public authority/authorities, at Union level or national level, to which reports should be made[105].

[103] The U.S. Cloud Act, for example, removes the '*blocking*' provision under the Stored Communications Act in respect of law enforcement requests from those countries with whom the US has entered into a bilateral agreement (18 U.S.C. 2511(2)(j)). However, it does not mandate disclosure.
[104] Inception Impact Assessment. Regulation of the European Parliament and of the Council on the detection, removal and reporting of child sexual abuse online, and establishing the EU centre to prevent and counter child sexual abuse, (available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en).
[105] Ibid.

The public invitation for feedback submission resulted in 41 opinions[106] provided by representatives of various environments, including private sector and NGOs. Although the main views expressed there were neither homogeneous nor univocal, they indicated that the approach to prevention and combating CSEA at the EU level do not adequately address the existing challenges, therefore there is urgent need for a coherent and consistent legal framework at the EU level.

3.2.4 Implications for this report

With the liberalisation of the communications sector over the past 40 years, combined with rapid technological developments, such as cloud computing, the complexity of the marketplace can also present challenges to understanding and governing SP conduct. The communications market is both highly interconnected and heavily layered, with extensive supply chains at a physical, logical and operational level.

Supply chain complexity can have implications in terms of transparency, legality and accountability. While statutory provisions or regulations may identify a SP as legally responsible, fulfilment of any duty or obligation may be transferred to another SP through contractual agreement. The resultant allocation of responsibilities through a blend of public and private law mechanisms may serve to render opaque issues of liability and accountability for the operation of automated detection systems. The key point of note is that when referring to the conduct of a '*service provider*', notions of a singular entity often completely underestimate the complexity of the supply chain upon which the actual 'service' depends.

Another consequence is that SPs can access markets on a cross-border basis while operating out of a single territory. The jurisdictional implication of such flexibility is to render the service provider subject to concurrent jurisdictional claims, both from the territory in which they are located and the territories into which they are '*offering services*'.[107] Such jurisdictional concurrency has a '*cost*' for SPs, both in terms of compliance, i.e. having to comply with multiple and differing legal and regulatory regimes, as well as conflicts of law, i.e. where compliance in one jurisdiction results in a potential breach of law in another jurisdiction. While the former would seem a normal '*cost*' of doing business, the latter can have more profound implications in terms of exposing the SP to liability, both corporate and individual, as well as difficulties in ensuring that conduct that interferes with individual rights occurs in '*accordance with the law*'.[108]

[106] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online/feedback_en?p_id=16375286

[107] European Commission proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final (17.4.2018), Art. 1(1), (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN).

[108] I.e. ECHR, Art. 8(2).

3.3 Positive obligations under International and European Human Rights Law regarding the protection of children from online sexual exploitation and sexual abuse

International and European human rights law conceives of human rights in both a negative and positive sense. There is now an overlapping international consensus that *'rights go beyond subjective individual entitlements that places limitations on the State or other duty bearer, and that rights incorporate the notion that states or other actors have duties to respect and protect rights and not merely a duty to desist from violating them'*.[109] This conceptual starting point is central to the idea that States have duties of protection towards individuals at risk of harm from private actors.[110] Consequently, domestic courts internationally and regional human rights courts have upheld and developed protective duties in the terrain of criminal justice, including protection against OCSEA. While the potential for '*coercive overreach*' of this trend requires ongoing scrutiny,[111] it is now well established that States owe duties of protection to actual and potential victims of harm as a matter of international and European human rights law.

3.3.1 Children's rights and positive obligations under international and European human rights treaty law

United Nations

The starting point in the UN system regarding protection against OCSEA is the United Nations Convention on the Rights of the Child (UNCRC). Art. 3 UNCRC requires '*in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration'*. Moreover, Art. 3 asserts that *'State Parties undertake to ensure that child such protection and care as is necessary for his or her well-being'* and 'to *'take all appropriate legislative and administrative measures'* to this end. Art. 19(1) UNCRC requires States to *'take all appropriate legislative measures to protect the child from all forms of physical or mental violence, injury or abuse … maltreatment or exploitation, including sexual abuse*' Art. 19(2) requires States to implement '*protective measures*' including … '*other forms of prevention and for identification, reporting, referral, investigation … and 'for judicial involvement*'. Art. 34 UNCRC requires States to '*protect the child from all forms of sexual exploitation and abuse'*. It requires States parties to '*take all appropriate national, bilateral and multilateral measures to prevent (a) the inducement or coercion of a child to engage in any unlawful sexual activity; (b) the exploitative use of children in prostitution or other unlawful sexual practices; (c) the exploitative use of children in pornographic performances and materials*'. Finally, Article 36 UNCRC asserts that '*State Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare'*.

[109] L Lazarus et al, *'The Evolution of Fundamental Rights Charters and Case Law'*, European Parliament Directorate-General for Internal Policies, Citizen's Rights and Constitutional Affairs, 2011, 34.
[110] See in general L Lazarus, '*The Right to Security*' in (ed), Max Planck Encyclopedia of Comparative Constitutional Law (Oxford University Press 2017).
[111] L Lavrysen and N Mavronicola (eds), '*Coercive Human Rights'*, Hart 2020.

The UNCRC is supplemented by the Optional Protocol to the UNCRC on the Sale of Children, Child Prostitution and Child Pornography (OPSC).[112] An instrument which brings more focused attention to the State's obligations to criminalise, prevent, investigate, prosecute, punish and cooperate internationally in order to prevent the sale of children, child prostitution and child pornography both within and across State borders.[113]

Sexual violence, exploitation and abuse of children is also addressed in complementary UN instruments such as the '*Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children*', *supplementing the UN Convention against Transnational Organised Crime'*[114], as well as soft international law materials including: '*The UN Agenda for Sustainable Development*'[115], (Goals 5, 8 and 16), '*the Rio De Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents*[116]', the recent publication '*Terminology Guidelines of the Interagency Working Group on Sexual Exploitation of Children*',[117] and the UN Commission on Crime Prevention and Criminal Justice Resolution '*Countering child sexual exploitation and sexual abuse online'*.[118] Moreover, guidance has been issued through the reports of the UN Special Rapporteur on the sale and sexual exploitation of children including child prostitution, child pornography and other child sexual abuse material.[119]

Council of Europe

Lanzarote Convention

Under the CoE system, the Lanzarote Convention (LC) requires criminalisation of all kinds of sexual offences against children. It also '*provides a comprehensive and coherent framework covering prevention, coordination of different actors, protection and assistance to victims, comprehensive criminalisation of various forms of abuse and exploitation, [and] rules and instruments to facilitate investigation, prosecution, and procedural law*'.

---

[112] United Nations General Assembly, Volume 2171, A-27531 adopted 25 May 2000 (at July 2019 176 States had ratified or acceded to the Optional Protocol)
http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx

[113] At its eighty-first session (13–31 May 2019, the United Nations Committee on the Rights of the Child (UNCRC))adopted Guidelines regarding the implementation of the OPSC . The Explanatory Report of the OPSC Guidelines includes references to international and regional standards linked to the issues covered under the OPSC, the UNCRC relevant General Comments, and recommendations by other similar bodies, such as the Committee of the Parties to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, also known as the 'Lanzarote Committee'.

[114] https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx

[115] https://www.un.org/sustainabledevelopment/sustainable-development-goals/

[116] https://www.ecpat.org/wp-content/uploads/2016/04/WCIII_Outcome_Document_Final.pdf

[117] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, adopted by the Interagency Working Group in Luxembourg, 28 January 2016 (available at: http://luxembourgguidelines.org/).

[118] https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_28/ECN152019_L3REv1_eV1903716.pdf

[119] See latest report of the UN Special Rapporteur on the sale of children, child prostitution and child pornography, '*Sale and sexual exploitation of children*', A/HRC/43/40, 21 January 2020. See also: UN Special Rapporteur on the sale of children, child prostitution and child pornography, '*25 years of Fighting the Sale and sexual Exploitation of Children: Addressing New Challenges*' 2016, (available at: https://www.ohchr.org/Documents/Issues/Children/SR/25YearsMandate.pdf).

Of specific relevance to the area in question are in particular LC Articles 18 ('*sexual abuse'*), 20 ('*child pornography'*), 21 ('*child pornographic performances'*), 22 ('corruption of children') and 23 ('*solicitation of children for sexual purposes*'). All these provisions require State Parties to *'take the necessary legislative or other measures to ensure that the proscribed conduct is criminalised*'. The Interpretive Opinion, noted in the introduction to this document, has clarified that '*the existing offences in the Lanzarote Convention remain criminalised by national law in the same way, whatever the means used by sexual offenders to commit them, be it through the use of ICTs or not, even when the text of the Lanzarote Convention does not specifically mention ICTs*'.[120]

Moreover, the Interpretive Opinion calls on State Parties to '*ensure appropriate responses to technological developments and use all relevant tools, measures and strategies to effectively prevent and combat sexual offences against children which are facilitated through the use of ICTs*'; allocate resources to authorities responsible for investigation and prosecution '*in order to ensure effective investigation and prosecution of sexual offences against children facilitated through the use of ICTs'*;[121] and '*encourage the private sector working in the field of ICTs to contribute to preventing and combatting sexual exploitation and abuse of children that is facilitated by the use of ICTs'*.[122]

Of specific relevance to the area discussed is Art. 10 LC which, under Art. 10(b) requires '*mechanisms for data collection or focal points, at the national or local levels and in collaboration with civil society, for the purpose of observing and evaluating the phenomenon of sexual exploitation and sexual abuse of children, with due respect for the requirements of personal data protection*'. The Interpretive Opinion consequently encourages 'co-operation between the competent state authorities, civil society and the private sector in order to better prevent and combat child sexual exploitation and abuse that is facilitated through the use of ICTs.

Of further consequence for this enquiry are the requirements in the LC relating to '*investigation, prosecution and procedural law'*. Art. 30(5) requires State Parties to '*take the necessary legislative or other measures to ensure an effective investigation and prosecution of offences established in accordance with this Convention, allowing, where appropriate, for the possibility of covert operations*' and *'to enable units or investigative services to identify the victims of the offences established under Art. 20, in particular by analysing child pornography material, such as photographs and audiovisual recordings transmitted or made available through the use of information and communication technologies'*.

Finally, of significance to this enquiry is Art. 38 LC which sets out general principles and measure for international cooperation. This includes Art. 38(3) which includes a legal basis for mutual legal assistance in criminal matters or extradition. The Interpretive Opinion additionally calls upon States to 'co-operate in order to face the transnational character often present in sexual offences against children facilitated through the use of ICTs'.[123]

Further CoE instruments complement the LC in addressing certain protective aspects including Art. 7 of the European Social Charter (*special protection of children and young persons against physical and*

[120] Interpretive Opinion, para. 12.
[121] Ibid, para. 14.
[122] Ibid, para. 17.
[123] Ibid, para. 19.

moral danger),[124] Revised Social Charter Art. 17 (*the right to children to appropriate social, legal and economic protection*) and Article 17(1)(b) (*requirement of appropriate and necessary measures be taken to protect children and young persons against negligence, violence or exploitation*), the CoE '*Guidelines on Child-Friendly Justice*' adopted by the CoE Committee of Ministers in November 2010;[125] and the Istanbul Convention.[126] Most recently, the Committee of Ministers of the Council of Europe has issued the '*Recommendation on Guidelines to respect, protect and fulfil the rights of the child in the digital environment*' which emphasises the obligations of State and non-state actors (including of business enterprises) and asserts the right of children '*to be protected from all forms of violence, exploitation and abuse in the digital environment*'.[127] Notably, the guidelines recognise that '*any protective measures should take into consideration the best interests and evolving capacities of the child and not unduly restrict the exercise of other rights*'.[128]

Budapest Convention

Of particular significance to this report is the CoE Convention on Cybercrime (Budapest Convention - BC).[129] Article 9 BC requires Parties to criminalise '*offences related child pornography*', ranging from producing and offering to distributing, procuring and possessing such materials. Importantly, the BC includes procedural powers to investigate and secure evidence not only related to cybercrime but any offence involving evidence on a computer system. The same scope applies to the BC provisions on international cooperation.

The Parties to the BC – through the Cybercrime Convention Committee (T-CY) - are currently negotiating a 2nd Additional Protocol to the BC on enhanced cooperation and disclosure of electronic evidence. The full draft of this Protocol[130] was approved by the T-CY on 28 May 2021. This Protocol will provide for new types of measures previously not available in international criminal law agreements, including: direct cooperation with SPs in other States Parties to obtain the disclosure of subscriber information (Article 7), with entities providing domain name registration services to obtain the disclosure of registrant information (Article 6); expedited disclosure of stored computer data in an emergency (Article 9), and emergency mutual assistance (Article 10); and data protection safeguards for data transferred under this protocol (Article 14).

For the purposes of measures against CSAM, and for this present report, the 2nd Additional Protocol will be relevant for a number of reasons. Firstly, the BC currently has 66 State Parties, including the

[124] Council of Europe, European Treaty Series – No. 35, Turin 18.X.1961. This is interpreted by the European Committee of Social Rights to protect against '*all forms of commercial sexual exploitation of children*' including '*child prostitution, child pornography and trafficking of children*' (European Committee of Social Rights, Children's rights under the European Social Charter, Information Document).
[125] See also: Council of Europe Convention on '*Preventing and Combating Violence against Women and Domestic Violence'* (Istanbul Convention); the Council of Europe Convention on Actions against Trafficking in Human Beings, and the BC.
[126] Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention), available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210).
[127] CM/Rec(2018)7.
[128] Ibid, para. 50, p. 7. More information is available in Annex.
[129] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[130] https://rm.coe.int/0900001680a2aa1c

U.S. where many of the SPs are based. Secondly, the procedural powers and international cooperation provisions of this Convention are available to investigate offences and to secure electronic evidence not only for offences related to child pornography under Article 9 BC but also other offences covered under the Lanzarote Convention. Thirdly, the possibility of direct cooperation with SPs to obtain subscriber information under Art. 18 BC and of Arts. 6 and 7 of the future Protocol are available to identify users of an IP address or email or social media account or the registrant of a domain. Fourthly, the emergency measures of the new Protocol will be available to rescue child victims. Hence, in short, the measures of the BC and its new Protocol will also permit follow up to reports on CSAM received from SPs.

The negotiation of this 2nd Additional Protocol, however, has also underlined the need for safeguards, in particular in a cross-border context. For example, the measures of the Protocol apply only to specific criminal investigations and proceedings and do not entail general surveillance of communications. Moreover, State Parties will need to establish a legal basis under domestic law for carrying out the measures under the Protocol. In this respect, the Protocol permits a range of reservations and declarations in order to meet the specific requirements of the domestic law of State Parties. For example, State Parties may require that they are notified when another State Party sends an order directly to a SP in its territory. Further safeguards include: use limitations, confidentiality requirements or grounds for refusal which may apply; a detailed provision on the protection of personal data (Article 14) which was included to ensure that cross border transfer of personal data benefits from a standard of protection considered appropriate by all State Parties, including European Union Member States. Finally, SPs and entities providing domain name services will be reactive to orders or requests under the 2nd additional Protocol which also lists what such orders or requests can specify and what supplemental information shall be provided.

European Union

In the European Union the starting point in relation to the protection from OCSEA, is Art. 24 of the Charter of Fundamental Rights of the European Union (EU Charter). Art. 24(1) EU Charter states that '*children shall have the right to such protection and care as is necessary for their well-being*'. Moreover, Art. 24(2) EU Charter declares that '*in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*'. The '*rights of the child*' are also explicitly promoted under Art. 3 (3) of the Treaty of the European Union. Moreover, under Art. 83(1) Treaty on the Functioning of the European Union '*sexual exploitation of women and children*' is listed as a '*particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis*'.

Child Sexual Exploitation and Abuse Directive (CSEA Directive)

Currently, the leading EU legislative instrument on OCSEA is the CSEA Directive, which was adopted by the EP and the Council on 13 December 2011.[131] The stated purpose of the CSEA Directive is to '*protect children's rights'*, and ensure that the '*child's best interests*' are a '*primary consideration*' by '*public and private actors*'.[132] Moreover, it is to '*establish minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes'*, as well as to introduce '*provisions to strengthen the prevention of those crimes and the protection of victims thereof*'.[133] The CSEA Directive was the '*first comprehensive EU legal instrument*' covering the 'prevention, investigation and prosecution of offences, and assistance to and protection of victims'.[134] It is premised on the recognition that sexual abuse and exploitation of children, on and offline, constitute '*serious violations of … the rights of children to the protection and care necessary for their well-being*'.[135] The Directive is explicit in pursuit of the '*primary consideration*' of the '*child's best interests*' in accordance with Art. 24(2) of the EU Charter and Art. 3 of the UNCRC.[136]

An important and highly relevant provision to this enquiry is Art. 25 CSEA Directive which places two main obligations on Member States. Art. 25(1) requires Member States to '*ensure the prompt removal of web pages containing or disseminating child pornography' both in Member States territory and to 'endeavour to obtain the removal of such pages hosted outside of their territory*'. Article 25(2) is an optional and permissive clause allowing Member States to *'block access*' to such web pages'. It requires that the measures taken are to be '*set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction'*. Moreover, that these '*safeguards shall also include the possibility of judicial redress'*. Recital 47 CSEA Directive also notes in addition that compliance with Art. 25 CSEA Directive does not necessarily involve legislative measures: '*… The measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other. In that context, this Directive is without prejudice to*

[131] The CSEA Directive was prompted in part by the Stockholm Programme to combat '*trans-national threats*' to internal security of the EU and to further the project of mutual recognition in line with Art. 83(1) TFEU (The Stockholm Programme—An open and secure Europe serving and protecting citizens, 2010 /C 115/01, 4.5.2010). The CSEA Directive also coincided with the realisation of the EU Agenda for the Rights of the Child (*An EU Agenda for the Rights of the Child*, Brussels, 15.2.2011 COM(2011) 60 final). The *Agenda* restated the EU commitment to eliminating all forms of violence against children, including sexual violence' (p.7). Over the same time period, complimentary objectives were set within the *EU Safer Internet Programme* which included the objective to: 'reduce the amount of illegal content circulating online and deal adequately with harmful conduct online, mainly online distribution of child sexual abuse material' (Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, 27.2.2008, COM(2008)106 final). Together these moves within the EU prompted decisive reform of the existing Framework Decision 2004/68/JHA and the adoption of the CSEA Directive (See Recitals 6 and 48 CSEA Directive).

[132] Recital 1, 2 and 6 CSEA Directive.

[133] Art. 1 CSEA Directive.

[134] 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'*, 24.7.2020 COM(2020) 607 final (CSA Strategy).

[135] Recital 1 CSEA Directive.

[136] United Nations General Assembly resolution 44/25 of 20 November 1989.

voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States'.

In 2016, the European Commission and Council published an assessment report on the implementation of Art. 25 CSEA Directive (the Art. 25 report).[137] The report noted the crucial necessity of '*cooperation between the private sector, including industry and civil society, and public authorities, including law enforcement agencies and the judiciary*' in order to fulfil the objectives of Art. 25.[138] Moreover, that '*non-legislative measures needed to be measured against the outcomes of Art. 25 in practice*'.[139] After surveying the measures in place, the Art. 25 report concluded that Member States should be encouraged to do more to comply in practice. The '*key challenges*' identified related both to removal of child sexual abuse material and also to the safeguards required where internet users were blocked. The report therefore called for further multi-stakeholder collaboration at the EU level.[140]

The EP CSEA Resolution subsequently expressed regret that '*only half of the Member States have incorporated provisions into their legislation making it possible to block access*' and further urged wider use of the '*more effective' removal measures*'.[141]Moreover, it called upon Member States and EU institutions to cooperate with the Internet industry, Europol/European Cybercrime Centre, Eurojust, Interpol, third country states, as well as various initiatives such as INHOPE and Connecting Europe Facility, in realising the objectives of Art. 25 .[142]

These calls have been followed up in the more recent EU Strategy for a more effective fight against child sexual abuse,[143] and has been restated in the EC initiative, *Delivering for children: an EU Strategy on the Rights of the Child*.[144] Both of these documents suggest that the CSEA Directive will require modification or replacement to remain fit for purpose in the fight against OCSEA, in particular in light of the fact that '*offenders have become increasingly sophisticated in their use of technology and technical capabilities including encryption and anonymity*'.[145]

3.3.2 Jurisprudence on the protection of children from online sexual exploitation and sexual abuse

This section will focus specifically on the judicial development of positive obligations on States regarding protection of children from online sexual exploitation and abuse.

---

[137] Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Art. 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872 final, Brussels 16.12.2016 (henceforth Art. 25 Report).

[138] Art. 25 Report, p. 4.

[139] Ibid.

[140] Ibid.

[141] European Parliament resolution of 14 December 2017 on the implementation of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (2015/2129(INI)) (henceforth EP CSA Resolution)., paras 40 and 44.

[142] European Parliament CSA Resolution, paras 45, 46, 47, 48, 49.

[143] EU Strategy for a more effective fight against child sexual abuse, Brussels, 24.7.2020 COM(2020) 607 final, (available at: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf).

[144] EC, Delivering for children: an EU strategy on the rights of the child, Ref. Ares(2020)3149750 – 17/06/2020, (available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12454-EU-strategy-on-the-rights-of-the-child-2021-24-_en).

[145] CSEA Strategy, p. 6, emphasis in original.

European Court of Human Rights (ECtHR)

The ECtHR has asserted and developed positive obligations in relation to child sexual abuse since the mid-1980s.[146] Initially these obligations were framed within the framework of Art. 8[147] of the ECHR. In *MC v Bulgaria*,[148] however, rape and sexual abuse and sexual exploitation were framed as violations of the absolute prohibition on inhuman and degrading treatment under Art. 3 ECHR. Subsequent case law regarding sexual exploitation and abuse of children has since treated serious cases of abuse as a violation of Art. 3 ECHR, while less serious offences may also be considered by the ECtHR to be a violation of Art. 8.

As sensibilities regarding the seriousness of child sexual abuse have shifted over time, the Court's view of the State's margin of appreciation as regards realisation of positive obligations has narrowed. This was evident already in the *KU v Finland* case which described OCSEA as 'an abhorrent type of wrongdoing , with debilitating effects on its victims'.[149] Increasingly, the ECtHR has referred to the LC and the UNCRC, in particular '*the protection of the best interests of the child*', to clarify the content of the obligations to protect against and effectively investigate child sexual abuse.[150]

In the last three years, the Grand Chamber (GC) of the ECtHR has addressed the positive obligations of States in relation to child sexual abuse in the two major decisions of *A and B v Croatia* (2019) and *X and others v Bulgaria* (2021).[151] These cases represent the culmination of over 25 years of the ECtHR jurisprudence in this area, and provide authoritative guidance on the shape of Member States obligations in this field.

In *A and B v Croatia*,[152] the ECtHR was called upon to examine the treatment of an alleged sexual battery of a four and half year-old victim by her father. First, the Court had to examine the adequacy of the legal framework governing the conduct of the authorities in investigating and processing cases of sexual abuse of children. Second, it scrutinised '*whether the competent authorities had carried out a thorough, effective and prompt investigation*'. Third, it examined '*whether the authorities had afforded sufficient protection to the applicant's right to respect for private life, and especially for her personal integrity in light of her vulnerability due to her young age and alleged sexual abuse and taking the best interests of the child as a primary consideration'*. Thus, the issue was '*not only the effectiveness*

[146] X and Y v The Netherlands, App. No. 8978/80, 26 March 1985; Stubbings v United Kingdom, App. No. 22083/93, 22 October 1996; MC v Bulgaria, App. No 39272/98, 4 December 2003; K.U. v Finland, App. No. 2872/02, 02 March 2009; O'Keeffe v. Ireland [GC], no. 35810/09, ECHR 2014; Y. v. Slovenia, no. 41107/10, § 101, ECHR 2015; M.G.C v Romania, no. 61495/11, 15 March 2016; Trabajo Rueda v Spain, App. No 32600/12, 30 May 2017; A and B v Croatia, GC, App No. 7144/15, final 4/11/2019; X and others v Bulgaria, GC, App. No. 22457/16, 2 February 2021.

[147] X and Y v The Netherlands, App. No. 8978/80, 26 March 1985, see para. 23; Stubbings v United Kingdom, App. No. 22083/93, 22 October 1996, paras 62 – 64.

[148] MC v Bulgaria, App. No 39272/98, 4 December 2003.

[149] K.U. v Finland, App. No 2872/02, 02 March 2009, para. 46.

[150] Söderman v Sweden, App. N0 5786/08, 12 November 2013, para. 80 - 82.

[151] A and B v Croatia, GC, App No. 7144/15, final 4/11/2019; X and others v Bulgaria, GC, App. No. 22457/16, 2 February 2021.

[152] MC v Bulgaria, App. No 39272/98, 4 December 2003. See also: O'Keeffe v. Ireland [GC], no. 35810/09, ECHR 2014; Y. v. Slovenia, no. 41107/10, § 101, ECHR 2015; M.G.C v Romania, no. 61495/11, 15 March 2016.

of investigation, but the alleged lack or inadequacy of measures aimed at protecting in criminal proceedings the rights of a child, who had allegedly been the victim of sexual abuse'.[153]

The ECtHR noted that Art. 3 (along with Art. 8) ECHR, '*entail an obligation on the State to safeguard the physical and psychological integrity of a person' and moreover that 'children and other vulnerable individuals, in particular, are entitled to effective protection'*.[154] The court noted that under Art. 3 '*authorities hold a positive obligation*' which includes '*a duty to maintain and apply in practice an adequate legal framework affording protection against acts of violence by private individuals*'[155] as well as '*requirements related to the effectiveness of the investigation*'.[156] Consequently, Member States must '*ensure that criminal-law provisions for the effective punishment of sexual abuse of children are in place and that they are applied in practice through effective investigation and prosecution'*.[157] As regards the State's margin of appreciation in fulfilling these obligations, the GC noted that '*where a particularly important facet of an individual's existence or identity is at stake, or where the activities at issue involve a most intimate aspect of private life, the margin allowed to the State is correspondingly narrowed*'.[158]

The GC concluded the general assessment with the following important paragraphs which encapsulate the current ECtHR position on the weight accorded to the positive obligations with regard to child sexual abuse, drawing also on the LC:[159]

> *The Court reiterates that in cases of sexual abuse children are particularly vulnerable … The Court also recalls that the right to human dignity and psychological integrity requires particular attention where a child is the victim of violence … The Court recalls that the obligations incurred by the State under Articles 3 and 8 of the Convention in cases such as this, involving and affecting a child, allegedly victim of sexual abuse, require the effective implementation of children's right to have their best interests as a primary consideration … and to have the child's particular vulnerability and corresponding needs adequately addressed by the domestic authorities.*
>
> *In view of the above, the Court considers that States are required under Articles 3 and 8 to enact provisions criminalising the sexual abuse of children and to apply them in practice through effective investigation and prosecution … being thereby mindful of particular vulnerability of children, their dignity and their rights as children and as victims. These obligations also stem from other international instruments, such as, inter alia, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence …*

In *X and others v Bulgaria*,[160] the GC dealt with the State's failure to protect against, and investigate, sexual abuse of children in an orphanage in Bulgaria prior to their adoption in Italy. The facts of the case required international cooperation between the Italian and Bulgarian authorities in the investigation of the alleged abuse. The GC summarised the case law of the ECtHR and laid out the

[153] A and B v Croatia, para. 105.
[154] Para 106, citing O'Keeffe v. Ireland para 144; X and Y v. the Netherlands, paras 23-24 and 27, and M.C. v. Bulgaria, para. 150.
[155] Para. 107, citing Söderman v. Sweden [GC], no. 5786/08, para. 80, ECHR 2013 with further references.
[156] Para. 108.
[157] Para. 110, citing MC v Bulgaria para. 153.
[158] A and B v Croatia, para. 113.
[159] A and B v Croatia , paras 111 and 112.
[160] X and others v Bulgaria, GC, App. No. 22457/16, 2 February 2021.

general principles which applied, echoing those set out in *A and B v Croatia*. On this basis, the GC asserted that:[161]

> *'it emerges from the Court's case-… that the authorities' positive obligations under Article 3 of the Convention comprise, firstly, an obligation to put in place a legislative and regulatory framework of protection; secondly, in certain well-defined circumstances, an obligation to take operational measures to protect specific individuals against a risk of treatment contrary to that provision; and thirdly, an obligation to carry out an effective investigation into arguable claims of infliction of such treatment. Generally speaking, the first two aspects of these positive obligations are classified as "substantive", while the third aspect corresponds to the State's positive "procedural" obligation'*.

With regard to the requirement of an effective criminal investigation, the GC was noted that this may '*include an obligation for the investigating authorities to cooperate with the authorities of another State, implying an obligation to seek or to afford assistance'*. While noting that the nature and scope of this cooperative obligation is inevitably fact dependant, the GC noted that '*States concerned must take whatever reasonable steps they can to cooperate with each other, exhausting in good faith the possibilities available to them under the applicable international instruments on mutual legal assistance and cooperation in criminal matters*'. Moreover, that the Court '*normally verifies in this context whether the respondent State has used the possibilities available under these instruments'*.[162]

Importantly, the Court noted that the positive obligation under Art. 3 ECHR to establish an '*efficient*' and practically '*effective*' 'legislative and regulatory framework to shield individuals sexual abuse was reinforced by 'articles 18 to 24 of the Lanzarote Convention'.[163] Moreover, '*in that connection the Court reiterates that the Convention must be applied in accordance with principles of international law, in particular those relating to the international protection of human rights*' (179).[164] Finally, the general interpretive influence of the founding principles of the Lanzarote Convention were reasserted by the GC in the conclusion of its analysis of the applicable legal standards:

> *Lastly, it is clear from the Court's case-law that, in cases where children may have been victims of sexual abuse, compliance with the positive obligations arising out of Article 3 requires, in the context of the domestic proceedings, the effective implementation of children's right to have their best interests as a primary consideration and to have the child's particular vulnerability and corresponding needs adequately addressed (see A and B v. Croatia, cited above, § 111, and M.M.B. v. Slovakia, no. 6318/17, § 61, 26 November 2019; see also M.G.C. v. Romania, cited above, §§ 70 and 73). These requirements are also set out in other international instruments of relevance to the present case such as the Convention on the Rights of the Child, the Lanzarote Convention and the instruments adopted within the framework of the European Union (see paragraphs 124-27 and 135-37 above).* ***More generally, the Court considers that in cases potentially involving child sexual abuse the procedural obligation under Article 3 of the Convention to conduct an effective investigation must be interpreted in the light of the obligations arising out of the other applicable international instruments, and more specifically the Lanzarote Convention.***[165]

[161] Ibid, para. 178.
[162] Ibid, para. 191.
[163] Ibid, para. 179.
[164] Ibid.
[165] Ibid, para. 192.

*Court of Justice of the European Union (**CJEU**)*

The CJEU has had few opportunities to address OCSEA. Nevertheless, two decisions related to the offences proscribed under the CSEA Directive indicate the weight afforded to the rights of child victims of sexual abuse, exploitation and pornography.

The first decision, *P.I.* v *Oberbürgermeisterin der Stadt Remscheid*,[166] was decided shortly after the CSEA Directive was adopted. It dealt with the question of whether committing the crime of sexual exploitation of children by a person in the circle of trust as defined under Art. 3 and 9 CSEA Directive, constitutes a sufficiently serious crime to be covered by the concept of '*imperative grounds of public security*' capable of justifying an expulsion measure under Art. 28(3) Directive 2004/38/EC. In the course of this decision, the CJEU underlined the gravity of the offences under the CSEA Directive as constituting '*a particularly serious threat to one of the fundamental interests of society, which might pose a direct threat to the calm and physical security of the population*' and as displaying '*particularly serious characteristics*'.[167] To arrive at this conclusion, the CJEU cited the inclusion of sexual exploitation of children as a '*particularly serious crime with a cross-border dimension in which the European Union legislature may intervene*' under Art. 83(1) TFEU.[168] The CJEU also reiterated Recital 1 CSEA Directive in recognising sexual abuse and sexual exploitation of children as constituting a serious violation of the rights of children to the protection and care necessary for their well-being as provided in the UNCRC and the EU Charter of Fundamental Rights of the European Union.[169] Finally, it drew guidance from the minimum punishments proscribed in the CSEA Directive itself:[170]

> *'The serious nature of those kinds of offences is also apparent from Article 3 of Directive 2011/93, which provides, in Article 3(4), that engaging in sexual activities with a child who has not reached the age of sexual consent is to be punishable by a maximum term of imprisonment of at least 5 years, and Article 3(5)(i), which states that engaging in such activities where abuse is made of a recognised position of trust, authority or influence over the child is to be punishable by a maximum term of imprisonment of at least 8 years. Under Article 3(5)(iii), where use is made of coercion, force or threats, that term of imprisonment must be at least 10 years. In accordance with Article 9(b) and (g) of Directive 2011/93, the fact that the offence was committed by a member of the child's family, a person cohabiting with the child or a person who has abused a recognised position of trust or authority and that the offence involved serious violence or caused serious harm to the child are to be regarded as aggravating circumstances.'*

In sum, the *P.I.* v *Oberbürgermeisterin der Stadt Remscheid* decision reaffirms the gravity of the crimes listed under the CSA Directive within the EU order, and the recognition of them as grave fundamental rights violations of children.

---

[166] P.I. v Oberbürgermeisterin der Stadt Remscheid, Case C-348/09, 22 May 2012.
[167] Ibid, para. 28
[168] Ibid, para. 25.
[169] Ibid, para. 26: '*Reflecting that objective, the first recital in the preamble to Directive 2011/93 states that sexual abuse and sexual exploitation of children constitute serious violations of fundamental rights, in particular the rights of children to the protection and care necessary for their well-being, as provided for by the United Nations Convention on the Rights of the Child of 20 November 1989 and the Charter of Fundamental Rights of the European Union*'
[170] Ibid, para. 27.

The second decision of relevance to OCSEA is *La Quadrature du Net and others v Premier Ministre and others*, which was decided by the GC on 6 October 2020.[171] In this case, the CSEA Directive arose in discussion of the '*preventive retention of IP addresses and data relating to civil identity for the purposes of combating crime and safeguarding public security*'.[172]

In respect of retention of IP address data, the CJEU noted that the seriousness of the interference with respect to Art. 7 and 8 EU Charter could only be justified by '*action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security*'. The actions taken in pursuance of the CSEA Directive were determined by the CJEU to fall squarely within this category, and were covered by Art. 15(1) of the Directive on privacy and electronic communications, '*provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of that data*'.[173]

The reasoning of the CJEU in this case gives valuable indication as to the weight to be given to the competing imperatives of protection against OCSEA and data protection rights:

> *154. In order to strike a balance between the rights and interests at issue …, account must be taken of the fact that, where an offence is committed online, the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified. To that consideration must be added the fact that the retention of IP addresses by providers of electronic communications services beyond the period for which that data is assigned does not, in principle, appear to be necessary for the purpose of billing the services at issue, with the result that the detection of offences committed online may therefore prove impossible without recourse to a legislative measure under Article 15(1) of Directive 2002/58, something which several governments mentioned in their observations to the Court. As those governments argued, that may occur, inter alia, in cases involving particularly serious child pornography offences, such as the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of CSEA Directive.*
>
> *155. In those circumstances, while it is true that a legislative measure providing for the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the Internet would catch persons who at first sight have no connection, …, with the objectives pursued, and it is also true, … that Internet users are entitled to expect, under Articles 7 and 8 of the Charter, that their identity will not, in principle, be disclosed, a legislative measure providing for the general and indiscriminate retention of only IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, provided that that possibility is subject to strict compliance with the substantive and procedural conditions which should regulate the use of that data.*
>
> *156. In the light of the seriousness of the interference entailed by that retention with the fundamental rights enshrined in Articles 7 and 8 of the Charter, only action to combat serious crime, the prevention of serious threats to public security and the safeguarding of national security are capable of justifying that interference. Moreover, the retention period must not exceed what is strictly necessary in the light of the objective pursued. Finally, a measure of that nature must establish strict conditions and safeguards concerning the use of that data,*

[171] La Quadrature du Net and others v Premier Ministre and others, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020.
[172] Ibid, para. 152.
[173] Ibid, para. 155.

particularly via tracking, with regard to communications made and activities carried out online by the persons concerned.

3.3.3 Implications for this report

The evolving international jurisprudence on positive obligations over the last decades has been coupled with an increase in international and regional treaty norms and instruments. The result is an established body of international and European human rights obligations placed upon States to criminalise, prevent, investigate, prosecute and punish violations of fundamental rights by private actors. Alongside protection to life, security and gender violence, the protection of children from sexual abuse is a key objective of this field of law.

The best interests of the child as a primary consideration of all public authorities, and protection from sexual violence, abuse and exploitation, is embodied in the UNCRC and the related Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography. These instruments underpin a range of more recent international law instruments in safeguarding these fundamental rights of the child.[174] In the Council of Europe, the LC is the leading specialised treaty which '*arguably constitutes the highest international standards for protection of children against sexual abuse and exploitation'*.[175] This instrument complements a range of CoE standards, in particular the Budapest Convention, aimed at protection of children from sexual violence and exploitation both offline and online.[176] In the EU, Art. 24 EU Charter, and Art. 3(3) of the Treaty of the EU, safeguard the rights of the child and the principle that '*children shall have the right to such protection and care as is necessary for their well-being*'.[177] Moreover, Article 83(1) of the Treaty on the Functioning of the European Union lists '*sexual exploitation of women and children*' as a '*particularly serious crime with a cross border dimension*'. Finally, the CSEA Directive is a specialised legislative instrument designed to embed the protections of the LC into EU Law. Like the LC, the CSEA Directive includes specific State obligations to protect children from OCSEA.

In the ECtHR, the protection of children from sexual abuse and exploitation is affirmed as a positive obligation arising from Article 3 and Article 8 ECHR. The scope and structure of this general obligation has been developed over twenty-five years of ECtHR jurisprudence, and has evolved in light of developing international and European standards. The ECtHR emphasises that the realisation of this positive obligation must be '*practical and effective'*. States must consequently achieve their stated objective in practice, and not in a theoretical or illusory sense. As recently encapsulated in two leading

[174] Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UN Convention against Transnational Organised Crime (15 November 2000); UN Agenda for Sustainable Development, Goals 5, 8 and 16; Rio De Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents (2008); '*Terminology Guidelines of the Interagency Working Group on Sexual Exploitation of Children*'; and the UN Economic and Social Council, Commission on Crime Prevention and Criminal Justice, '*Countering child sexual exploitation and sexual abuse online*' (24 May 2019).
[175] EU COM Proposal for a Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (COM (2010) 94 final, p. 2.
[176] Art. 7 European Social Charter; Art. 17 Revised European Social Charter; Council of Europe Guidelines on Child-Friendly Justice (2010); Recommendation on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (CM/Rec(2018)). See further Annex.
[177] Art. 24(1) Charter of Fundamental Rights of the European Union.

cases,[178] the obligation consists of a duty to 'maintain and apply in practice an adequate legal framework affording protection against acts of violence by private individuals. This entails that States adopt criminal law provisions for the effective punishment of sexual abuse of children and apply these provisions in practice through effective investigation and prosecution. The obligation also requires States to cooperate with the authorities of other States to seek or afford mutual assistance, and exhaust '*in good faith*' all '*applicable international instruments on mutual legal assistance and cooperation in criminal matters*'. [179]

The CJEU recognises the weight of the prohibition on child sexual abuse within the EU legal order, noting the gravity of the crime as a *'particularly serious threat to one of the fundamental interests of society',* [180] constituting a '*serious threat to public security*', [181], and displaying '*particularly serious characteristics*'.[182] The CJEU views child sexual abuse as a grave violation of the fundamental rights of children, and has embedded the protection against OCSEA in the principle of the best interests of the child as expressed in Art. 24 EU Charter, the UNCRC and the CSEA Directive.[183]

The jurisprudence on positive obligations has also been clear that States have a margin of appreciation as regards the means of fulfilment of protective obligations. Where the State's margin of appreciation is correspondingly narrow because it is defined by an absolute right, there is a strong presumption that the positive obligation must be fulfilled through practical, effective and adequate means. This is clearly the case with respect to protection against OCSEA which has repeatedly been held to be a violation of the most fundamental rights guarantees in the international and European human rights orders. While the scope of the State's margin of appreciation in this context is narrow,[184] the ECtHR has not yet required States to adopt a mandatory system of reporting by private parties. Moreover, it is clear from both the ECtHR and CJEU jurisprudence that States cannot be required to negate countervailing rights to privacy and data protection.[185] Member States consequently must find the optimum balance between the respect of countervailing negative rights protections to privacy and data protection, while also fulfilling the minimum standards required by the positive obligations placed upon them.

3.4 Data protection conditions and safeguards

Voluntary detection and reporting of OCSEA by SPs is often characterised as an unlawful restriction of individual privacy and consequently impermissible on data protection grounds under the applicable data protection legislation. While such data processing does indeed constitute a considerable interference with the rights to privacy and to the protection of personal data, this section provides

[178] A and B v Croatia, GC, App No. 7144/15, final 4/11/2019; X and others v Bulgaria, GC, App. No. 22457/16, 2 February 2021.
[179] X and others v Bulgaria, para. 191.
[180] P.I. v Oberbürgermeisterin der Stadt Remscheid, para. 28
[181] La Quadrature du Net and others v Premier Ministre and others, para. 152.
[182] P.I. v Oberbürgermeisterin der Stadt Remscheid, para. 28.
[183] P.I. v Oberbürgermeisterin der Stadt Remscheid, para. 32.
[184] K.U. v Finland, App. No 2872/02, 02 March 2009; Söderman v Sweden, App. N0 5786/08, 12 November 2013; A and B v Croatia, App No. 7144/15, final 4/11/2019; X and others v Bulgaria, GC, App. No. 22457/16, 2 February 2021.
[185] CJEU: La Quadrature du Net and others v Premier Ministre and others; ECtHR: Trabajo Rueda v Spain, App. No. 32600/12, 30 May 2017.

guidance in relation to the data protection conditions and safeguards under which voluntary detection and reporting of OCSEA can be undertaken. More specifically, it will provide guidance on which content (such as images, video and text) or traffic data can be scanned to automatically detect OCSEA and to voluntarily report its instances to the competent authorities in criminal matters and/or to recognised hotlines or other organisations acting in the public interest against OCSEA. The data protection and safeguards hereafter are addressed to SPs as defined in the introduction of this report. This includes communication and SPs, including both providers of the already mentioned NI-ICS as well as intermediaries providing publicly available services relating to the storage, transmission or provision of information through the Internet (such as hosting, mere conduit, (cloud) space for uploading content) (hereafter: SPs). Moreover, and in line with the overall focus of this report, this section focuses on the practice of voluntary detection and voluntary reporting of OCSEA by SPs mainly based on grounds of public interest as described by existing applicable legal frameworks.

3.4.1 Relevant ECtHR jurisprudence on Art. 8 ECHR

Conditions for the lawful use of exceptions were first developed by the ECtHR in cases related to the state surveillance of communications such as in the case of *Malone v. United Kingdom* as to the 'foreseeability of measures',[186] *Huvig v France*, *Kruslin v France* as to the 'sufficiently clear nature of the underlying legislation',[187] *Weber & Saravia v Germany* with respect to 'minimum safeguards',[188] and *Zakharov v Russia* and *Szabó v Hungary* on 'reasonable suspicion', 'strict necessity' and 'judicial authorisation'.[189] In cases such as *K.U. v Finland* 'positive obligations of states' to provide effective means for the protection of individuals against OCSEA was given significant weight in the balance against conditions protecting the confidentiality of communications .[190] In *Trabajo Rueda v Spain*, however, 'disproportionate search and seizure' of OCSEA material was viewed as a violation of Art. 8 and in *Benedik v Slovenia* 'respect for procedural safeguards' as well as on 'admissibility of evidence before a court' was prioritised in relation to the prosecution of OCSEA.[191]

3.4.2 Global Data Protection of the Council of Europe

The following data protection rules and safeguards that service providers can rely upon when voluntarily detecting and reporting OCSEA are based on obligations under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, hereafter: Convention 108), and upon its entry into force, Convention 108 as amended by Protocol CETS 223 (hereafter: Convention 108+) which constitutes as the general data protection framework of the Council of Europe. These are also in line with other potentially applicable data protection frameworks including those of the European Union. The guidelines are only relevant if personal data is actually processed when OCSEA is detected, reported and deleted or for any other compatible subsequent processing. It is important to note that whilst the use of hashing technology for the non-reconvertible

[186] Malone v United Kingdom, App. No. 8691/79, 2 August 1984.
[187] Kruslin v France, App. No. 11801/85, 24 April 1990; Huvig v France, App no. 11105/84, 24 April 1990.
[188] Weber and Saravia v Germany, App. No. 54934/00, 29 June 2006.
[189] Zakharov v Russia, App. No. 47134/06, 4 December 2015; Szabó and Vissy v Hungary, App. No. 37138/14, 06 June 2016.
[190] K.U. v Finland, App. No 2872/02, 02 March 2009. See also section 3.3. above on positive obligations to protect against OCSEA.
[191] Trabajo Rueda v Spain, App. No 32600/12, 30 May 2017; Benedik v Slovenia, App. No 62357/14, 8 April 2015.

pseudonymisation of images and videos is considered an important safeguard - in view of their anonymised comparison with verified child sexual abuse and exploitation material in trustworthy and data quality ensuring repositories or databases - this does not exempt such detection processes from the requirements of data protection law. Hashing is a privacy-preserving technique only, and the very process of anonymisation of personal data such as image and video content involves the processing of personal data, which remains subject to data protection law. In addition, any reporting based on a positive '*hit*' following comparison or based on reasonable suspicion following (AI-based) pattern detection in text or traffic data, using, in some instances, historical data, will involve the transfer of personal data (user or IP information) and thus be subject to data protection law.

Lawful Basis

For SPs in CoE Member States to be able to automatically detect and voluntarily report OCSEA when it involves the processing of personal data, such processing must comply with conditions set forth by Article 8 ECHR as well as with applicable domestic data protection rules, including pursuant to obligations under Convention 108+.

Whilst Article 11 Convention 108+ allows for exceptions to a limited number of data protection principles subject to strict conditions, no derogation is allowed from Articles 5.2 and 5.3 Convention 108+, which require a lawful basis for any envisaged processing.

Whilst Article 5.3 Convention 108+ requires any processing of personal data to occur lawfully, Article 5.2 limits the potential basis for SPs to automatically detect and voluntarily report OCSEA to either (a) the free, specific, informed, and unambiguous *consent* of the users concerned, or some 'other legitimate basis laid down by law', which, according to paragraph 46 of the Explanatory Report to Convention 108+, encompasses, inter alia, data processing (b) for overriding *legitimate interests* of the controller or of a third party or (c) carried out on the basis of grounds of *public interest*.[192]

The three above potential grounds for automatic OCSEA detection and voluntary reporting are assessed on their merits below.

Consent

The question whether SPs may base their processing for the automatic detection and voluntary reporting of OCSEA on mere user *consent*, i.e. by stipulating in their terms and conditions that the user acceptance thereof implies that the latter accepts that communications content or traffic data will be automatically scanned in order to detect possible OCSEA and to report it to the authorities or to recognised hotlines or other organisations acting in the public interest, must be negatively answered. User consent, in order to qualify as a valid basis for processing of personal data, must not only be specific and informed (as may be the case if stipulated as above in the terms and conditions), but must also be *freely* given. According to paragraph 42 of Explanatory Report Convention 108+*, 'consent must represent the free expression of an intentional choice, […] which clearly indicates in this specific context the acceptance of the proposed processing of personal data*', so that *'consent should not be regarded as freely given where the data subject has no genuine or free choice'*. In the case of mandatory

[192] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 223) (henceforth: Explanatory Report Convention 108+), Strasbourg 10.X.2018, para 46.

acceptance of the terms and conditions, there is inherently no genuine or free choice. Moreover, since detected OCSEA would also be reported, either or not through the intermediary of recognised hotlines or other organisations acting in the public interest, to the competent authorities in criminal matters, in order to enable such authorities to investigate and prosecute OCSEA, mandatory user consent is even less acceptable as a legal ground for processing.

Legitimate interest

The answer as to whether SPs can successfully base their processing for the automatic detection and voluntary reporting of OCSEA on 'overriding legitimate interests' (as defined in paragraph 46 Explanatory Report Convention 108+) of either themselves (as data controllers) or of a third party, is more complex.

Whilst the competent authorities in criminal matters to which OCSEA would be voluntarily reported or disclosed, have an interest in receiving such information, their 'third party' interest (to investigate and prosecute) would not easily qualify as a legitimate basis under Article 5.2 of Convention 108+. For this latter case Member States would be better placed processing personal data based on public interest as discussed below.

When it comes to the SP's own legitimate interest, the answer to the question at stake may vary, depending on the domestic rules that apply to them and/or whether they legally qualify as electronic communication SP. In the EU, for instance, electronic communication SP are under a *strict* obligation to ensure the confidentiality of communications content and related traffic data, under Articles 5 and 6 of the e-Privacy Directive, from which *no* derogation is allowed on the basis of their own legitimate interest. In accordance with Article 15 of the e-Privacy Directive, restrictions of their obligations under Articles 5 and 6 are *only* possible based on *legislative* measures adopted by the Member States. Hence, providers under the geographical and material scope of the e-Privacy Directive, which since 21 December 2021 is inclusive of providers of NI-ICS are only allowed to automatically scan for OCSEA and report if they can rely on a legal basis, adopted in the public interest. Such a legal basis must be in pursuit of the objectives, and in line with the specific provisions, of applicable international instruments such as the Lanzarote Convention (discussed below). In cases where SP are under a mandatory obligation to scan OCSEA, the provisions of any such mandatory regime would provide a legal basis.

As a result, only those SP which are not under such strict an obligation, may lawfully base their envisaged automatic detection and reporting of OCSEA on their own legitimate interest, be it under conditions and limitations. Whilst it is a legitimate corporate perspective for SPs to want their services to be free from content and material which they find undesirable, or because they do not wish to facilitate the online availability of such material (which may even go beyond unlawful content, such as OCSEA), this does not provide SPs with an unconditional or unlimited ability to reserve the right (i.e. in their terms and conditions) to automatically scan communications content or traffic data in order to detect such content or material and remove it or, in the case of OCSEA, report it.

Both automatic scanning and reporting are processing operations which, even if performed in the SP's legitimate corporate interest, warrant a balancing test. According to paragraph 48 Explanatory Report Convention 108+, *'what is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each*

instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society'. Paragraph 46 Explanatory Report to Convention 108+, as already stipulated above, is even stricter, in requiring that the legitimate interest of the data controller must be 'overriding', meaning that that it may not be overridden by the interests or fundamental rights and freedoms of the data subject(s) involved, including their right to data protection, privacy and the confidentiality of their correspondence. OCSEA scanning and reporting affects entire user populations, the indiscriminate and generalised monitoring of whose content and traffic data will only stand the balancing test where subject to strict privacy-preserving conditions and safeguards.

Public interest

According to paragraph 47 Explanatory Report Convention 108+, data processing carried out on grounds of public interest should be provided for *by law*, and may, inter alia, be carried out for the prevention, investigation, detection and prosecution of criminal offences, like OCSEA. As mentioned above, a public interest-based legal framework will, for many providers, depending on the domestic rules to which they are subject, provide the strongest lawful avenue for automatic scanning for OCSEA and related voluntary reporting. Hence, CoE Member States are strongly recommended, in line with their positive obligations as established in the jurisprudence of the ECtHR,[193] in relation to Article 3 and 8 ECHR and the protection of children against OCSEA, to establish a bespoke public interest-based framework, enabling SPs to automatically detect and voluntarily report OCSEA under a number of conditions and safeguards. In this context, the Lanzarote Convention could represent shared standards on the definition of such a public interest.

Sensitive data

Where the processing of images and videos for the purposes of detection of OCSEA is revealing of the sexual life/preference of individuals, including of children, such data should be considered to constitute sensitive data. This implies, in accordance with Art. 6 Convention 108+, that such processing will only be allowed where, in addition to the safeguards included in Convention 108+, appropriate safeguards have been enshrined in law. These safeguards should protect against the risks that the processing concerned may present to the interests, rights and fundamental freedoms of the data subjects.

Protection of the interests, rights and fundamental freedoms of children entail that SPs, throughout their activities relating to the automatic detection, removal and voluntary reporting of OCSEA, prevent undue interference with the rights of teenagers featuring in sexually explicit conduct, including to their right to privacy and the exploration of their sexuality as dimensions of their right to private life. Notwithstanding the technological and legal challenges in making qualitative distinctions between images, protection of children's right to privacy should encompass the right to discover their sexual identity in a safe and private environment. Moreover, SPs should protect development of children's sexual identity and experiences, and the privacy of explicit pictures or videos in which children feature themselves and send to peers, or, where they have reached the age of sexual consent under national law, share such material more widely. SPs should also avoid the reporting of solicitation of children to

[193] See section 3.3 above.

the competent authorities in criminal matters where users and those depicted have reached the age of sexual consent under national law.

Further, the comparison of images and videos should avoid using biometric data that are processed through technical and legal means allowing the unique identification or authentication of a natural person. This requires that an assessment is made as to whether the data processed constitutes biometric data.

3.4.3 Conditions and safeguards[194]

Notwithstanding the fact that other important safeguards need to be put in place, such as rule of law, criminal law, and procedural safeguards the below conditions and safeguards are minimum standards on data protection, without prejudice to the full application of Article 8 ECHR and of applicable domestic data protection rules, including pursuant to obligations under Convention 108, and upon its entry into force, Convention 108+.

It must also be noted that, to the extent that the automatic detection and voluntary reporting of OCSEA may be based on legitimate interest (see above), no exceptions to Convention 108+ are allowed. For this particular basis for the data processing, the "balancing test" (i.e. balancing the overriding legitimate interest of the controller with the rights and interest of the data subjects provided that appropriate safeguards have been put in place) should be the rule. Exceptions under Article 11 Convention 108+ will be allowed only if it is set forth by law and only to a limited number of data protection principles. In any case such restrictions should be founded on a public interest framework framed in legislation, have a legitimate aim and constitute '*a necessary and proportionate measure in a democratic society*' as it results from the relevant case law of the ECtHR on data protection.

Strict purpose limitation

According to Article 5 (4) b Convention 108+, any processing of personal data by SPs when scanning communications and related traffic data must be limited to the sole purpose of detecting OCSEA with the aim of its removal and/or the voluntary reporting or disclosure to the competent authorities in criminal matters and/or to recognised hotlines or other organisations acting in the public interest against OCSEA.

[194] Inspired both by Convention 108+ standards and the draft Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online. The suggested conditions and safeguards incorporate text fragments from the draft Regulation, especially the amendments proposed by the LIBE Committee, in its latest version publicly accessible at the time of writing: Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online. State of play of technical meetings with EP and discussion on proposed changes, Brussels, 26 January 2021, 5616/21.

Data minimisation and proportionality

The personal data processed in the detection and voluntary reporting or disclosure used must be minimised to what is strictly necessary in line with Article 5 (4) b Convention 108+ so as to ensure that proportionality as a key principles of data protection is respected.

Data protection by design

SPs, as set forth by Article 10 (2) Convention 108+, shall design the data processing in such a manner as to prevent or minimise the risk of interference with the rights and fundamental freedoms of data subjects. Hence, the technologies they use for automatic detection:

- must be the least privacy-intrusive in accordance with the state of the art in the industry;
- must, where they are used to scan image or video content, preferably use hashing for the non-reconvertible pseudonymisation of images and videos in view of their anonymised comparison with verified child sexual abuse and exploitation material in trustworthy and data quality ensuring repositories or databases;
- may, where they are used to scan communications containing text, not be able to understand the substance of the content but solely to detect patterns pointing to possible OCSEA, using relevant key indicators and objectively identified risk factors;
- must be sufficiently reliable in that they limit the error rate of false positive 'hits' or false positive pattern detection (i.e. where content is wrongly identified as or suspected to represent OCSEA) to the maximum extent possible in accordance with the state of the art in the industry, and, where such occasional errors occur, their consequences must be rectified without delay;
- where technically possible, must not interfere with any communication protected by professional secrecy, such as between doctors and their patients, journalists and their sources or lawyers and their clients.

Impact assessment

SPs shall examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and must have indicated that the intended processing will not result in a high risk to the rights and fundamental freedoms of data subjects or that they have taken measures to mitigate the risk.

Transparency

SPs shall inform the data subjects in their terms and conditions about the restriction of the confidentiality of their communications and related traffic information for the sole purpose of detecting OCSEA in view of its removal and/or the voluntary reporting or disclosure thereof to the competent authorities in criminal matters and/or to recognised hotlines or other organisations acting in the public interest against OCSEA.

In addition, in the event of a positive 'hit' following comparison with verified child sexual abuse and exploitation material in trustworthy and data quality ensuring repositories or databases or in the event

of reasonable suspicion following (AI-based) pattern detection in text or traffic data, using, in some instances, historical data, the data subjects are to be given the following information:

- the competent authorities in criminal matters and the recognised hotlines or other organisations acting in the public interest against OCSEA with whom their personal data have been shared;
- the avenues for redress with the SPs; and
- the possibility of lodging a complaint with the competent supervisory authority and of a judicial remedy, and the identity of those authorities.

Delay of the provision of such information is possible where to do so would be prejudicial to an ongoing investigation, in which case the provision of that information may be delayed to the extent strictly necessary and the data subjects shall be informed without delay after the investigation is closed.

Reporting of OCSEA after automated detection

Since the reporting of OCSEA after automated detection may significantly affect the data subject concerned, no reporting shall be based solely on the outcome of the automated detection process. Hence, SPs must ensure human oversight and intervention for the automated processing of personal data. Moreover, without prior human reassessment and confirmation no positive '*hit*' or reasonable suspicion is to be reported or disclosed to the competent authorities in criminal matters and/or to recognised hotlines or other organisations acting in the public interest against OCSEA.

Data security

SPs shall establish internal procedures to prevent abuse, unauthorised access, use, erasure or transfers.

Limited retention

Where no OCSEA has been detected and confirmed as such, all content data, related traffic data and any result of processing of these data shall be erased immediately after the processing.

Where OCSEA has been detected and confirmed as such, the strictly relevant content data, the related traffic data and personal data generated through such processing, are retained solely for the following purposes and only for the time period that is strictly necessary, after which the data are to be deleted immediately and permanently:

- in order to report and transfer data without undue delay to the competent authorities in criminal matters and/or to recognised hotlines or other organisations acting in the public interest against OCSEA;
- in order to block the account of the user concerned or to suspend a service offered to him or her;
- concerning personal data undoubtedly identified as OCSEA, in order to create a hash for future comparison;
- for the purpose of enabling complaints and the pursuit of judicial and non-judicial sanctions and/or remedies.

Effective complaint mechanism and remedies

Without prejudice to their right to remedies for any violation of data protection rules, users who have been adversely affected by the use of specific technologies for the processing of personal data to detect and remove or report OCSEA shall be able to submit a complaint against the action of the SP and have the right to an effective remedy where the material removed or reported does not constitute OCSEA. Hence, SPs shall establish effective and accessible complaint mechanisms and the Council of Europe member shall put in place effective procedures for remedies, including the cases where:

- the users' content has been removed or their account has been blocked or a service offered to them has been suspended;
- the users' content or identity have been reported to the competent authorities in criminal matters or to a recognised hotline or other organisation acting in the public interest against OCSEA.

Transborder flows of information

Throughout the process of automatic comparison of scanned image or video content with external repositories or databases and/or the reporting or disclosure of OCSEA to the competent authorities in criminal matters and/or to recognised hotlines or other organisations acting in the public interest, SPs should fully respect the applicable conditions for transborder flows of personal data, such as those laid down in Chapter III of Convention 108+.

This implies that SPs could rely on Article 14 of Convention 108+ once the amending Protocol CETS No 223 enters into force and send personal data without any additional conditions to other Parties to that Protocol if none of the exceptions under Article 14.1 applies for that particular data transfer. As this is unlikely to happen in the immediate future and certainly not before 2023, and still then probably not for every major jurisdiction involved in data transfers for OCSEA purposes, Article 14.3 Convention 108+ could also play a role for a SPs wishing to send personal data to another state or jurisdiction.

While not being yet binding, 'an appropriate level of protection based on the provisions of this Convention is secured' during the transfer and in the receiving state which should give enough reassurance to any private party in order to cooperate and send data through one of the methods described below. According to Article 14(3) of Convention 108+, 'an appropriate level of protection can be secured by: a) the law of that State or international organisation, including the applicable international treaties or agreements; or b) ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing'. Consequently, further efforts would be required in assessing and, where applicable, developing such interim safeguards.

The terms and conditions of Article 14 of the second additional Protocol to the Budapest Convention (as described in section 3.3.1 above) could also play a pivotal role when deciding on condition a) (i.e. whether the law of a country affords an appropriate level of protection for individuals during cross-border data transfers). In line with Convention 108+ - and especially its first exception regime described in Article 11.1 - as well as the data protection regime of the European Union and State Parties to the Budapest Convention (including the US, Canada, Australia and Japan, etc.), those terms and conditions could be looked at when States are engaging in criminal justice cooperation which also involves the handling of electronic evidence, while aiming to ensure an appropriate level of protection during the transfer of data between authorities regarding specific ongoing investigations that concern already

available data often held by SPs. The second additional Protocol to the Budapest Convention is due to be open to signature in Spring 2022. The transfer regime it would provide upon its entry into force would presuppose for SPs that the country they are established in takes a range of measures, including legislative measures, upon ratifying it and that they continue to comply with data protection regulations of that country. Therefore, it is likely that condition b) (i.e. when the appropriate level of protection is guaranteed via ad-hoc or approved standardised legally binding safeguards) is going to be used by private entities for some time.

In order to assist them in assessing the level of protection that a state or an international organisation could guarantee via its legislation, interested stakeholders could be encouraged and supported to develop 'data importer registries' and 'country report hubs' which are already in use or being developed by global private and public entities. Such tools include lists of countries based on thorough legal assessment to where personal data could be sent without lowering the level of the protection of personal data that is afforded in the country where the SP is established or provides services. Public body assessments, such as the adequacy decisions of the European Commission or the assessments carried out by the Committee of Convention 108 vis-à-vis countries requesting accession to Convention 108 or in the future requesting an evaluation of their level of protection pursuant to Article 23 e and f, could also be used as guides.

In terms of complying with condition b) of Art. 14 (3) Convention 108+, several options are already available and could give guidance on how to transfer personal data from one jurisdiction to another with respect to the level of protection already afforded, *inter alia*: the Standard contractual clauses (SCC) for data transfers between EU and non-EU countries which can also be safely used in a non or non-exclusively EU context; and the standards under Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures both adopted by the European Data Protection Board (EDPB).

Both the SCC's and the Recommendations, however, need to be assessed in light of the decisions of the CJEU decision in *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems ("Schrems II")*[195]. The *Schrems II* decision, while invalidating the bilateral transfer instrument between the European Union and the US for a second time, touches upon two specific requirements. The first is the need for legal remedies, i.e. effective and enforceable rights of individual redress, in front of an independent and impartial court. The second, regarding the scale of certain surveillance programmes, is the absence of limitations on the access by State authorities to personal data, thereby infringing the principle of strict necessity. In light of the judgment a new, more durable and sustainable agreement is being negotiated between the European Union and the US which could also have an impact on data transfers for the purpose of OCSEA and has already had direct consequence on the updated SCC recently published by the European Commission on 4th June 2021[196]. Moreover, this decision also prompted the EDPB to summarise the essential requirements that a data controller needs to observe when transferring personal data from the European Union to a non-EU Member States. This contains very similar conditions to those set forth by Article 11 Convention 108+ that is based on the preceding jurisprudence of the ECtHR explained above.

[195] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Case C-311/18, 16 July 2020.
[196] Standard contractual clauses for international transfers | European Commission (europa.eu)

Some of the models that have been developed (and published) within the industry, such as the practice of 'Data transfer impact assessments' would also need further attention. The full methodology of such assessments cannot be described here, but some of their key elements could serve as a basis for further reflections. These usually recommend, after mapping out all transfer operations, technical solutions as safeguards additional to those already applied to the transfers (in relation to data security, data quality, transparency, appropriate legal basis, due care of sensitive data, accountability requirements, etc). Examples of such solutions include encryption with the key held by the personnel of the sending country, and bringing strategic transfers onshore. In addition, the assessments usually recommend the elaboration of the company's Binding Corporate Rules in order to be validated by the local Data Protection Authority and *in fine* by the EDPB. Finally, as a long-term solution, the assessments recommend arranging for local data storage and local hosting to use more subtle technical solutions such as cloud services facilitated by providers in the same jurisdiction, blockchain, data fiduciaries, data trusts, etc.

3.4.4 Implications for this report

The automated detection and voluntary reporting of instances of OCSEA impacts upon the confidentiality of communications content and related traffic data, which SPs must ensure. It constitutes an interference with the right to private and family life and protection of personal data of the persons involved, i.e. the users, including potential offenders, as well as children featuring in OCSEA, which must also be able to confidentially communicate with a trusted adult, organisations active in the fight against child sexual abuse or exploitation, and their lawyers.

Whilst the use of hashing technology for the non-reconvertible pseudonymisation of images and videos - in view of their anonymised comparison with verified child sexual abuse and exploitation material in trustworthy and data quality ensuring repositories or databases - is considered an important safeguard, it does not exempt such detection process from the requirements of data protection law. Hashing is a privacy-preserving technique only, and the very process of anonymisation of personal data such as image and video content involves a processing of personal data, which remains subject to data protection law. In addition, any reporting based on a positive '*hit*' following comparison or based on reasonable suspicion following (AI-based) pattern detection in text or traffic data, using, in some instances, historical data, will involve the transfer of personal data (user or IP information) and thus be subject to data protection law.

4. KEY CONCLUSIONS AND RECOMMENDATIONS

More than twice as many types of sexual exploitation and sexual abuse of children exist today when compared to the late 90's. The prevalent use of information and communication technologies (ICTs) give rise to a situation in which children may be exposed to many of the same risks online as they are offline. The call for a concerted action to protect them from OCSEA is even stronger in light of the influence of the COVID-19 pandemic on the main threats behind OCSEA.

> ***Recommendation 1: Successful prevention and combating of the current forms of OCSEA require State actors to stay up to date and react to constant technological developments in this area, facilitated especially by the prevalent use of continuously evolving ICTs. The use of automated technology in the fight against OCSEA is, in this regard, essential.***

There is an existing discrepancy between the use of automated detection technologies and the publicly available level of information on their adoption. This insufficient level of information makes it difficult for policymakers and regulators to develop a proper opinion on how to regulate these technologies and suggest adequate safeguards.

> ***Recommendation 2: To ensure a proper balance between privacy and protection of children against sexual exploitation and abuse fostering a dialogue between private sector companies and policymakers/regulators is of the utmost importance. Such dialogue should primarily aim at securing adequate transparency on the choice of the technology used and processes around its use.***

The present, insufficient level of transparency on the quality and size of hashlists of known CSAM limits to some extent the potential of a technological solution in relation to the swift removal of such material.

> ***Recommendation 3: Initiatives aiming at improving coordination in this area should be indicated and supported as they are vital to the reliability of the reference databases. In this regard, it is also necessary to secure more clarity on how the accountability mechanisms are managed, including the recruitment and training of individuals employed by private sector companies who are responsible for the assessment of illegal content, such as CSAM.***

When it comes to defining safeguards, a well-tested, well-documented and stable technology is a safer choice for policymakers and regulators. However, to address current challenges in regards to OCSEA it may be advisable or necessary to use more powerful technologies in an early phase of their development.

> ***Recommendation 4: To better maintain a balance between privacy and protection of children against sexual exploitation and abuse, defining the proper level of safeguards should take place as early as possible in the process of development of technology. Policymakers and regulators should place particular focus on the dataset used by that technology to train complex combinations of algorithms.***

Each OCSEA detection tool is different and has its own objectives. Identifying the least restrictive means of detecting OCSEA requires a very precise understanding of the objective and the environment for which any technology will be selected.

> ***Recommendation 5: In order to enhance privacy while prioritizing protection of children against sexual exploitation and abuse it is necessary to promote technological solutions that are the most efficient for the purpose considered.***

The limited number of experts across different subject areas leads to discussions taking place in silos whereas the debate around the controversy surrounding the EC proposal highlighted the need for proposals for powerful system solutions aimed to prevent and combat OCSEA.

> ***Recommendation 6: Initiatives oriented at cross-sectional dialogue should be identified and supported.***

It is worth noting the considerable weight given by relevant international bodies, the European Court of Human Rights and the Court of Justice of the EU to the need for protection from sexual offences against children, as well as the Lanzarote Convention and CSEA Directive, when reconciling child protection and data protection rights.

> ***Recommendation 7: The weight that is accorded to positive obligations against OCSEA under international and European human rights law, bearing in mind the best interest of the child, needs adequate appreciation in the legislative debate going forward.***

The still evolving laws which are currently governing automated detection technology do not adequately address the challenge of preventing and protecting children from OCSEA while ensuring maximum privacy in online communication.

> ***Recommendation 8: Acknowledging the current legal lacunae, consideration should be given by CoE Member States to the need for a harmonised and sustainable legal framework which can provide legal certainty to SPs and address future technological developments.***

The analysis of CoE data protection treaty norms, in light of applicable ECtHR jurisprudence, concludes that a bespoke public interest-based legal framework will provide the strongest lawful avenue for automatic scanning for OCSEA, related voluntary reporting and transborder flows of personal data, and that the Lanzarote Convention could represent shared standards on the definition of such a public interest.

> ***Recommendation 9: The CoE Member States are strongly encouraged, in line with their positive obligations to protect children against OCSEA, to establish a public interest-based framework grounded in the Lanzarote Convention, enabling SPs to automatically detect, remove, report and transfer OCSEA-related information under data protection and privacy conditions and safeguards listed in section 3.4.***

5. GLOSSARY

AI – Artificial Intelligence

CoE – Council of Europe

CSAM – Child Sexual Abuse Material

CSEA – Child Sexual Exploitation and Abuse

CV – Computer Vision

DL – Deep Learning

EC – European Commission

EDPS - European Data Protection Supervisor

EECC - European Electronic Communications Code

EESC - The European Economic and Social Committee

EOKM - Expertisebureau Online Kindermisbruik

EP – European Parliament

EDPB – European Data Protection Board

ESN – European Service Network

SPs –Service Providers

EUROPOL - The European Union Agency for Law Enforcement Cooperation

FH – File Hashing

HCS – Hash Check Service

ICCAM - I see Child Abuse Material

IP – Internet Protocol

ICCAM – I see Child Abuse Material

ICSE - International Child Sexual Exploitation image and video database

ICTs - Information and Communication Technologies

INHOPE - International Association of Internet Hotlines

INTERPOL – The International Criminal Police Organization

IOCTA - Internet Organised Crime Threat Assessment

IWF - Internet Watch Foundation

LCt – Lanzarote Committee

LC – Lanzarote Convention

LIBE - The Committee on Civil Liberties, Justice and Home Affairs

ML – Machine Learning

MVNO - Mobile Virtual Network Operator

NCMEC - National Center for Missing & Exploited Children

NI-IC - Number-Independent Interpersonal Communications

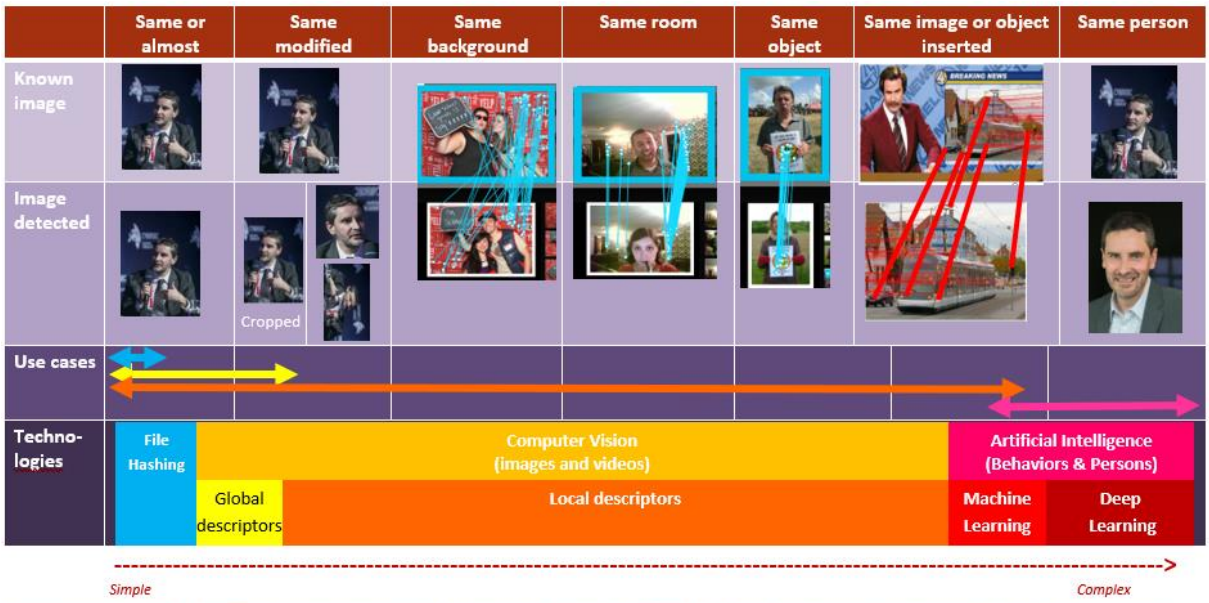
OCSEA – Online Child Sexual Exploitation and Abuse

OPSC - Optional Protocol to the UNCRC on the Sale of Children, Child Prostitution and Child Pornography

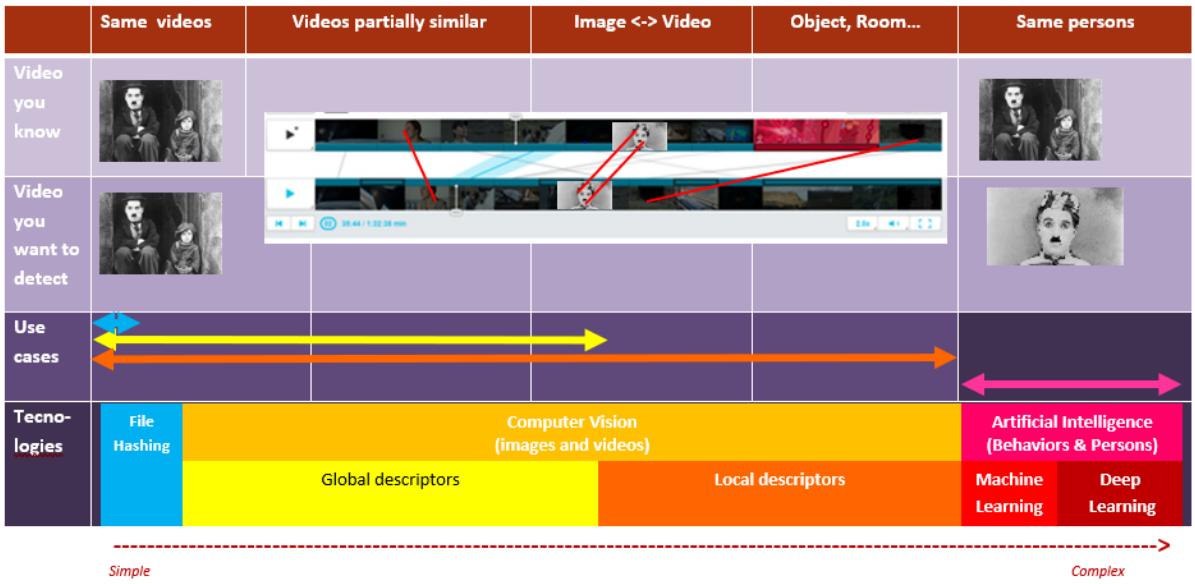
OTT - Over the Top communication services

6. ANNEX

1. Simplified overview on technologies to detect visual content in images and videos.



How to read this diagram: File hashing technology applies only to detect the same file, this is why the arrow in blue applies only to detect "same or almost". As the file hashing technology cannot detect images with minor changes (change of 1 pixel), the arrow is short. "Global descriptors" applies well to detect same images and can also detect images with partially the same content. "Local descriptors" is efficient to detect all the scenarios (same, similar, modified etc.). "Artificial intelligence" can cover many use cases, more than what is shown on this diagram, but it is also more complex to use than computer vision technology.



How to read this diagram: Same as in section 3. The range of application of each of these technologies is indicative. Also, the range is not indicative of the level of adoption. For instance, file hashing is shown with the smallest range on this table, but it is in practice much more broadly used than the other technologies.

2. Additional sources:

- https://www.culture.gouv.fr/ or https://bit.ly/3vWJRip - a report published in 2020 by the French Ministry of Culture in the context of the Copyright Directive, establishing that computer vision is a mature and affordable technology for organisations of all sizes;
- Guidelines Regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, specific provisions on 'data collection' and 'prevention':

- **B Data collection**
- 20. The Committee urges States parties to develop and implement a comprehensive and systematic mechanism for the collection, analysis, monitoring and impact assessment of data, as well as for its dissemination, on all issues covered by the Optional Protocol.
- Importantly, data collection should be coordinated between all relevant stakeholders, including the national statistical bureau and child protection entities, and data should be centralized to avoid incoherent or contradictory data between different State agencies. The Committee recommends, in particular, that States parties:
- (a) Implement a disaggregated approach to data, addressing how these offences affect different groups of children. At a minimum, data should be disaggregated by sex, age and form of exploitation;
- (b) Collect data on how children access and use digital and social media and their impact on children's lives and safety, and on factors that affect children's resilience as they access and use ICT;
- (c) Collect data on the number of cases reported, prosecutions, convictions and sanctions, preferably including redress provided to victims, disaggregated by the nature of the offence including with regard to online and offline activity, the category of perpetrator and the relationship between the perpetrator and the victim, and the sex and age of the child victim;
- (d) Develop common indicators and a standardized data collection system if data are collected at the regional or local levels (for example, municipalities).
- 21. All data should be collected with due respect for children's right to privacy.

- **C. Prevention of online sale and sexual exploitation of children**
- 37. States parties should prevent and address online sale, sexual exploitation and sexual abuse of children through their implementation measures. National legal and policy frameworks should be assessed to ensure that they adequately cover all manifestations of the sale, sexual exploitation and sexual abuse of children, including when these offences are committed or facilitated through ICT.
- 38. Online-specific analyses, research and monitoring should be conducted to better understand these offences, and responses to online offences should be developed in close collaboration with the relevant industries and organizations.
- ….
- 41. Considering that child sexual abuse material, such as images and videos, can circulate indefinitely online, the Committee alerts States parties to the fact that the continuous circulation of such material, in addition to perpetuating the harm done to child victims, contributes to a perception of the child as a sexual object and risks strengthening the belief among persons with a sexual interest in children that it is "normal" since many others share the same interest. The Committee therefore urges States parties to ensure that Internet service providers control, block and remove such content as soon as possible as part of their prevention measures.
- 42. The Committee draws States parties' attention to the need to address "sexting" by children, whereby self-generated sexual content is sent via mobile phone to others. Sexting often appears to be a product of youth peer pressure and, to a certain extent, teenagers increasingly consider sexting to be "normal". While this conduct in and of itself is not necessarily illegal or wrongful, it involves a number of risks. Sexualized images of children can easily spread online or offline beyond or against the will of the child, can be very difficult to remove and can be used in the context of bullying and for sexual extortion, which can have serious and traumatizing consequences for children, including suicide. This complex issue needs careful attention, and the Committee encourages States parties to establish clear legal frameworks that protect children and, through prevention efforts, ensure that they are educated about and made aware of the gravity of spreading images of others and of oneself.

- The Digital Environment Recommendation (CM/Rec(2018)7, Paras 51 – 66.) includes the following 'measures regarding child sexual abuse material':

Measures regarding child sexual abuse material

61. Policing with respect to child sexual abuse material should be victim-focused with the highest priority being given to identifying, locating, protecting and providing rehabilitative services to the child depicted in such materials.

62. States should continually monitor whether and how child sexual abuse mate- rials are hosted within their jurisdiction and require law-enforcement authorities to establish databases of "hashes",[2] with a view to expediting actions to identify and locate children subjected to sexual exploitation or abuse and apprehending perpetrators.

63. States should engage with business enterprises to provide assistance, including as appropriate technical support and equipment, to law-enforcement authorities to support the identification of perpetrators of crimes against children and collect evidence required for criminal proceedings.

64. Mindful of available technologies and without prejudice to the principles of liability of internet intermediaries and their exemption from general monitoring obligations, States should require business enterprises to take reasonable, pro- poportionate and effective measures to ensure that their networks or online services are not misused for criminal or other unlawful purposes in ways which may harm children, for example in relation to the production, distribution, provision of access to, advertising of or storage of child sexual abuse material or other forms of online child abuse.

65. States should require relevant business enterprises to apply hash lists with a view to ensuring that their networks are not being misused to store or distribute child sexual abuse images.

66. States should require that business enterprises and other relevant stakeholders take promptly all necessary steps to secure the availability of metadata concerning any child sexual exploitation and abuse material found on local servers, make them available to law-enforcement authorities, remove these materials and, pending their removal, restrict access to such materials found on servers outside of their jurisdiction.