BRIEFING

European Parliament

Curbing the surge in online child abuse

The dual role of digital technology in fighting and facilitating its proliferation

SUMMARY

The volume of child abuse materials circulating on the internet has increased dramatically during the pandemic, as both children and child sex offenders spend more time, and interact more, online. Enabled by digital technologies, child sex offenders have tapped into opportunities that were previously unavailable to communicate freely and directly with each other and with children, creating online communities where they share their crimes. Today, they can reach children via webcams, connected devices and chat rooms in social media and video games, while remaining anonymous thanks to technologies such as cloud computing, the dark web, end-to-end encryption and streaming. There has been a rise in grooming and sextortion incidents.

Conversely, it is again digital technologies, such as artificial intelligence (AI) and improved online age verification methods or age-appropriate design, which can help to curb the surge of the above crimes. Due to its capacity and speed of analysis, AI could play an important role in tackling the problem and assisting law enforcement in reducing the overwhelming amount of reports that need to be analysed.

This is one of two EPRS briefings on the subject of fighting online child abuse. This one looks at technological aspects while the second one will cover legislative and policy issues.

In this Briefing

EPRS | European Parliamentary Research Service

Author: Mar Negreiro
Members' Research Service

PE 659.360 – November 2020

EN

A worsening online threats landscape

Over the past 20 years, online child sexual abuse has increased dramatically worldwide. The United Nations (UN) estimated about a decade ago that at any given time there were over 750 000 child sex offenders searching for child sexual abuse material (CSAM) online. Nowadays the Internet Watch Foundation (IWF) estimates that there are at least 1 million of them. As for CSAM, quantifying its precise volume is difficult, as there are numerous ways in which it can be distributed online, and knowledge about its existence – a fraction of what is really out there – is obtained from reports provided by the tech industry, and also by NGOs, users and hotlines on a voluntary basis. Yet hotlines remain predominantly reactive to reports they receive. A very small number of hotlines (four[1]) engage in proactive search for CSAM online themselves. According to the IWF annual reports, compared to the 1 million reports of CSAM worldwide in 2010, in 2019 the number had jumped to 17 million in 2019, including nearly 70 million images and videos.

Most of these reports are submitted by Electronic Service Providers (ESPs) that find CSAMs with the help of technology, or by their users (who are often the victims of online child abuse themselves). In the US, once companies have removed such content, they report it to the US-based non-profit National Center for Missing and Exploited Children (NCMEC), as required by US federal law.[2] However, they do not have to notify cases and data to the police or prosecutors in the child sex offenders' country of origin. The NCMEC then makes these reports available, on a voluntary basis, to law enforcement agencies around the world to aid with investigations and prosecutions. Thus, the NCMEC is a key source in the provision of CSAM reports worldwide, including for EU countries. In the EU, companies are not obliged to do this by law. In fact, according to the Irish hotline, 80 % of the tips they receive about CSAM in Ireland are from the NCMEC. In the UK, 2 500 persons were arrested in 2019 thanks to NCMEC reports.

For the EU as a whole, the NCMEC has noted an increase in child sexual abuse online: from 23 000 in 2010, reports have jumped to more than 725 000 in 2019, with over 3 million images and videos. That was before the onset of Covid-19; the situation has since deteriorated, with higher peak levels.

The EU hosts most of the CSAM worldwide

According to the IWF, over the past five years the EU has become the largest host of CSAM globally. Already in 2016, most child sexual abuse webpages assessed were hosted in the EU. Since then, this trend has only become worse: about 80 % in 2018 and almost 90 % in 2019 of all known URLs containing child sexual abuse material were hosted in Europe. North America comes second in this regard, having hosted 9 % of all known child sexual abuse URLs in 2019, a drop from 18 % in 2018.

Within the EU, the Netherlands accounts for most of the hosting; over a single year, the relative amount of CSAM in this country almost doubled, from 47 % of the total detected globally by the IWF in 2018, to 71 % in 2019. The Dutch hotline and Dutch hosting companies have been asked to remove 94 000 webpages in the past year alone. Given the fact that each webpage can accommodate hundreds of individual images, this equates to millions of individual images. Until now, hosting companies in the Netherlands could refuse to take remedial action regarding illegal content without a court order, but this loophole in the Dutch legal system may soon close thanks to new legislation in the pipeline.

Peak levels reached during lockdowns

The coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation of societies around the world. Yet, it has also exacerbated existing problems, such as the digital divide, and contributed to a global rise in cybersecurity incidents. During this unprecedented situation, there has been an increase in malicious cyber-activity across Member States, as revealed by a recent Europol report. Unfortunately, this has also resulted in an alarming increase in demand for CSAM.

Schools in a majority of countries worldwide have temporarily closed down. According to the latest available data from Unesco, this has affected 1.57 billion pupils in more than 190 countries worldwide, or more than 90 % of the total number of students globally. As a result, the number of children using the internet to attend school remotely has risen exponentially. Social media platforms too have recorded historic levels of usage by online participants, including children.

The pandemic has created a unique situation that has seen both child sex offenders and minors spending more time online. Despite the dramatic rise in the use of the internet by young children, awareness of the potential risks remains low and cases of online sexual abuse and exploitation have increased significantly. In the first quarter of 2020, the NCMEC became aware of child sex offenders' online postings in forums, openly discussing the pandemic as an opportunity to entice unsupervised children into producing sexually explicit material themselves while in confinement at home.

At the same time, there has been an explosion in reporting to hotlines, from both the public and electronic service providers. The NCMEC recorded an over 90 % increase in online reports between the first half of 2019 and the first half of 2020. In March 2020, Spanish hotlines received a record amount of calls reporting child sex abuse compared to the same period in other years, according to Europol.

As a result of travel restrictions and other measures during the pandemic preventing them from travelling to pursue their crimes, child sex offenders have had to resort to exchanging CSAM online, and not just images or videos. According to Europol, there has been an increase in web-streaming of sexual abuse, including on demand, against children and vulnerable communities. Assuming the false identity of children, child sex offenders (and other offenders) often establish contact with real children on social media or in online video games with chat rooms. Once they have won the children's trust (*groomed* them), they can then abuse them sexually online. Another related phenomenon, *sextortion,* where *children are extorted into producing and sharing sexual images or videos of themselves,* has tripled since March 2020 in many countries. The cyber-trafficking of children is also on the rise.

The IWF has warned that the number of child sexual abuse images being removed globally has fallen by 89 % during the pandemic, as, while internet traffic has grown exponentially, many organisations have been working with limited capacity. According to Europol, the volume of online CSAM in the EU has become simply unmanageable for many of the law enforcement units dealing with it. This ongoing increase reflects the continuous distribution and redistribution of CSAM content.

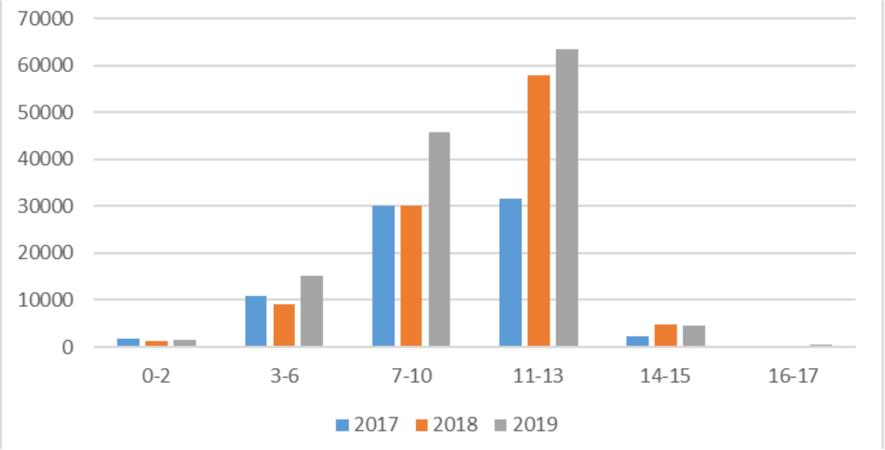
According to the WePROTECT global alliance, governments' and law enforcement' focus on Covid-19 and the disruption caused by the associated protective measures have led to a lower prioritisation of the fight against online child sexual exploitation in many jurisdictions worldwide.

How technological development is helping child sex offenders

During the 1990s and early 2000s, the data transfer capacity for accessing and sharing online CSAM was lower, given the slow internet narrowband connectivity. Yet, it provided the first evidence that the internet was going to create new types of risks to children. Some of the technologies used back then included emails, search engines, instant messaging and peer-to-peer file-sharing. It was more difficult for child sex offenders to get in contact with one another and directly approach children online anonymously. Moreover, very few children were using the internet on a regular basis.

However, as faster broadband connections and mobile devices have become accessible to more and more people, and social media platforms have gained global popularity, CSAM has increased in volume, given that child sex offenders now have more technical possibilities to produce and share it with each other. In addition, CSAM distributors are targeting mainstream platforms to reach wider audiences. Moreover, research from the UK National Crime Agency (NCA) found that one can find child exploitation images within three clicks when using mainstream search engines. Prior to the internet, child sex offenders had operated mainly in isolation; today, they have a host of opportunities to communicate with each other online. Moreover, not only is the scale of CSAM crimes getting greater, it is also getting more severe, as increasingly younger children are being exploited. IWF estimates from 2019 show that 46 % of the child sexual abuse material contained in the external sources' reports assessed by the foundation depicted children aged 10 or under; more than 40 % of this imagery was in the most serious categories of abuse– A and B.[3]

Figure 1 – Number of children aged 0-17 appearing in IWF reported imagery (2017-2019)



Source: IWF 2019 Annual Report (p. 47).

Studies have shown a strong correlation between those downloading such material and those who are abusive offline. According to the police, over half of those who consume online CSAM admit to abusing children physically offline. Furthermore, some 80 % of the offenders abuse children with whom they have a close relationship.

Some of the developments that have facilitated this global surge in online CSAM are described below.

Lack of online verification systems to assess the real age of participants

Children use the internet avidly, and most of them use it on a regular basis and access it from an increasing variety of places and devices, not always under the supervision of an adult. According to Unicef, one third of all internet users are children, and at least 800 million of those are online social media users.

The internet brings children many opportunities to learn, be creative and have fun, but it is also a source of threats, as young children have limited or no perception of online risks. A McAfee study in India found that 70 % of youngsters posted their personal details on the internet, making them an easy target for cybercriminals. Many are using apps that use their phone's location settings.

Among children's favourite online activities are online watching and sharing of videos (often their own), participating in online social media platforms and playing online games,[4] where they communicate with other known and unknown users and players. Most platforms allow children above 13 years old to use them. In the EU, since the updated General Data Protection Regulation (GDPR) came into effect, this age has been increased to 16 years.[5] However, social media platforms have limited possibilities to perform age control; what is more, children under the age of 13 are increasingly accessing the internet through, among other things, mobile devices, and children as a whole are increasingly spending more time online, about twice as much as in 2010.

A study by Ofcom, the UK telecoms regulator found that children are using a wider range of social media platforms than ever before and are spending an increasing amount of time on them. WhatsApp in particular, despite the minimum age limit of 16 for its users, has grown in popularity among 12-15 year-olds since 2019. Almost half of parents are aware that WhatsApp has an age requirement, but only 5 % are aware that 16 is now the required age. YouTube remains the top platform used by children, with more than two-thirds of 8-15 year olds using it.

Social media platforms have been shown to have insufficient age verification procedures, allowing predators access to children. Most child-grooming offences in England and Wales are committed over Facebook-owned applications. Worldwide in 2020, Facebook owns four out of the five most downloaded and most used apps. All top five apps are social or communication ones. Nearly 70 % of millennials have said that social media apps are among their most commonly used ones, and smartphone users between the ages of 13 and 24 are the heaviest mobile app users.

A recent UK inquiry report has called on the UK government to introduce legislation to compel the companies to adopt more effective checks to deter under-age users. In many cases, the only test is to require users to fill in a date-of-birth form, which is easy to falsify.

A study in Ireland has shown that more than 90 % of children aged 8 to 12 own a device that can connect to the internet, and most have been contacted by strangers online. It has also found that 65 % of pre-teenagers are on social media despite an age limit of at least 13 on most popular platforms and a digital age of consent set at 16 by Irish law.

Given the scale of online CSAM, some argue that companies should take reasonable steps to easily and effectively identify the children among their users, and adopt enhanced measures for protecting these children from offenders. They could also design *high privacy by default* settings for children, such as those included in a recent UK code[6] on age-appropriate design listing recommendations for online service providers. The guidelines from the International Communications Union (ITU) also call for a global standard for children's privacy online.

A recent global survey on online violence shows that more than half of teenage girls have been harassed or abused online mainly in social medial platforms, with 50 % saying online harassment is more common than street harassment.

Likewise, children can easily be exposed to adult material online, where access may be unrestricted (for example, 23 of the top 25 adult websites visited by UK users provide instant, free and unrestricted access to hard-core pornographic videos). Yet, parental supervision and monitoring of children's online activity is not that common at present. In fact, in many countries it is children who help their parents in solving problems related to their online use or their mobile devices, which is a clear example of the digital skills generational gap between them.

Both France and Italy are introducing nationwide age verification systems for pornography websites. In the UK, a similar system had to be withdrawn due to privacy concerns. YouTube too announced in September 2020 its new system for verifying age in online adult content.

More broadly, the European Council in its conclusions from 1 and 2 October 2020 has asked the European Commission to introduce an EU-wide digital ID system by 2021, requiring identification for the use of public and private online services. In response, the Commission is planning to introduce a proposal for a regulation in the first quarter of 2021.

Digital technology that help child sex offenders stay undetected

According to Europol, child sex offenders use defensive forensic measures including anonymisation and encryption of their illegal online activities to evade law enforcement. Studies and reports on online child sexual exploitation confirm that current offenders show a much higher degree of computer literacy and forensic awareness. They often forensically clean their devices, making detecting their offences more difficult, and use precautions: password protection, IP masking, evidence elimination, hard drive partitioning and locking of portable hard drives and thumb drives.

On the other hand, some national investigation teams lack the necessary technological knowledge and tools to deal with situations such as detecting CSAM among a vast number of seized photos or videos, locating victims or offenders, or conducting undercover investigations in the dark web or in peer-to-peer networks, despite the fact that abuse, harassment and some of the most serious illegal activity towards children occur in private spaces, such as hidden online community forums.

Encryption

The introduction of end-to-end (E2E) encryption systems is beneficial in ensuring privacy and security of communications. Therefore, there is a general trend in recent years for online community forums, chat rooms and messaging apps to E2E encrypt their communications to allow the highest privacy levels for their participants and make them more resilient to cyber-attacks.

Yet, E2E encryption also gives offenders easy access to secure channels where they can hide their actions, such as trading images and videos, from law enforcement. Nearly half of the police officers polled in a survey considered that encryption is the biggest challenge they face in child sexual abuse investigations. Europol's 2020 cybercrime report highlights encrypted communication as the one issue that has for a number of years frustrated police investigations, and that encryption is easy to use even by less tech-savvy offenders. The report finds that CSAM distribution and sharing among larger groups takes place on social networking platforms and E2E encrypted communication applications such as WhatsApp, which protect CSAM data during their transmission and storage by default. This happens even though Facebook, which owns WhatsApp, bans approximately 250 000 WhatsApp accounts a month for sharing child exploitation images, just by proactively looking into the non-encrypted part of WhatsApp, such as scanning the public profile photos for known CSAM.

Facebook has announced its plans to introduce E2E encryption by default in its instant messaging service. This could reduce dramatically the number of total reports of child sexual abuse globally, as it is among the most active ESP company in reporting CSAM. In 2019, it sent almost 16 million reports to the NCMEC (94 % of the total that year), while other US-based companies sent fewer than 1 000 reports, and some, such as Amazon, fewer than 10. More than 100 child protection organisations have urged Facebook to halt plans for strong E2E encryption, saying this would allow predators to operate even more freely. Moreover, seven countries[7] whose total population represents a fifth of Facebook's users across the world, have issued an international statement asking, among other things, social media platforms to reconsider how they implement E2E encryption to safeguard child safety online.

Some argue that E2E encryption might solve another growing problem for social media platforms. As countries demand that these platforms take responsibility for preventing not only illegal but also other harmful online content, platforms might see E2E encryption as a solution; as companies cannot moderate encrypted online content and be liable for it if they cannot technically access it. Some see this as one of the reasons why social platforms want to promote E2E encryption, in addition to improving the privacy of its users. Conversely, industry representatives and civil society groups have expressed concern that to avoid E2E encryption, platforms could take steps that create unacceptable, negative impacts on users' privacy, as a way to provide proactive moderation of private online spaces.

Another related issue is the definition of what constitutes a 'private communication' today. Traditionally, private communication included mainly one-to-one phone calls or messages. Today, social media platforms enable many participants to take part in an online videoconference or group chat, sometimes involving hundreds of users. Videoconference companies such as Zoom have been obliged to introduce greater protection, including E2E encryption, after suffering 'Zoom-bombings', where hackers or trolls hijacked Zoom group video calls. Many of those took place while online remote school classes were taking place during lockdown.

The UK inquiry report mentioned above highlighted the good practices of French app Yubo whose algorithms detect possible instances of child nudity during live streaming, which are further analysed by a human moderator. It also uses artificial intelligence to verify the age of child users.

As part of the EU internet forum, the European Commission has launched an expert process with industry to map and preliminarily assess E2E encrypted electronic communications, to explore whether there are technical solutions that allow for the detection of CSAM while maintaining the same or comparable benefits of encryption, and to address regulatory and operational challenges.

In the US, new legislation – Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) – is currently being prepared, which could result in the user privacy and security guaranteed up to now by digital platforms being undermined, as it might also affect E2E encryption, according to a coalition of tech companies and fundamental rights organisations. According to experts, preserving the confidentiality of E2E encrypted messaging services, while still allowing for the automated scanning of CSAM, is a very difficult problem to be resolved in the short term.

More broadly, encryption is a security tool that is not only used for private chats and videoconference communications. While this section focuses on the challenges posed by E2E encryption for law enforcement, other encrypted services available, including device encryption, encrypted applications and encryption across integrated platforms (see next section) also place limitations on its activities. The report of Europol's observatory function on encryption identified in a broader sense the latest developments for hiding CSAM materials likely to have an impact on law enforcement's access to data. Other areas of technological development are also expected to decrease access to data and evidence for law enforcement authorities even further, because access becomes more complicated: examples include domain name services (DNS) and 5G, the fifth generation of mobile communication. The European Commission is working alongside Europol and the EU Member States to identify appropriate ways of preserving lawful interception capabilities in 5G networks.

The dark web, livestreaming and the internet of things

The 'dark web,' also known as the 'dark net,' is part of the greater 'deep web', a network of secret websites that exist on an encrypted network.[8] It consists of proxy networks, where the location of the hosting server cannot be traced or known as in the open web. The most well known such network is called Tor, a collection of secret websites that require special software to access them and re-routes connections through several servers, allowing users to remain anonymous. One of the positive aspects of the dark web is that it affords internet users as much privacy as possible, which is useful for undercover law enforcement investigators, human rights activists and journalists in repressive countries, or for military use. In fact, the dark web was created by the US government to allow spies to exchange information completely anonymously.

Yet, the dark web also has negative aspects, as many use it to accomplish illegal activities and to commit crimes undetected. Among them, the use of the dark web for CSAM distribution is on the rise. In 2019, the IWF identified 288 new hidden services, up from 85 in 2018 (i.e. a 238 % increase). These include online communities of persons sharing CSAM and their sexual interest in children. According to investigators, these enhance the legitimisation of people's sexual interest in children. Such online communities also provide technical and security advice, along with hints on how to access or approach children for abuse. An increasingly important need for law enforcement activity in these spaces is the ability to effectively infiltrate particularly dangerous online groups of offenders, such as those committing online child sex abuse streaming in real time. Livestreaming is particularly complex because it allows offenders to interact with child sexual abuse happening in real time, while leaving limited evidence.

As previously mentioned, child sexual abuse and exploitation on both the surface open web and in the hidden dark web have increased significantly during the pandemic. Unfortunately, increased internet penetration in the developing world too also opens up new opportunities for child abusers. It has been shown that child sex offenders in developing countries, many in Asian ones such as the Philippines, are abusing children at the instigation of offenders located elsewhere in the world, who commission the abuse online and watch it over a live stream for a fee. Within the EU, a large Europol operation uncovered significant levels of livestreaming taking place in Romania. This is not only happening over the hidden dark web: according to police reports, in 2019 Skype was the world's most common platform for live-streamed child sexual abuse.

Europol points to another related trend: the emerging use of alternative payment methods, such as bitcoin, that ensure further anonymity and facilitate the spread of pay-per-view CSAM websites. In

Thailand, according to media reports, this has created a new category of abusers: those who abuse children for money, not for personal pleasure. The 2020 Europol cybercrime report highlights the commercialisation of CSAM as one of the main current threats. Uploading CSAM to legitimate hosting services allows the uploaders to acquire credit based on the number of CSAM downloads.

In addition, the internet of things (IoT) that is bringing billions of connected devices to the internet around the world is also bringing opportunities for child sex offenders to approach children in a hidden manner. Recent years have seen a growth in the number of IoT connected products; children too are using an increasing number of connected devices in their bedrooms, such as smart speakers and smart TVs. A study carried out at the request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) has shown that hacked devices, such as CCTV in schools and other locations where children are present, will create new threats, as they allow to track personality traits, behaviour and location, offering child sex offenders more possibilities to track victims down. There have already been a number of cases involving children's toys, web cameras and baby monitors, which were hacked because they had been linked with insecure connected products.

Cloud storage

Physical offline storage of CSAM data in hardware such as laptops, mobile phones and USB sticks remains the most common storage medium for child sex offenders. Yet, according to a recent survey among police officers by Swedish tech company Netclean, use of online storage provided by cloud computing services appears to be increasing year on year, with offenders storing and sharing links online. Rather than sending or receiving file images – which is riskier and allows sharing of a more limited amount of CSAM data – offenders now seem to prefer cloud storage as a way of sharing links, as the cloud enables private access to storage that can host massive collections at a very low cost. This is challenging law enforcement's traditional methods of acquiring and collecting electronic evidence. In addition to the technical challenges, there is also the challenge related to the jurisdictional issues when the cloud host is based in another country, which further impedes access to online and offline evidence. This gives child sex offenders an advantage, as they avoid the risks associated with physically transporting CSAM through airports and with other checks, including in their homes.

According to media reports, the cloud computing industry does not take full advantage of the existing CSAM screening tools to detect images or videos in cloud computing storage.[9] For instance, big industry players, such as Apple, do not scan their cloud storage. In 2019, Amazon provided only eight reports to the NCMEC, despite handling cloud storage services with millions of uploads and downloads every second. Others, such as Dropbox, Google and Microsoft perform scans for illegal images, but 'only when someone shares them, not when they are uploaded'.

How digital technologies are helping investigators

Law enforcement authorities and investigative teams play a key role in the fight and prosecution of CSAM. To identify CSAM and related sexual abuse of children effectively, EU Member States' law enforcement teams participate in collaborative EU and international efforts. Yet, tackling this problem over the past 20 years has not delivered the necessary improvements, and there is now an urgent need for all players to step up their efforts, including through innovative technical capacities, especially in view of the surge in online CSAM. Thanks to digital technologies, it is now both easier and cheaper than ever before to create and store huge amounts of data, including CSAM. According to police data, a typical police CSAM case might involve anywhere between 50 000 and 5 million images, many of which do not contain child sexual abuse. Analysis and classification of such a vast number of images is a major challenge for the human brain. The increasing volume of CSAM that needs to be analysed is a major barrier in the way of efficient investigations and of swiftly providing safety to children globally.

On the other hand, digital technologies can support investigation teams in detecting child sexual abuse material in a vast number of seized photos or videos, to locate victims or offenders, or to conduct investigations in hidden networks.

In order to help with the reporting of CSAM, the tech industry, together with NGOs (such as End Violence against children, the IWF, and Thorn[10]), has developed technical approaches to stop the recirculation of CSAM through blocking, hashing, crawlers and AI.

Blocking

Blocking happens when internet service providers (ISPs) block data while they travel through their networks. Blocking technologies can pick up and block domains and URLs in the open web that are already known to contain online CSAM. Blacklists of websites containing or disseminating child sexual abuse material are commonly used in the implementation of blocking measures. ISPs find and block CSAM by using technology and lists from existing databases and systems, for example, from Interpol, the IWF, the NCMEC, police forces or hotlines.

Hashing

One of the most established hashing tools, developed over 10 years ago, is Microsoft's PhotoDNA, a shared system for detecting and responding to images of child sexual abuse based on hashing,[11] an automated content recognition technology that allows already known images to be recognised and filtered or reported. Among the most widely used databases is the Hash Value Sharing platform, where hotlines such as those of the IWF,[12] NCMEC and INHOPE create and share hash values from identified child sexual abuse images.

However, hashing only works if electronic service providers have access to the plaintext of the images for scanning, typically at the messaging platform's servers. If the provider cannot read the image file because, for instance, it is included in E2E encrypted messaging, hashing would not work. Another limitation is that this filtering process happens after the material has already become available for others to see and redistribute, as it is based on existing material already classified as CSAM. It does not apply to unknown and new material.

Web crawlers

A web crawler is automated software that search engines and other bodies use, for example, to find and index what is new on the internet. In the fight against online CSAM, one of the most successful web crawlers – Project Arachnid crawler – was developed by the Canadian Centre for Child Protection in 2016. Project Arachnid operates by using Photo DNA technology along with hashes from existing lists generated by several organisations, including the NCMEC, the Royal Canadian Mounted Police and Interpol. Project Arachnid tracks URL links from websites known to contain CSAM across the open and dark web. If CSAM is detected, a notice is sent to the hosting provider requesting its removal. Project Arachnid detects images and video content at a speed exponentially faster than previous methods, with over 100 000 unique images per month that require analyst assessment. Once potential CSAM content is detected, then it needs to be verified by three different human analysts to ensure that the image can be effectively classified as CSAM. Once this is done, a notice is sent to the hosting provider, requiring that the material be removed. As of 1 October 2020, it had already processed over 125 billion images, out of which over 24.3 million had been triggered for human analyst review that resulted in over 6.2 million notices sent to providers for take-down. Some 85 % of these notices relate to victims who are not known to have been identified by police.

There are other crawlers, such as the IWF's Image Hash List, which is also a very effective tool. The EU is currently developing one under the broader Aviator project (i.e. Augmented Visual Intelligence and Targeted Online Research), funded by the European Union's Internal Security Fund. The national police of the Netherlands have been using the first version of the AviaTor tool since December 2019.

Artificial intelligence

AI technology is helping law enforcement personnel to speed up their working processes and better cope with CSAM images. AI now helps them to reduce the time spent in assessing and prioritising CSAM reports for human review. It also help them process reports faster and avoid duplication, while also ensuring more accuracy and faster take-down of both seen and previously unseen CSAM. The threat to children depicted in new material is often different to that in known material. Newly generated material is more time critical, as it is likely to indicate current and ongoing offending, such as against an unidentified victim who continues to be abused or a child who is being groomed and coerced into producing new abusive images. AI technology accelerates the identification of victims, while at the same time easing the psychological burden on operatives tasked with classifying CSAM and helping them deal with duplicates. According to Netclean's 2019 survey, one in five police officers has used AI tools in their investigations.[13]

Likewise, the tech industry is now developing its own AI to recognise CSAM. Service and social media providers are already using AI and analytics to detect and stop exploitation within their networks as a way to fight against CSAM. An example is Google's Content Safety API, a tool that uses AI to help organisations better prioritise CSAM for review. It uses machine-learning technology to flag potentially harmful or 'toxic' content to moderators in both existing and new material. Some other companies are using AI to help verify the age of their online users.

To recognise victims and offenders, some companies maintain searchable databases tied to facial recognition. One of the most controversial companies doing this is Clearview AI, a start-up that put together a searchable database containing over 3 billion photos and images from the web and social media platforms, which it sold to the police and law enforcement to help them identify among others child victims of sexual abuse. As it generates a unique face print of each person inside it, the database is capable of matching photos or video images of unknown people to their photos or images it already contains. Yet, despite the company's claims that it has helped police officers identify both perpetrators and child victims, it is eyed as controversial and is the subject of numerous lawsuits, as its pool of images was assembled without permission. According to media reports, over 600 law enforcement agencies worldwide are using it. In the EU, the European Data Protection Board (EDPB) has said that Clearview AI is most likely not respecting EU legislation. The European Commission has already pointed in its White Paper on Artificial Intelligence[14] to the specific risks to fundamental rights related to the use of biometric technologies for identification purposes, including facial recognition.

Other existing face recognition tools are Rekognition by Amazon and Azure by Microsoft. Though Amazon has banned police from using Rekognition for one year following the George Floyd killing in Minneapolis on 25 May 2020, the software remains accessible to other organisations, such as Thorn, the NCMEC, and AI start-up Marinus Analytics, to help rescue human-trafficking victims. IBM has gone out of the facial recognition business and Microsoft has also banned its face recognition system like Amazon, while waiting for clearer legislation in this domain regulating how the technology can be employed.

AI can also be used to develop anti-grooming technology tools. One such example, Project Artemis, was developed using Microsoft's Xbox technology, to assist online service companies that offer a chat function. It evaluates and rates conversations, flagging those that need to be reviewed by human moderators. Human moderators would then be capable of identifying imminent threats for referral to law enforcement.

Finally, AI technology is only as good as the data that it has been provided with, and it needs a large amount of consistent data to be developed. If the classification of images, videos or conversations is incorrect, the AI will draw the wrong conclusions from these data. This means that the technology still relies heavily on human verification to ensure that the classification of data is right. In the fight against CSAM, one of the main challenges according to a recent report is the lack of standardised classifications among the different parties involved – NGOs, hotlines, law enforcement agencies and the internet industry – each of which currently classify CSAM content in a different way.

Future prospects

The digital transformation is creating new types of risks to children, who have become an easier target for child sex offenders online. Despite many efforts from many stakeholders to fight the surge in online CSAM, the situation has been deteriorating over the past 20 years, reaching dramatic proportions at global level during the current pandemic. There is evidence that these crimes are continuing to increase and develop alongside technological advances. In this regard, it would be right to say that digital technologies play a dual role, as they both help in the fight against CSAM, and facilitate its proliferation. Moreover, social media platforms have accelerated the pace of CSAM creation and distribution and facilitated offenders' access to children. Law enforcement and hotlines are overwhelmed with the amount of reports they get, even though these are only a fraction of the real number of offences, as child sex offenders use defensive forensic measures, including anonymisation and encryption of their online illegal activities. Given that tools such as web crawler Project Arachnid have already gone through billions of images and videos, the volume of the real CSAM circulating online might be more dramatic than reported. There is therefore an urgent need for all players to step up their efforts in fighting the surge in online CSAM. Otherwise, the situation will only get worse as high levels of internet use and mobile connectivity continue increasing. The gigabyte society that 5G will enable might complicate things even further, given its complex, multi-layered and encrypted secure infrastructure.

Conversely, digital technologies – such as AI, blocking, hashing and web crawlers – but also improved online age verification methods or age-appropriate design by default, are among the solutions to fight the surge in CSAM. Due to its capacity and speed of analysis, AI could play an important role in tackling the problem, though there are some challenges that need addressing, such as the lack of standardised data classification, global collaboration and AI legislation. While seeking to find technical solutions to keep young children safe online is important, there is also a need to safeguard internet freedoms, avoid digital surveillance and increase global levels of digital cybersecurity and digital competences to avoid vulnerable groups being cyber-attacked.

Even though the EU has funded many safer internet activities over the past 20 years and introduced related legislation, the situation remains unsatisfactory. A zero-tolerance approach is needed, with a shift towards more forward-looking technological tools, policies and legislation. The new Commission EU strategy for a more effective fight against child sexual abuse goes in that direction, aspiring to step up technical cooperation and global solutions in the fight against child sexual abuse offline and online. However, it will also have to fight to remain relevant, given the focus on the pandemic, which has already led many jurisdictions worldwide to attach lesser priority to the fight on CSAM.

MAIN REFERENCES

Curbing the surge in online child abuse: New EU legislative and policy proposals, EPRS, (forthcoming).

Internet Organised Crime Threat Assessment (IOCTA), report, Europol, October 2020.

The impact of algorithms for online content filtering or moderation, study, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, September 2020.

Age Appropriate Design Code, UK Information Commissioner Office, September 2020.

Quayle E., Prevention, disruption and deterrence of online child sexual exploitation and abuse, ERA Forum, September 2020.

Carr J., Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse, Council of Europe, November 2019.

Internet Watch Foundation Zero Tolerance, Annual Report, 2019.

Child safety online: definition of the problem, in-depth analysis, Policy Department for Cohesion and Structural Policies, European Parliament, February 2018.

Combating child sex abuse online, study, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, October 2015.

ENDNOTES

[1] The UK's IWF, Canada's Cybertip.ca and the National Centre for Missing and Exploited Children (NCMEC) in the US do so. The Lithuanian hotline Švarus internetas undertakes limited and circumscribed proactive search in the form of guided Uniform Resource Locator (URL) crawling

[2] See US Federal Law 18 U.S.C. § 2258A.

[3] There are three categories of abuse (grades A, B and C): category A is the most severe one including sexual penetration, category B includes other types of sexual abuse without penetration, and category C covers the least severe situations that do not fall under A or B.

[4] Popular online video games for youngsters include World of Warcraft, League of Legends, Clash of Clans and The Sims, where they connect with other gamers and chat while playing.

[5] In the EU, the GDPR age limit is set at the age of 16 as a default position, but EU Member States have been granted a margin of manoeuvre to reduce the age of consent for privacy matters down to age 13.

[6] Among them, 1) a minimum amount of personal data should be collected and retained; 2) children's data should not usually be shared; 3) geolocation services should be switched off by default; 4) nudge techniques should not be used to encourage children to provide unnecessary personal data, 5) weaken or turn off their privacy settings; and 6) recommendations for parental control and profiling.

[7] UK, Australia, Canada, India, Japan, New Zealand and the United States.

[8] Websites on the deep web are not indexed and do not appear when looked for with a search engine as on the open web.

[9] In 2019, Facebook reported to the NCMEC about 17 million combined images and videos, Google reported about 3.5 million and Yahoo about more than 2 million. Dropbox, Microsoft, Snapchat and Twitter reported more than 100 000 images and videos. Apple reported just over 3 000 in total, and zero videos (Apple explains these figures with the fact that its messaging app is encrypted and that it does not scan its cloud computing file storage service, iCloud). Amazon sent only eight reports to the NCMEC.

[10] Thorn is an NGO that builds technology to defend children from sexual abuse.

[11] Cryptographical hash algorithms are used for file identification and evidence authentication in digital forensics. By creating databases of hashed child sexual abuse material, new material can quickly be matched against already known files. When previously unknown images are found, they are processed and hashed.

[12] Analysis of the 471 239 hashes on the IWF Hash List at the end of 2019 showed that of the image hashes relating to children assessed as 10 years old or younger, 64 % were at the highest levels of severity (grade A or B), compared to 47 % of the image hashes relating to children aged 11-17. Of the image hashes relating to babies and toddlers aged 2 and under, 87 % showed the most severe forms of abuse (see pg. 49).

[13] According to Interpol and UNICRI, there are four broad categories on how AI and robots support law enforcement: 1) prediction and analysis, 2) recognition, 3) exploration, and 4) communication.

[14] in Section D point f).

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

Photo credits: © Graphicroyalty / Adobe Stock.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)