SciencesPo

CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Is encryption a fundamental right?

A case study on CSAM regulation in the EU

Stavroula Chousou, Julia Magaud,

Ludovica Pavoni & Morgan Williams

Comparative Approaches to Big Tech Regulation (Spring 2023)

Professor Florence G'sell

April 2023

May 2022

Table of contents

Abstract

1.

Two current policy debates collide into a complex and evolving European legal landscape: Is it possible to protect children and prevent the dissemination of child sexual abuse materials (CSAM) when end-to-end encryption (E2EE) technology makes messages inaccessible to law enforcement? As CSAM continues to proliferate online messaging platforms, political debates and long legal proceedings are looking to create criminal proceedings backdoors and obligations for telecommunications and online media firms to scan their services for CSAM evidence. Some argue that encryption in the era of digitization is not up for debate, rather it approaches a state of fundamentality. Encryption protects privacy and security online, both of which are recognized as undisputed fundamental rights. But is encryption itself a fundamental right? What happens when a fundamental right enables crimes against the most vulnerable in our society? Is there a way to protect children from CSAM while simultaneously protecting the right to private communications online for all? By examining the role of encryption and the current regulatory framework in the EU, with an emphasis on the developing proposal to prevent and combat child abuse by screening private messages, we establish the fundamentality of encryption in the private lives of all internet users, including children.

2. Introduction

Billions of users communicate via private messaging on platforms like Facebook, Twitter, and Signal each day. Unfortunately, the confidentiality on these platforms can be exploited for large-scale spam, harassment, propagation of fake information, terrorist propaganda, and distribution of child sexual abuse material. On one hand, the platform's use of encryption to protect users' privacy while, on the other hand, protecting these perpetrators from law enforcement. Governments worldwide have proposed or implemented measures that require access to encrypted data, arguing that they are necessary for the prevention and detection of crimes. However, this raises important questions about the balance between privacy and security, as well as the rights of individuals to protect their personal information. Specifically in the European Union, online child sexual abuse material (CSAM) scandals of recent years, have raised severe concerns about the means and procedures in our possession to protect children online. The technologically ambivalent EU was met by increased debates surrounding encryption's role in harboring dangerous criminals in that respect. But are those fears sound when it comes to encryption's technicalities and functions? And if so, what are the alternatives? Is encryption a necessary evil, an ad hoc requisite, or a safety-blanket-clause of an ever-digitized society?

In this policy analysis, we will explore whether encryption is a fundamental right and the consequences of this determination on the EU's approach towards regulating encryption and protecting children from CSAM. The structure of the report is as follows: Explain what encryption is (Section 1) and uncover the stakes associated with regulating encryption (Section 2), outline the timeline of regulations regarding encryption in the EU (Section 3) and their flaws (Section 4), and finally, clarify whether encryption should be protected as a fundamental right (Section 5) and how the EU should, instead, approach encryption regulation (Section 6).

3. 1. What is encryption?

Encryption is the process through which information is converted into secret codes that hide the information's true meaning. It has been defined by the OECD as

"the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality" (p. 9). This means that it is a way of scrambling data so that only authorized parties can understand information; put in technical terms it is the process of converting human-readable *plaintext* into incomprehensible text, also known as *ciphertext*.

Image 1: Schematic representation of how encryption works

Source: "What is encryption? | Types of encryption". *CloudFlare*.

From this description we can infer that encryption is a process which is almost intrinsic to world history, seeing as civilization progressed also methods to conceal delicate information advanced. There is evidence of encryption methods that date back to the Ancient Egyptians that used hyper-complicated hieroglyphs to prevent lower-level people from understanding privileged information and to the Greeks in the eighth century B.C. as they devised methods to confound information from enemies. Significant advancement in the field of encryption was made by Arab mathematician Al-Kindi through the study of the statistics of the frequency of letters in a text, that he reported in his book *On Decrypting Encrypted Correspondence* that to this day is considered being the first book on the topic. Further encryption strategies were observed through the centuries, but we witnessed a peak in encryption technologies in the 1900s, with military-developed hardware-based encryptions to protect sensitive information from foreign intelligence entities. During the Second World War there was significant advancement with encryption technologies, as evidenced by Alan Turing's de-encryption of Germany's *Enigma*. (Schlesinger and Yanisky-Ravid, 2022, p. 574).

As the world entered the information and technology age, we witnessed the advent of advanced computing which gave rise to a new type of protection: digital encryption. Seeing as computer technologies have advanced and the availability of digital computing has become more widespread, it is increasingly more obvious that the use of encryption has shifted from being more state-centric to becoming accessible to a wider range of actors and users. Indeed, from being something closely related to protecting states' secrets and from being used for military purposes, encryption

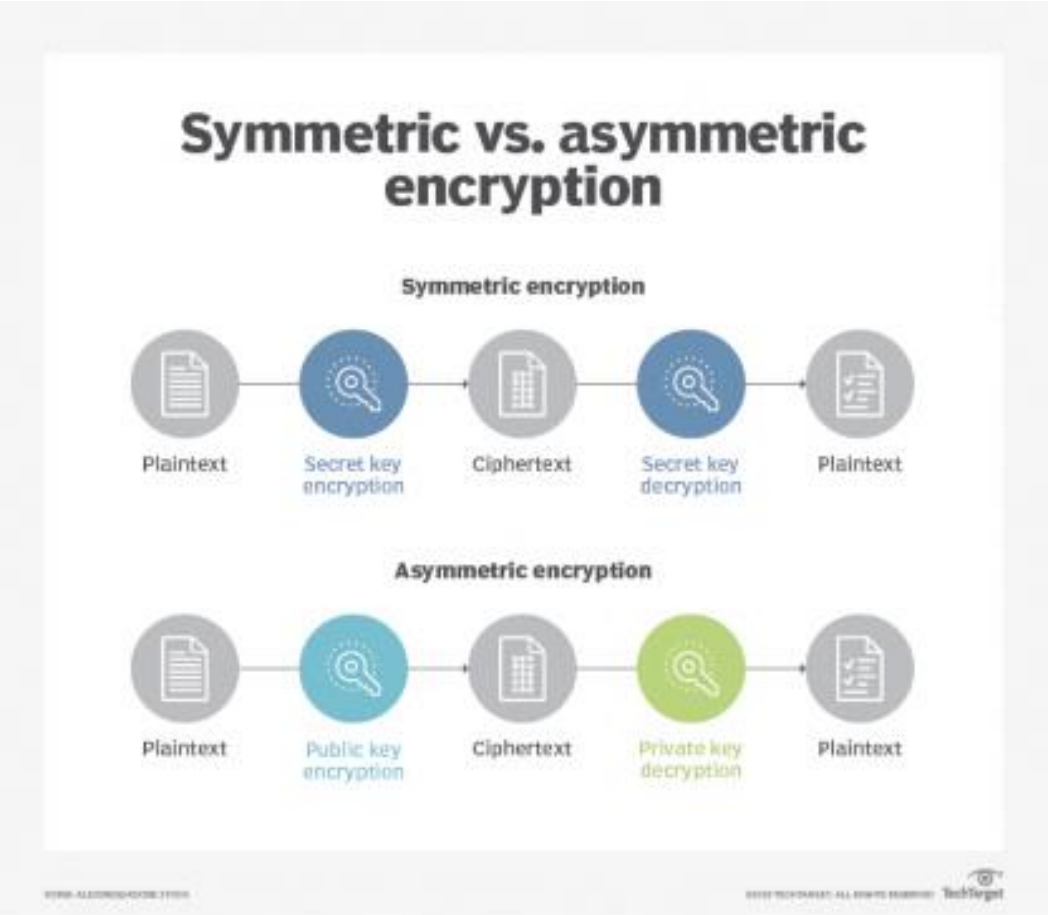
nowadays is part of the broader field of cryptography that is widely accessible to common users. Technology has advanced to the point where the average user can utilize potentially unbreakable encryption methods without even realizing it.

1.1 Different types of encryption

There are two different types of encryption, symmetric and asymmetric encryption, also known as public key encryption. The two are defined in the following: (a) **symmetric encryption** is an older method that is fast as it only requires one key. Given its better performance and its faster speed it is typically used for bulk encryption (e.g. database encryption) and the secret key is usually only available to the database itself while (b) **asymmetric encryption** uses two separate keys, one used for encryption and the other for decryption. This first key is public, for everyone to use, while the second key is private and only the authenticated recipient has access to it (Conrad et al., 2012).

The main difference between the two is that symmetric encryption requires only one key, and all the parties use the same secret key to both encrypt and decrypt information. Asymmetric encryption instead has two distinct keys, one used for encryption and the other used for decryption (Prima Santoso et al., 2018, p. 2). A second difference between the two is the length of the keys used. Symmetric encryption requires a shorter key, which of course depends on the level of security needed while asymmetric encryption needs to have longer keys seeing as the two different keys need to be related and complex enough as to not be cracked.

Image 2: Symmetric and asymmetric encryption



Source: Brush, K., Rosencrance, L.,& Cobb, M. (2021, September). "Asymmetric encryption (public key cryptography)". TechTarget.

1.2 End-to-end encryption (E2EE)

For the purpose of this paper we will only focus only on asymmetric encryption as it is a big family that comprises the so-called End-to-end encryption (E2EE), which is the fulcrum of the debate on whether encryption is a fundamental right or not. E2EE is a process of encrypting data between devices so that only the sender and the receiver can view the contents of the message. This means that this method encrypts the messages before they are sent and decrypts them after they are delivered[1]; through this process both the messages themselves and the data they contain are secure (Knodel et al., 2021). The encrypted data therefore can be read only by the two parties

[1] Linking back the concept of E2EE to asymmetric encryption, the public key is used to encrypt the data and the private key, which is only available to the owner, is used to decrypt the data.

- the sender and the receiver - and no one else can read the encrypted message, not hackers, not governments, not the server through which data passes.

This encryption method might sound familiar, and it indeed is because it is widely used in applications that the average person accesses on a daily basis. Messaging apps such as WhatsApp, Telegram, and Signal all use E2EE to ensure private conversations between the users. Email service providers and all the major communication apps, such as Zoom, as well as social media platforms have also introduced this encryption method to ensure secure communication (Kamara et. al, 2022, p. 14). To clarify further how E2EE works, we provide the following example:

"If we consider two WhatsApp users that are texting, we know that their messages - thus their data - passes through a WhatsApp server while bringing the message from one side to the other. E2EE happens at the device level, this means that messages are encrypted before they leave one device by a public key which is available to all but are only decrypted by the recipient's private key when they reach the second device."

By encrypting the information at the device level and not at the server level, E2EE keeps the information encrypted and the service provider itself cannot intercept that data to decrypt it. This means that law enforcement authorities and government agencies also are not able to access the data, even when they have authorization to. Therefore, by using E2EE no one can access the data other than the two parties, in theory.

4. 2. Benefits and risks associated with encryption

2.1. Overview

The use of end-to-end encryption (E2EE) in instant messaging services, such as WhatsApp, poses both risks and benefits for end-users, instant messaging services, and governments. Governments, in particular, are threatened by E2EE because it creates barriers to monitoring and enforcing illegal activity on the internet. Meanwhile, instant messaging services wish to protect the privacy of their users (Endely, 2018, p. 96). Ultimately, labeling E2EE as a "good" or "harmful" technology depends on whether the stakeholder prioritizes individual privacy over public safety. With that said, it is not abundantly clear whether most end-users themselves understand exactly what E2EE

is and the risks and benefits associated with the technology, as well as the stakes of this debate (Kamara, 2022, p. 12). This section will disentangle the various arguments surrounding E2EE (See Table 1) and debunk recurring myths.

Table 1. Benefits and risks of E2EE by stakeholder

Stakeholder	Benefits		Risks	
End-Users	I. II. III. IV.	Enhanced privacy Protection against data breaches Trustworthy communication Free expression	I. II.	Can be misused for illegal activities Can be difficult to manage different encryption keys
Instant messaging services	I.	Protection against data breaches	I.	More difficult to monitor harmful or illegal content on the platform
Governments	I. II.	Protection against data breaches Promotes free expression online	I.	Difficult to monitor criminal activity

2.1 Benefits associated with encryption

Benefits of E2EE are characterized by enhanced security and protection against data breaches. Following the 2013 Snowden disclosures and the 2016 Cambridge Analytica scandal, social media and instant messaging users have become increasingly more aware that their personal data is at risk of being misused by governments and large corporations through data breaches (Song, 2020, p. 4). The Cambridge Analytica scandal exposed how foreign governments could leverage personal information from over 50 million Facebook users to exploit users' psychological profiles and influence democratic elections. Many of these Facebook users felt deeply disturbed that their personal information was being collected and sold without their consent, which in turn, damaged their trust in the social media platform (Song, 2020, p. 5). In response, many instant messaging services faced pressure to reassure their businesses and private individuals that their data is protected from government surveillance and eavesdropping (Endely, 2018, p. 96). This pressure is likely what motivated Meta's decision to test E2EE on Facebook Messenger in 2022.

Users of instant messaging services with E2EE could rest assured that their conversations could be read by themselves, and no one else, including the service provider or any other third party. Since the data is encrypted at both endpoints, it is difficult for hackers or corporations to steal or sell the data. With E2EE, consumers and businesses have access to a trustworthy mode of communication, where they can feel confident sharing their personal or confidential information, such as those relating to their medical history or finances. In addition to messaging services, E2EE enables secure online transactions, such as banking or e-commerce.

Data protection regulations, such as General Data Protection Regulation (GDPR) in the European Union (EU) and the California Consumer Protection Privacy Act (CCPA) highlight the important role of encryption in ensuring consumer and business security (Song, 2020, p. 6). Although neither regulation explicitly requires encryption, they both strongly recommend that messaging services encrypt personal messages. The CCPA goes as far as establishing a safe harbor that enables companies to avoid financial penalties if they encrypt personal data. Taken together, government agencies have expressed that encryption is preferable to protect the safety and security of personal data. However, they did not specify the type of encryption. Therefore, the stance is not explicitly in conflict with other agencies within governments that have reservations about the use of E2EE.

Advocates for E2EE argue that the technology promotes freedom of expression by preventing interference from states and corporations (Kamara, 2022, p. 12; Song, 2020, p. 6; Grover, 2021, Introduction). The tool is particularly appealing for individuals in authoritarian regimes, where minority groups, journalists, researchers, lawyers, and civil society need a space to communicate freely without fear of surveillance or harassment from the state (Grover, 2021, Introduction). Given the increasing importance of online communication to our society, blanket bans of E2EE may provide states with unprecedented ability to monitor and surveil citizens' private conversations and data. As a consequence, bans on E2EE would place individuals at risk of victimization from oppressive or authoritarian regimes (Song, 2020, p. 12). On the contrary, preservation of E2EE protects and preserves "individualism and personal safety" (Song, 2020, p. 11).

2.2 Risks associated with encryption

The discussion opposed to E2EE is characterized by crime and threats to public safety. Given the closed nature of E2EE, it is impossible for governments to monitor criminal activity and investigate crime. Therefore, if instant messaging services are unable to access private conversation, criminals or terrorists can take advantage of the privacy to organize crimes (Kamara et. al, 2022, p. 15; Song, 2020, p. 7; Grover, 2021, Introduction).

Critics of E2EE argue that secrecy can pose threats to national security, in the case of terrorist attacks. For example, the terrorists who planned the 2015 attacks in Paris used Telegram, an instant messaging service protected by E2EE, to organize and spread propaganda (Song, 2020, p. 8). They were able to securely allow these terrorists to collaborate and delegate tasks that ultimately led to the death of 130 individuals. Without a secure messaging platform, it may have been more challenging for the terrorists to coordinate across various groups and carry out an attack of this scale. It is possible that the French government may have been able to identify suspicious activity and prevent the attack from occurring if they had access to a back channel on the messaging platform.

Criminals and non-criminals alike are allotted the same rights and privileges to privacy and security on instant messaging platforms with E2EE. In addition to preventing the identification of terrorist activity, the technology can also be misused by non-terrorist criminals, such as drug traffickers or pedophiles, to conceal their criminal activity (Song, 2020, p. 8). Not only do E2EE instant messaging platforms enable criminals to collaborate without surveillance or risk of data beaches, it is impossible for instant messaging platforms to provide law enforcement with digital evidence to investigate the crime (Grover, 2021, Introduction). These arguments are particularly relevant to the EU's case against E2EE used for the distribution of child pornography, which will be discussed in greater detail below.

In response to these accusations, supporters of E2EE argue that criminals and terrorists will find other motives of communication if they can no longer use messaging services protected by E2EE, such as Telegram (Song, 2020, p. 8). Therefore, a blanket ban on E2EE would not result in a meaningful reduction in criminal activities.

E2EE limits instant message platforms' ability to moderate content for illegal or harmful activities, such as hate speech or cyberbullying. In theory, as hosts, instant messaging services have the authority to moderate content that, while legal, violates their set community guidelines or terms of service. Different hosts take different approaches towards content moderation depending on their user base, business model, or other considerations (Kamara et. al, 2022, p. 8). From a business perspective, dissemination of illegal or harmful content on their platform creates reputational risks for the company. However, E2EE ensures that the instant messaging service does not have access to content shared on their platform, which disables them from exercising content moderation. Even if it were possible for instant messaging services to screen the messages, it is difficult to distinguish illegal or harmful content from content that does not infringe on the host's community guidelines because it does not have distinguishable characteristics from innocuous content (Kamara et. al, 2022, p. 16).

Although E2EE is meant to increase safety and security, there are some "loopholes and unknown risks" that have undermined its reliability (Song, 2020, p. 8). As the technology continues to evolve, it is conceivable that technological advancements in the software are accompanied by glitches or weaknesses. To prevent third parties from accessing messages, instant messaging platforms, such as Telegram, established a policy of erasing messages as soon as they are decrypted as a second layer of security. However, in June 2018, an online messaging service, Signal, did not encrypt a part of the decrypted messages. While these technical glitches are rare, it demonstrates that E2EE is not always completely secure.

5. 3. How is the EU trying to regulate encryption?

3.1 European legal scope around encryption

The science and technology sector falls under the category of **shared competences in the EU** (Article 4 of the TFEU[2]**).** Consequently, both the EU and the Member States are able to legislate and adopt legally binding acts on related matters,

[2] "Member States exercise their own competence where the EU does not exercise, or has decided not to exercise, its own competence." https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E004&from=EN

such as encryption. However, member states have the discretion to impose their own national laws and provisions to the use and access to encryption as long as it does not conflict with other EU legislation e.g. the GDPR, its encryption-related directives etc. This has resulted in increased heterogeneity in encryption regulation and severe digital gaps among member states. The heterogeneity element, refers to the fact that among the states that have a legal stance on encryption, there exists a wide range of alertness degrees and of assigned importance. Moreover, states employ widely ranging approaches and tools to enforce their regulations. On the other hand, many countries do not yet have national encryption-related legislation, reflecting their digital integration level (Global Partners Digital, 2023). Specifically, only 11[3] out of the 27 member states have some form of legal provision on encryption.

The lack of a designated EU competence has resulted in a fragmented European stance on the matter both domestically and internationally, allowing for two major debates to arise: (1) one that revolved around the position of telecommunication companies when it comes to and their jurisdiction in deciphering data for criminal investigations, and the other (2) specifically revolving around the severe issue of child abuse cases in the digital space of the EU. That is particularly problematic since encryption technologies are developing in rapid paces, reflecting the increased need and urgency for both protection and privacy.

3.2 First steps towards regulation (1995-2016)

On a European level, the first comprehensive data protection law was the Data Protection Directive (95/46/EC)[4], adopted in 1995. The directive did not specifically address encryption but required member states to take appropriate measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. In 1999, the EU adopted the Electronic Signatures Directive (1999/93/EC)[5], which provided a legal framework for the use of electronic signatures and certificates. The directive recognized the use of cryptographic techniques, including encryption, in relevant activities. In 2002, with the ePrivacy Directive

[3] Ireland, France, Germany, Belgium, The Netherlands, Denmark, Czech Republic, Croatia, Greece, Estonia and Finland.
[4] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01995L0046-20031120
[5] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01999L0093-20081211

(2002/58/EC)[6], member states and businesses were required to ensure the confidentiality and security of their communications, underlying networks and services. In 2006, the EU adopted the Framework Decision on the European Arrest Warrant (2002/584/JHA)[7], which established the procedure for issuing and executing arrest warrants between EU member states. The decision required member states to ensure that any request for interception of electronic communications was authorized by a court or other independent body and that **the interception was necessary and proportionate**.

In 2008, the EU amended the ePrivacy Directive with the Telecoms Package (2009/140/EC)[8], which required member states to ensure that any interference with electronic communications, including encryption, **was authorized by law, necessary, proportionate, and subject to adequate safeguards**. The Stockholm Programme was introduced in 2010[9], setting out the EU's priorities for justice and home affairs for the period 2010-2014, calling for measures to strengthen the fight against serious crime and terrorism, including the use of interception and decryption of electronic communications. In 2012, the Data Protection Directive was replaced by the Data Protection Regulation (EU) 2016/679[10]. It required businesses to implement appropriate technical and organizational measures to ensure the security of personal data, including encryption and pseudonymization.

EU laws and directives up until 2016 generally favored the use of encryption as a means of protecting personal data and electronic communications. They included provisions on interception and decryption under specific circumstances; those were quite ambiguous, as they do not clarify what exactly constitutes a necessity or a proportionate action. Overall, the encryption-related provisions up until this point lacked technical nuance and precision.

[6] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
[7] Available at: wur-lex.eu/Framework Decision on the European Arrest Warrant (2002/584/JHA)
[8] Available at: https://eur-lex.europa.eu/legal-content/fr/ALL/?uri=CELEX:32009L0140
[9] Available at: eur-lex.europa.eu/ Stockholm Programme 2010-2014
[10] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

3.3 First European debate on encryption: Prevention of terrorism

In 2016, many European countries experienced devastating terrorist attacks, the most severe of which took place in Paris and Nice. As experts suggested that terrorist groups favored better-encrypted communication channels for their communications, France embarked upon a domestic campaign to render all telecommunications firms operating in its jurisdiction compliant with the principle of full disclosure in criminal investigations. On the EU level (Acharya et al., 2017), France proposed a law in the European Commission, which would oblige communication platforms to fully cooperate in judicial investigations tracking down terrorists by giving the authorities full access to the data required (Reuters, 2016).

However, encryption was too new in the European political scene and France's proposal was met by a divided EU. Many European countries, most notably Germany and The Netherlands, distinguished their positions from the French one, reaffirming their intentions not to sabotage the development of better and more efficient encryption methods (Benner & Hohmann, 2016). Germany highlighted its ambitions to become a European hub for encryption, which came as no surprise, since Germany follows a path similar to the US where despite the presence and activity of terrorist groups, there is a culture of investigative government hacking (Acharya et al., 2017). However, France was not alone in its demands; Hungary and the (then European) UK had their own internal debates about the legality and limits of encrypted services (Benner & Hohmann, 2016).

In this context, the European Organisation of Cybersecurity (ENISA), strongly supported its previously stated position that strengthening encryption backdoors and implementing up-to-date encryption protocols and techniques is the only viable measure to facilitate law enforcement investigations without endangering the privacy of the citizens using such platforms (Stupp, 2016), as fleshed out by ENISA's NIS Directive (ENISA, 2016). The same year, another important regulatory benchmark was reached in that respect. The General Data Protection Regulation (GDPR) was adopted in 2016 and came into effect in May 2018. GDPR required businesses to implement appropriate technical and organizational measures to ensure the security of personal data. This may take the form of encryption or pseudonymization. GDPR has become the basis of the data protection framework in the EU, however, as stated in Section 2.3,

there are no explicit provisions that oblige services to use encryption. GDPR only imposes on companies and organizations to apply the best practices for the protection of the personal data they store and/or process.

Indeed, in the period from 2016 to 2019, the EU was confronted in various respects with its lack of preemptive thinking. Nevertheless, this debate initiated continued efforts to update and strengthen the rules on encryption and electronic communications in the EU, starting in 2017 with a series of non-legislative measures to explore the issue and create training resources and tools for law enforcement (DigitalEurope, 2020). These preliminary working groups slowly paved the way for further and more precise regulations and directives.

3.4 Second & current European Debate on encryption: Child sexual abuse material

In the past ten years, there has been a significant rise in reports of internet child sex abuse. Global complaints of child maltreatment have increased from 23,000 in 2010 to over 725,000 in 2019 (NCMEC, n.d.). Nearly nine out of ten reported URLs for child sexual abuse material (CSAM) are housed in the EU, making it the continent with the highest concentration of CSAM worldwide (Koomen, 2021). In fact, Europol identifies a significant increase in CSAM reports in 2020, often on peer-to-peer networks (IOCTA, 2020, p. 34-37). This is linked to the pandemic, as with more criminals staying at home came a raised demand for CSAM by as much as 25% in some EU member states. Tragically the supply side increased to meet the sharp rising (Koomen, 2021). Over 94% of the reported incidents involved content filtering on Facebook and its apps, including Messenger, Instagram, and WhatsApp. In 2020, Facebook revealed its plans for a social network that would be "privacy-focused," including the implementation of E2EE throughout all of its services, rendering both law enforcement and Facebook unable to identify 70% of the CSAM instances on Facebook (Koomen, 2021).

To address these issues, the European Commission launched two important strategies in July 2020; one for combating child sexual abuse specifically, and another for updating the EU's Security Union Strategy (Europa, 2020) more broadly. Both pointed to encryption from a public safety and security standpoint as means for perpetrators to "*mask their identity*" and "*hide their actions from law enforcement*"

(Koomen, 2021). Specifically, the Strategy to Combat Child Sexual Abuse included sector-specific regulations, operational efforts, and technical solutions, which highlight the role of the private sector and call on companies "*to detect and report child sexual abuse in E2EE communications".* The updated EU Security Union Strategy (2020) confirmed that the EU will "*promote an approach which both maintains the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism*".

In September 2020, a leaked draft revealed details behind the European Commission's thinking about technical "solutions" to detect CSAM in E2EE communications. The document was more technically nuanced than past rhetoric in EU encryption debates as it focused on the client side, or technology provider side, and the detection of CSAM. However, the draft did not offer a proposed solution - instead it highlighted a "least bad" option, which could be a persuasive, albeit somewhat manipulative, tactic (Koomen, 2021).

To proceed, the European Commission launched the Interim Derogation for the detection and removal of CSAM content, which includes a provision that would require online platforms to detect and report CSAM using automated tools (EPRS, 2021). Later that year, the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) issued its report criticizing the provision on CSAM detection and reporting, stating that it is "not proportionate" and "poses risks for fundamental rights, including the right to privacy" (EPRS, 2021). The European Parliament adopted its position on the proposal, approving the provision on CSAM detection and reporting but adding several safeguards, including the requirement that any automated tools used for detection must be subject to human oversight[11]. At the end of 2021, the Council of the European Union arrived at its own position on the proposal: it supports the provision on CSAM detection and reporting but also adds safeguards, including the requirement for independent audits of the automated tools used for detection (EDPB-EDPS Joint Opinion 4/2022). After that, the Parliament, the Council of the EU, and the Commission began trialogue negotiations on the proposal - the negotiations are ongoing at the time

[11] European Parliamentary Research Service, 2021: "The assessment finds that while the EU has the competence to adopt the proposed regulation per Article 5 of the Treaty on European Union, the impact of such practices on human and fundamental rights has not been adequately addressed. It should provide a clear legal basis for these practices, along with effective remedies for users. Some technologies covered by the proposed regulation have a disproportionate impact, and thus require additional safeguards unavailable in the proposal in its current form."

of writing this paper and a final agreement has not yet been reached.

6. 4. Is this proposal the right method to tackle encryption?

Many see the proposed EU regulation to prevent and combat child sexual abuse and evidence of grooming as a necessary step towards combating online CSAM while others question whether the proposed legislation is the most effective and appropriate approach to target said sensitive content. In particular, what is most concerning is the disregard the proposal seems to have towards safekeeping encryption, that is at the core of the privacy vs safety debate.

4.1 Legislative critiques

With the proposal for a regulation to 'prevent and combat child sexual abuse' the European Parliament and the Council set out to harmonize and implement new obligations on online service providers to selectively scan users' private messages for CSAM and grooming behavior. According to the proposal, any selected online provider of communications services, if on the receiving hand of a 'detection order' from the EU, would be required to scan its users' messages through technologies approved by the EU. The proposal does not call for the end of encrypted services per se, but it does require companies to install any software the EU deems necessary to detect CSAM and this would make E2EE - as conceived today - effectively impossible. According to Art. 10, section 2, the providers are obliged to: (a) "install and operate technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children", (b) make sure that these technologies are "effective in detecting the dissemination of known or new child sexual abuse material or the solicitation of children [as well as] not able to extract any other information from the relevant communication", (c) and be the "least intrusive in terms of the impact on the users' rights to private and family life, including the confidentiality of communication, and to protection of personal data".

As such, the proposal puts forward the requirement for a technology narrow enough as to not extract any other information from the relevant communication, while at the same time posing that the technology needs to be able to detect known and new

CSAM. This is in itself somewhat of a contradiction seeing as the proposal does not specify nor disclose any information about the technologies to implement, but it simply posits some very vague parameters, leaving room and possibility for more generalized surveillance. The leaked draft on the other hand provided a comprehensive menu of options on how to maintain encryption while at the same time ensuring the detection of CSAM. Unfortunately, the draft, despite being more technologically sound and sophisticated, failed to provide a meaningful solution to the difficult balance between encryption and content detection. The proposal posits to detect *new* and *unknown* CSAM and this leaves the door open to further criticism seeing as service providers would have to scan and detect all conversations in order to find new instances of CSAM and in doing so they would go against the proposal itself as it calls for a "targeted and specific" technology. Therefore, the proposal does not provide clear information on the specific technologies to use nor on the process to ensure that the technologies are effective while also being the least intrusive.

Going further, the provision (26) of the proposal highlights the generalized feeling that it is the firm's job to find efficient ways to maintain privacy and protection while complying with the principle of full disclosure and cooperation for CSAM detection purposes - essentially, it's ordering them to do the impossible. The vagueness of the proposal leaves much room for overindulgence. This aligns with one of the European Digital Rights Association's key concerns: granting too much power to big tech and allowing private companies to be responsible for surveillance and censorship mechanisms, that instead should be the responsibility of public authorities.

The proposal puts great emphasis on the technological side of CSAM detection but does not effectively address the root of the problem: the causes of child sexual abuse. It places significant weight on surveillance and criminalization of online behavior rather than on prevention, education, and rehabilitation for the victims of abuse. Once again this is evidence of how institutions lack the technical understanding and consequently produce proposals and laws which are vague and imprecise, thus unenforceable.

4.2 Policy critiques

It is not clear that the EU's proposal to regulate Child Sexual Abuse (otherwise known as "Chat Control") is the most effective policy instrument to prevent CSAM and protect children from harm on the internet. While the intention of the proposal is admirable, children, as well as adults, rely on E2EE for security and privacy with regards to the threats discussed in Section 2.2, such as government or private misuse of data and limits to freedom of expression. By weakening or removing encryption, the proposal would undermine the autonomy that individuals have over the use of their data and the assurance that their encrypted messages remain private from hackers and the government (Voge, 2022). Not to mention, the proposal is widely unpopular among citizens of the EU (YouGov, 2021).

Although the original proposal claims that its requirements are compatible with E2EE, The Internet Society found that the demands would require the removal or weakening of encryption because there are no existing technologies that can comply with its screening requirements (Voge, 2022). With that said, policymakers have pointed to: 1) encryption backdoors, and 2) client-side scanning to detect CSAM without removing E2EE. Encryption backdoors allow law enforcement to access encrypted messages through a channel that is deliberately designed by the platform's developers. In theory, the solution would enable law enforcement to access encrypted messages. In practice, they create vulnerabilities that can be exploited by hackers, criminals, and other hostile actors, which puts *all* internet users at risk (Voge, 2022 & Radauskas, 2023). With encryption backdoors, internet users must naïvely trust that government agencies and law enforcement are unhackable.

The second solution, client-side scanning, breaks E2EE by scanning users' messages and devices before they are encrypted and sent (Voge, 2022). Similar to encryption backdoors, client-side scanning creates a new vulnerability that can be exploited by hostile actors and place users' safety and security at risk. Furthermore, it proves to be extremely difficult, if not technologically impossible, to identify cases of CSAM with a high level of accuracy using client-side scanning. In an impact assessment commissioned by the European Parliament and presented to the Committee on Civil Liberties, Justice, and Home Affairs, researchers found that there would be a high false positive rate of CSAM images because *all* messages would be

scanned (Tar, 2023). Innocuous images from adult-related exchanges would be flagged and forwarded to law enforcement, which may make internet users feel uneasy. Therefore, the solution would create a backlog for law enforcement and infringe on users' privacy, rather than advancing the identification of CSAM cases. Despite the proposal's claims, the impact assessment was skeptical that the quality of detection would meaningfully improve soon, given the decades of research and development that have already been devoted to identifying cases of CSAM with greater accuracy (Tar, 2023).

EU countries, such as Austria, agencies, and members of EU Parliament have asserted that by weakening encryption, the proposal would consequently undermine trust in messaging services that are essential to "family, medical, and financial lives", as well as democracy (Antrag auf Stellungahme, 2022). In a joint opinion, the European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB) expressed that the proposal goes beyond what is necessary and proportional given the high error rate associated with the technologies (2022, p. 6). In fact, encryption plays an important role in individuals', "private life and confidentiality of communications, freedom of expression as well as innovation and growth of the digital economy," which are dependent on trust and confidence in the privacy that encryption offers (2022, p. 6). Therefore, the two bodies argue that policy should identify more effective ways to balance the tradeoff between fighting abuse and protecting secure modes of communication.

The EU leverages a highly emotional topic, dissemination of CSAM, as a means to attract less criticism for weakening encryption, in the same way that it used terrorism as an excuse to undermine digital security in the past. However, European citizens are not as easily swayed. According to a YouGov poll from 2021, 72% of Europeans are against, "the automatic searching of all personal electronic mail and messages of each citizen for presumed suspicious content in the search for child pornography" (YouGov, 2021). Instead, the EU can continue to prioritize more targeted policy instruments to protect children from CSAM, such as preventing sexual abuse at the source (rather than after dissemination), improved education, providing therapy and support, and reducing backlogs for law enforcement as part of the '2020 EU Strategy for a more effective fight against child sexual abuse' (Negreiro, 2022, pg. 2). In doing so, it is

possible that policy instruments targeted at the root of CSAM can prevent the further dissemination of child pornography without sacrificing the privacy and security of all internet users.

4.3 Where do we go from here?

The EU regulatory landscape on encryption is composed of a combination of legislative and regulatory tools, including laws and regulations, directives, and case law. EU courts, including the Court of Justice of the European Union, have also issued rulings on encryption-related issues. For example, in a 2020 ruling, the Court of Justice of the European Union found that EU member states could not require electronic communications service providers to implement a general and indiscriminate retention of traffic and location data, as this would be inconsistent with EU law and the right to privacy.

Another important regulation that will impact the regulation of encryption is the final adoption of the ePrivacy Regulation (ePR), which is currently being developed by the EU and is expected to replace the current ePrivacy Directive. The ePR will provide specific rules for the protection of personal data in electronic communications and will also address the specificities of the use of encryption. Other regulations and guidelines that address the use of encryption in the EU, are the GDPR, the NIS 1 & 2 Directive, and the European Telecommunications Standards Institute (ETSI) standards. The ETSI standards provide guidelines, technical specifications and best practices for the use and implementation of encryption in various areas, such as telecommunications, electronic signatures, and electronic identification. The ETSI standards may be the most specific encryption regulatory tool in the EU's possession, apart from the upcoming ePR- albeit its relative efficiency, the legal nature of the ETSI standards is non-binding.

Encryption is indeed hard to regulate when the involved parties are coming from widely different legal and cultural backgrounds, as well as possess different levels of technical understanding. In a sense, encryption reflects a broader debate - that of how technology fits into security and ethical norms and what constitutes a fundamental rights' violation in an ever-digitalized world. In the EU, this lack of unanimity may have been reinforced since encryption considerations started quite late, and the discussions

surrounding them were sparked due to politically charged social issues, rather than the technology regulation itself.

To facilitate the urgently-needed discussions, European, international civil society organizations and industry players have coalesced around the topics of encryption and CSAM, with the European Digital Rights Association, highlighting five fundamental rights problems: (1) lacking clarity of services covered and the legal basis for current practices; (2) lacking impact assessment and key public consultations; (3) risking the normalization of exceptional measures; (4) empowering big tech companies, putting private companies in charge of surveillance and censorship mechanisms that, because of their impact on fundamental rights, should be the responsibility of public authorities; and (5) potentially attacking encryption (EDRi, 2022). These overarching categories will be important tools to navigate future discussions and regulation efforts. While regulators from around the globe are pushing for technology-based solutions to encryption, this debate and long-term negotiations showcase the complexity and conflicting interests involved and highlight that the core of the debate is actually the debated fundamentality of encryption.

7. 5. Should there be a fundamental right to encryption in the EU?

5.1 What is a fundamental right?

The concept of fundamental human rights was first established in the Universal Declaration of Human Rights (UDHR) proclaimed at the United States General Assembly on 10 December 1948 in order to set out rights pertaining indiscriminately to all people and across all nations for the first time. Thus, the UDHR is a milestone in the protection of human rights because it defines certain rights as being “fundamental”, implying they apply indiscriminately to all, should be applied universally and should be highly protected against infringement. In fact, these rights are said to be inalienable, meaning they cannot be infringed upon or removed by any entity. The UDHR has paved the way for legally binding treaties such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). (United Nations, Universal Declaration of Human Rights).

5.1.1 Encryption-relevant fundamental rights for UN member nations

The UDHR is not a treaty so it is not legally binding, though some argue it has become binding as customary international law due to its frequent invocation (Australian Human Rights Commission). The rights listed in the UDHR, which are most relevant to the topic of encryption are: (a) the **right to no arbitrary interference with their privacy,** daily, home or correspondence and (b) the **right to the protection of the law against such interference** or attacks (Art. 12 UDHR); (c) the **right to freedom of opinion and expression**, including the freedom to hold opinions **without interference** and to seek, receive and impart information and ideas regardless of frontiers (Art. 19 UDHR); (d) **the right to freely participate in the cultural life of the community** (Art. 27 UDHR).

5.1.2 Encryption-relevant fundamental rights in the European Union

In the European Union, fundamental rights are enshrined in three documents: (1) The European Convention on Human Rights (1950), (2) The Fundamental Freedoms of the European Union (1986) and (3) The Charter of Fundamental Rights of the European Union (2000). The Charter of Fundamental Rights notably establishes all personal, political and economic rights of people in the EU. Though national courts must apply the laws of the European Union, when the violation of a fundamental right is reported, it is up to national courts to decide on the issue because the Charter serves as a complement to national legal systems (European Parliament). The rights enshrined in the Charter which are most relevant to encryption are the right to **respect for private and family life** (Art. 7); the **protection of personal data** (Art. 8)**;** the **freedom of expression and information** (Art. 11); the **freedom of assembly and association** (Art. 12); **non-discrimination** (Art. 21)**;** and **consumer protection** (Art. 38).

5.2 The evolution of fundamental rights in a digitalized EU

The emergence of digital technologies has led to the redefinition of certain fundamental rights and the establishment of new rights. First, with the intensification of data collection and usage, particularly of personal data, concerns emerged about the right of individuals to have their data protected and whether or not it should possess a

fundamental, inalienable nature. The **right to the protection of personal data** is considered as logically flowing from the fundamental right to privacy (Conseil d'Etat Français, 2016). Indeed, Article 8(1) of the EU U and Article 16(1) of the TFEU state all individuals have the right to the protection of their personal data. The GDPR derives from this idea of personal data protection as a fundamental right and tackles some of the new privacy and data problems brought about by new technologies for which no rights have been defined yet. One example is the "right to be forgotten" or "right to erasure" in Article 17 allowing one to request organizations erase their personal data when it is no longer required for the purposes for which it was obtained (Department of Justice Office of Privacy and Civil Liberties, 2022).

Second, there has been an evolution of Article 7 of the EU Charter about privacy to better protect private communications. Article 7 now states that, "*everyone has the right to respect for his private and family life, his home, and his* ***communications***" (Official Journal of the EU C 303/17 - 14.12.2007). The terminology was changed from *correspondence* to *communications* to reflect advancement in technology, indicating the role and importance of technology to private, online communications. Although Article 7 is not an absolute right, the confidentiality of communications remains an important element of fundamental rights in the EU and the "essence of the right" must not be interfered with.

Another example of the impact of digitalization on individual rights is the **calls to recognize a fundamental right to internet access**. Indeed, a significant portion of people have internet access in developed countries, but some groups still struggle to access the internet, for instance, due to the costs for faster internet (Custers, 2022) or lack of infrastructure. Ensuring the right to internet access means ensuring all have the possibility to inform and express themselves online. Though the EU does not recognize internet access as a right, it is being increasingly recognized nationally on the basis that it arises from the right to freedom of speech (Conseil d'Etat Français, 2016). France established internet access as a human right with the Constitutional Council ruling that freedom of speech guaranteed by Article 11 of the Declaration of the Rights of Man and the Citizen "implied the freedom to access such services" (judgment no. 2009-580 DC of 10 June 2009, §12). Similarly, access to broadband internet of at least 1 Mbit/s connections for all citizens has been a constitutional right in Finland since 2010. In

Greece and in Spain, the right to internet access is also recognized to some extent (Custers, 2022). More broadly, in 2016, the UN suggested the recognition of a fundamental right to internet access in order to protect from government censorship and governments' deliberate disruption of internet access (Custers, 2022).

Overall, the digital age has raised various questions about the definition of fundamental rights, their enforcement and the need for new fundamental rights. For instance, private correspondences are increasingly being shared using the same medium as the press and business and states interrogating their right to censor speech and seeking to identify new ways to combat illegal content online. As constitutional texts never fail to acknowledge, fundamental rights can be limited within reason. The question is thus, what consists of a reasonable motive to limit these rights?

When assessing the aforementioned rights in light of the CSAM proposal, it appears that the proposal effectively undermines individuals' fundamental right to data protection, to private communications (EDPB-EDPS, 2022) and could threaten their right to internet access by attempting to weaken or eliminate encryption online messaging platforms. In addition to infringing on the right to protection of data, the CSAM proposal would also likely conflict with precedent set by *Schrems* and *Digital Rights Ireland and Seitlinger and Others*, where the Court ruled that granting law enforcement or the government access to electronic communications would conflict with Article 7, the right to respect for private and family life. While Article 7 does not explicitly mention encryption, analysis of case law suggests that the protection of confidential communications, includes encryption, and should be protected by the Charter of Fundamental Rights of the EU.

5.3 But what would make a right to encryption fundamental?

The rights recognized in the UDHR are universally recognized as fundamental rights, but fundamental rights can vary from one region or nation to another as nations have different references, values and systems for establishing fundamental rights. Indeed, these rights can be laid out in a national constitution, an international covenant or identified through substantive due process of law [12] in countries like the US.

[12] Substantive due process is a U.S. constitutional principle allowing courts to establish and protect certain fundamental rights, even if they are not listed in the Constitution.

In fact, the US provides an interesting conception of fundamentality. Most fundamental rights including the right to freedom of speech (First Amendment), to peaceably assemble (First Amendment) and against unreasonable searches and seizures (Fourth Amendment) are enshrined in the Bill of Rights of the Constitution. In the US, fundamental rights (as compared to human rights) derive from a series of specific legal tests[13] intended, among other things, to determine the historical foundation, the historical protection of potential "fundamental rights" and the depth of a right's engravement in American traditions and consciences. This is how the right to privacy - which is not listed in the Bill of Rights- was extended as a fundamental right by the Supreme Court, resulting from *Union Pacific R. Co. v. Botsford* in 1891. As a result from later case law, this right to privacy has notably come to include (a) the **right not to have one's personal matters disclosed** or publicized; the right to be left alone; (b) **the right against undue government intrusion** into fundamental personal issues and decisions.

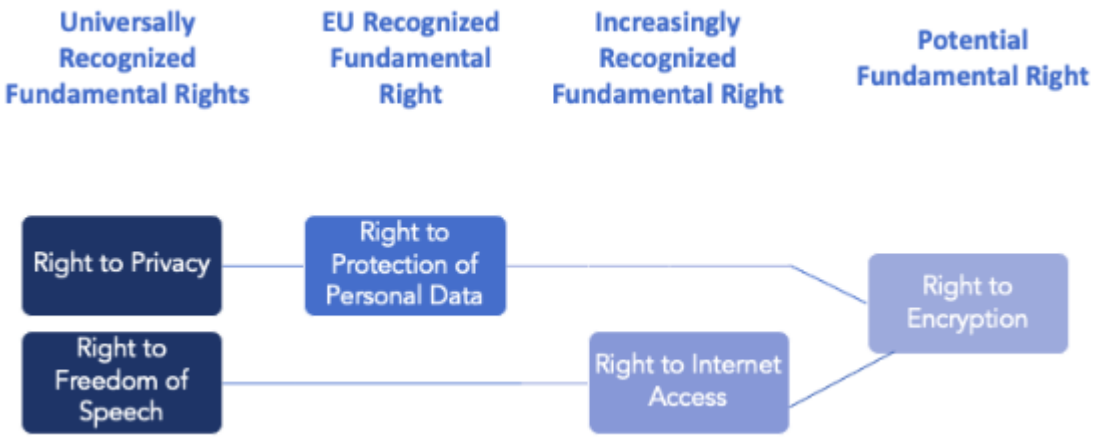
For the purpose of this policy brief focusing on an EU case, we will rely on a broader, less culture- and history-centric definition of "fundamentality". Political Science Professor Daniel N. Hoffman's 1987 article *What Makes a Right Fundamental* essentially holds that the argument required to support that a right is fundamental is that any person might find it fundamental at one point in time. More precisely, Hoffman states what makes a right fundamental, depends on the weighing on the three following questions: (1) "Is the right specifically identified as fundamental by a controlling text or authority, or logically entailed by a right so recognized?" (Hoffman, 1987, p. 527); (2) "Is the right empirically necessary to the realization of a recognized fundamental right?" (Hoffman, 1987, p. 527); (3) "Is possession of the right entailed by what it means to be a person, so that no person devoted to human dignity could reasonably prefer to live in a society in which the right was not recognized?" (Hoffman, 1987, p. 527). So what does this mean for encryption? We will examine each question in order to conclude whether or not encryption could be recognized as a fundamental right.

First, we must establish whether the right to encryption is specifically identified as fundamental by a "controlling text or authority, or logically entailed by a right so

[13] This is due to fundamental rights being highly protected in the US. Any law restricting these rights is evaluated thoroughly through the strict scrutiny process (i.e. the law is assumed to be invalid unless an argument can show the law to be vital to achieve a "compelling state interest" and to be narrowly tailored to that outcome).

recognized." Although the right to encryption itself is not identified in a fundamental text and though no "controlling authority" seems to recognize the right of encryption as such, the UNHCR, for instance, emphasizes the importance of protecting privacy of communications in the digital world to defend the right to privacy, the freedom of association and the freedom of expression using measures like encryption and anonymity (United Nations General Assembly Human Rights Council, 2019). Indeed, the freedom to use encryption technologies seems implied by the right to privacy, to freedom of expression and the right to freely participate in the cultural life of the community, respectively Art.12, Art. 19 and Art.27 UDHR applied to the digital world (Kühnel et al., 2015). Moreover, as mentioned prior, encryption is a technology that allows online personal conversations to be protected and enables individuals to express themselves freely in online communications without fear of persecution and/or restriction of their access to digital platforms. Consequently, encryption seems to enable the right to the protection of personal data (a fundamental right) and the right to internet access (a fundamental right which is increasingly recognized among EU members). Thus, one could conclude that the right to encryption is logically entailed by the right to freedom of expression and to privacy and should be a fundamental right.

Image 3: Representation of the link between the right to encryption and fundamentally recognized right including the right to privacy & the right to freedom of speech



Hoffman's second question concerns whether the right to encryption is empirically necessary to the realization of a recognized fundamental right - a question

asking about the intrinsic link between encryption and the four aforementioned rights. First, Art 12. of the UDHR states individuals have the right not to have interference with their correspondence. Applied to electronic communication, this suggests the state should not intercept and review what you send or receive. That being said, in today's world, even in democratic societies companies and states seem to carry out activities that would not be permitted in the offline world. For instance, states sometimes surveil their citizens' online communications and companies tend to sell data. Indeed, in many ways, digital communications are much easier to intercept than offline conversations or written correspondence. For instance, emails often go through spam filters and there is no way of knowing its privacy has been breached (United Nations General Assembly Human Rights Council, 2019).

Moreover, if the right to the protection of personal data and the right to internet access are considered fundamental rights, no encryption or weakened encryption strongly undermines these rights for both vulnerable groups and the general population. Indeed, as we live in increasingly digitized societies, the right to encryption appears as an important protection for individuals against the state. In resolution 42/15, the UN Human Rights Council calls upon states not to interfere with the use of encryption technologies and to create legislations protecting individual digital communications (United Nations General Assembly Human Rights Council, 2019). Beyond encryption bans, even the implementation of back-door access to encryption for legitimate purposes, has been criticized by the UN Special Rapporteur on freedom of expression in 2015 (Ferrari, 2022) and by Europol claiming that it threatens the privacy required to protect the right to freedom of expression. Therefore, one can conclude that ensuring the right to encryption is a prerequisite to ensure the four aforementioned fundamental rights in the digital world.

Hoffman's final question regards whether the possession of the right to encryption is entailed by what it means to be a person, so that no person could reasonably prefer to live in a society in which the right was not recognized. Given that the right to encryption appears implied by four fundamental rights - two universally recognized (right to privacy and to freedom of expression), an EU recognized fundamental right (right to the protection of data) and one increasingly recognized fundamental right (right to internet access) - and is necessary to their realization, one

would need a truly solid counter-argument to prevent a right to encryption from emerging. Indeed, an individual would only consider living in an encryption-less society if the right to encryption caused more harm than good.

However, advocacy groups and institutions alike recognize that the use of encryption is necessary to the protection of human rights online and offline. The consequences of weakened encryption can threaten human dignity and safety by facilitating criminal activity and state violations of fundamental rights (accessing people's private information and communications, exposing the sources of journalists, subjecting human rights defenders to government action, etc.). Groups at risk including gender and sexual minorities are particularly at risk for privacy violations. These online violations of privacy can translate into offline abuse and violence, but also into these groups being prevented from obtaining crucial information on topics considered taboo. As highlighted by the UNHCR in 2017 and the UN Special Rapporteur on freedom of expression, the ability of these groups to use encryption and anonymity is essential to their exercise of freedom of expression. (Ferrari, 2022) Consequently, the protection of encryption appears essential to protecting a wide array of fundamental rights and to generally, enabling a higher quality of life for individuals (Ferrari, 2022). Thus, it seems incoherent - if given the choice - that one would prefer to live in a society where encryption is banned - particularly since having the right to encryption does not require the individual to exercise that right by using encryption technologies.

All in all, based on the questions raised by Daniel Hoffman to determine whether a right is fundamental, the right to encryption should be recognized as a fundamental right due to its logically following from the protection of other fundamental rights and its being necessary to their realization. Ultimately, we hold that, at all factors considered, a reasonable person would not prefer to live in a world without the right to encryption.

8. 6. Policy recommendations

Having established that encryption should indeed be considered as a fundamental right, the EU proposal for detection of CSAM and grooming behavior should be rephrased, or better should present more detailed technological solutions that would guarantee the integrity of encryption.

6.1 Legislative policy recommendations

The EU must adapt its approach towards regulation to hold big technology companies accountable while simultaneously protecting citizens' fundamental rights. As previously established, encryption can be categorized as a fundamental right by EU standards, yet the Charter of Fundamental Rights in the EU or the current regulatory framework does not explicitly protect a right to encryption, which can lead to legal ambiguity. The EU can consider formalizing encryption as a fundamental right protected by Article 8 of the Charter. The current approach to data protection regulation has been criticized for employing technology neutral policies that can be difficult to enforce. Therefore, to further solidify encryption's role in data privacy, existing data protection regulations, such as the ePrivacy Directive and GDPR, can be updated to clearly specify that encryption is a means to protect against the unlawful processing of data.

If the Commission's ambition is to protect children's fundamental rights to privacy and safety from CSAM, they should focus on their current efforts targeted at the root causes of CSAM. For instance, the '2020 EU Strategy for a more effective fight against child sexual abuse' outlined several actions to improve the legal framework, prevention, and multi-stakeholder response to CSAM (Negreiro, 2022, p. 2). As part of the strategy, in 2023, the Commission plans to update the Child Abuse Directive (2011/93/EC) to patch its weaknesses that arose during the transposition into federal law. On the parliamentary side, the Parliament addressed harmful activities in the digital environment in its 2021 resolution on digital education policy. The combination of these policy instruments may yield a more measurable impact on the safety of children on the internet, as compared to the risks associated with undermining encryption.

6.2 Technical policy recommendations

If the Commission wishes to move forward with the CSAM proposal, they can consider several technical proposals that aim at providing some forms of content detection in E2EE while at the same time maintaining users' right to encryption and privacy.

Firstly, we recommend placing significant attention to **user reporting** and **user agency** through **message franking**. This is a way for the service providers to authenticate that the sender of flagged content is indeed responsible for sending content that was perceived problematic. This happens because the platform can see the sender and receiver identities and can verify reports using specially constructed ciphertexts that support message franking (Tyagi et al., 2019, p. 3). Through this approach, it would be possible to report content both in encrypted one-to-one and group chat settings (Kamara et. al, 2022, p.27). However, at this present time there needs to be further research in order to determine the most effective and efficient techniques to encourage user reporting.

Secondly, we recommend **metadata analysis**, namely 'data about data' analysis, that when applied to encrypted messages would be able to provide valuable information on file size, sender, file type and similar that would allow for meaningful analysis in content detection. In particular, by applying **machine learning (ML)** techniques to metadata analysis it would be possible to have a tool capable of identifying troublesome content by analyzing the quantity or dimensions of messages, and if the volume or dimensions are inconsistent with the providers' established standard for typical messaging behavior then it would be possible to intervene and check the nature of the content shared (Kamara et. al, 2022, p.21). Similarly, ML models could be trained on user behavior of banned users to then be able to detect sharing patterns of prohibited content. However, before using metadata analysis and ML more studies need to be carried out seeing as this method is liable for privacy-breaches risks[14], but there is consensus on the fact that if metadata analysis is confined to users' devices, their privacy is upheld and the assurance of E2EE is maintained (Kamara et. al, 2022, p.22).

Thirdly, we recommend **homomorphic encryption** seeing as it has the potential to balance both security and privacy concerns because it enables calculations to be performed on encrypted data without decrypting it first[15] (NSPCC, 2021, p. 18).

[14] There is evidence that previous metadata analysis used to reveal sensitive data such as the identities of the sender or receiver of encrypted messages. For more detailed information on the topic please refer to: Greschbach, B., Kreitz, G., & Buchegger, S. (2012). The devil is in the metadata—New privacy challenges in Decentralised Online Social Networks. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 333–339. https://doi.org/10.1109/PerComW.2012.6197506

[15] This happens because it converts data into *ciphertext* that can be analyzed and worked with as if it were still in its original form, *plaintext*.

However, this promising tool has very high computational costs and requires modifications and specific training for each use (Hamza et al., 2022, p. 532).

These technical proposals all oppose any modification to the underlying encryption schemes of service providers or any encroaching on the privacy and security guarantees of E2EE and all support encryption as a fundamental right.

9. Conclusion

The EU's proposal to prevent and combat child abuse by screening private messages is well-intentioned. However, as technology currently stands, it would be impossible to enforce the regulation without undermining or eliminating E2EE on online messaging platforms. The collective benefits that encryption has on privacy, trust, and democracy may outweigh the risks posed by creating a shield for pedophiles, terrorists, or other criminals, who will find alternative ways to commit crimes. Therefore, the regulation will do little to address the root causes of crime. Based on the analysis in Section 5, we established that encryption should be cemented as a fundamental right derived from the EU's fundamental right to privacy (Article 8) among others. Instead, the EU may consider policies targeted at the prevention or CSAM, as well as technical proposals that would protect the integrity of encryption without creating backdoors or vulnerabilities that can be exploited by hackers.

10. References

"A Short History of Human Rights." *University of Minnesota Human Rights Resource Center*, http://hrlibrary.umn.edu/edumat/hreduseries/hereandnow/Part-1/short-history.htm. Acharya, B., Bankston, K., Schulman, R., & Wilson, A. (2017). Deciphering the European encryption debate: France. *Open Technology Institute*. https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf

Benner, T., & Hohmann, M. (2018, January 28). *How europe can get encryption right*. POLITICO. Retrieved, from https://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/

Brush, K., Rosencrance, L.,& Cobb, M. (2021, September). "Asymmetric encryption (public key cryptography)". *TechTarget*. https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

Conrad, E., Misenar, S., & Feldman, J. (2012). Domain 5: Cryptography. In E. Conrad, S. Misenar, & J. Feldman (Eds.), *CISSP Study Guide (Second Edition)* (pp. 213-255). https://doi.org/10.1016/B978-1-59749-961-3.00006-6.

Conseil D'Etat Français, 2016, *Fundamental Rights in the Digital Age*, https://www.conseil-etat.fr/Media/actualites/documents/reprise-_contenus/etudes-annuelles/fundamental-rights-in-the-digital-age.pdf .

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 10 April 2023]

Council of the European Union, "German-French Letter Concerning Cooperation Between Law Enforcement Agencies and Electronic Communication Service Providers," November 7, 2016, http://data.consilium.europa.eu/doc/document/ST-14001-2016-INIT/en/pdf.

"Council Resolution on Encryption – Security Through Encryption and Security Despite Encryption," Council of the European Union, November 24, 2020, https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf.

Custers, Bart. (2022). New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era. *Computer Law & Security Review, 44*, p. 105636., https://doi.org/10.1016/j.clsr.2021.105636.

DigitalEurope. (2020, 16 March). Encryption: Finding the balance between privacy, security and lawful data access. *DigitalEurope*. https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf

EDPB-EDPS. (2022). Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. *European Data Protection Protection Board*. Retrieved from https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

EDRI20. (2022, August 16). *European Commission's online CSAM proposal fails to find right solutions to tackle child sexual abuse*. European Digital Rights (EDRi). Retrieved from https://edri.org/our-work/european-commissions-online-csam-proposal-fails-to-find-right-solutions-to-tackle-child-sexual-abuse/

ENISA. (2023, March 13). *NIS directive*. ENISA. Retrieved April 13, 2023, from https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

EPRS. (2021). Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse. *European Parliament*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf

European Commission. (2020). Technical solutions to detect child sexual abuse in end-to-end encrypted communications. *Politico*. Retrieved from https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf

European Commission, 2021, *Protecting Fundamental Rights in the Digital Age – 2021 Annual Report on the Application of the EU Charter of Fundamental Rights*, https://commission.europa.eu/system/files/2021-12/1_1_179442_ann_rep_en_0.pdf. Accessed 19 Apr. 2023.

European Commission. (2022). *European Security Union*. European Commission. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en#:~:text=The%20European%20Security%20Union%20aims,a%20whole%2Dof%2Dsociety%20approach

Ferrari, Veronica. “What Is Encryption and Why Is It Key to Human Rights?” *Association for Progressive Communications*, 23 Sept. 2022, https://www.apc.org/en/news/what-encryption-and-why-it-key-human-rights.

Global Partners Digital. (2023). *World map of encryption laws and policies*. Global Partners Digital. Retrieved from https://www.gp-digital.org/world-map-of-encryption/

Grover, G., Rajwade, T., & Katira, D. (2021). The ministry and the trace: subverting end-to-end encryption. *NUJS Law Review, 14*(2), 1-27.
Hamza, R. et al. (2022). Towards secure big data analysis via fully homomorphic encryption algorithms. *Entropy, 24*(4), 519-536. https://doi.org/10.3390/e24040519

Hoffman, Daniel N. “What Makes a Right Fundamental.” *The Review of Politics*, vol. 49, no. 4, 1987, pp. 515–529., https://doi.org/10.1017/s0034670500035440. Accessed 16 Apr. 2023.

“Human Rights.” *United Nations*, United Nations, https://www.un.org/en/global-issues/human-rights.

IOCTA. (2020). Internet organised crime threat assessment. *Europol*. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Kamara, S., Knodel, M., Llansó, E., Nojeim, G., Qin, L., Thakur, D., & Vogus, C. (2022). Outside looking in: Approaches to content moderation in end-to-end encrypted systems. *arXiv preprint arXiv:2202.04617*.

Knodel, M., Baker, F., Kolkman, O., Celi, S., & Grover, G. (2021). *Definition of End-to-end Encryption (IETF Active Internet-Draft)*. IETF. https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition/

Koomen, M. (n.d.). *The encryption debate in the European Union: 2021 update*. Retrieved April 13, 2023, from https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217

Kühnel, M., Schweda, S., & Härting, S. (2015). OHCHR. *Encryption from a Human Rights Perspective*, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/MarcoKuhnel.pdf. Accessed 18 Apr. 2023.

NCMEC. (n.d). What Happens to Information in a CyberTip? *National Center for Missing & Exploited Children*. https://www.missingkids.org/gethelpnow/cybertipline

Negreiro, M. (2022). Combating child sexual abuse online. *European Parliament.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf

NSPCC. (2021). End-to-end encryption: Understanding the impacts for child safety online. *The National Society for the Prevention of Cruelty to Children*. https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf

OECD, Recommendation of the Council concerning Guidelines for Cryptography Policy, OECD/LEGAL/0289

“Position Paper: An Introduction to Encryption in Europe,” Encryption Europe, January 2021, https://encryptioneurope.eu/positionpaper/.

Prima Santoso, P., Rilvani, E., Budi Trisnawan, A., Adiyarta, K. Napitupulu, D., Sutabri, T., & Rahim, R. (2018). Systematic literature review: Comparison study of symmetric key and asymmetric key algorithm. *IOP Conference Series: Materials Science and Engineering, 420*, 012111. doi:10.1088/1757-899X/420/1/012111

“Privacy Act of 1974.” *Department of Justice Office of Privacy and Civil Liberties*, 4 Oct. 2022, https://www.justice.gov/opcl/privacy-act-1974.

“Protecting Fundamental Rights within the Union.” *Fundamental Rights in the EU*, https://www.europarl.europa.eu/about-parliament/en/democracy-and-human-rights/fundamental-rights-in-the-eu.

Radauskas, G. (2023, January 31). *EU's proposal to combat online child abuse would put kids in more ...* EU's proposal to combat online child abuse would put kids in more danger, expert says. Retrieved April 21, 2023, from https://cybernews.com/editorial/eu-plans-combat-online-child-abuse-risk-to-encryption/

Reuters. (2016, August 23). *France, Germany Press for EU encryption law after attacks*. Reuters. Retrieved April 13, 2023, from https://www.reuters.com/article/europe-attacks-france-germany-idUSL8N1B41UM

Schlesinger, S. W., & Yanisky-Ravid, S. (2022). The right to data encryption. *San Diego Law Review, 59*, 569-598. https://digital.sandiego.edu/cgi/viewcontent.cgi?article=3444&context=sdlr

Song, S. (2020). Keeping Private Messages Private: End-to-End Encryption on Social Media. In *Boston College Intellectual Property and Technology Forum* (Vol. 2020, pp. 1-12).

Stupp, C. (2016, March 30). *EU cybersecurity agency slams calls for encryption backdoors*. www.euractiv.com. Retrieved, from https://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-backdoors/

Tar, J. (2023, April 13). *EU Parliament Study Slams Online Child Abuse Material Proposal*. www.euractiv.com. Retrieved April 21, 2023, from https://www.euractiv.com/section/law-enforcement/news/eu-parliament-study-slams-online-child-abuse-material-proposal/

“The Bill of Rights to the U.S. Constitution.” *American Civil Liberties Union*, https://www.aclu.org/other/bill-rights-us-constitution.

Tyagi, N., Grubbs, P., Len, J., Miers, I., & Ristenpart, T. (2019). Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption. In: Boldyreva, A., Micciancio, D. (eds) Advances in Cryptology – CRYPTO 2019. CRYPTO 2019. Lecture Notes in Computer Science(), vol 11694. Springer, Cham. https://doi.org/10.1007/978-3-030-26954-8_8

United Nations General Assembly Human Rights Council, The right to privacy in the digital age (27 September 2019) UN Doc A/HRC/RES/42/15

"United States Constitution, Bill of Rights, Declaration of Independence." *United for Human Rights*, https://www.humanrights.com/what-are-human-rights/brief-history/declaration-of-independence.html.

"Universal Declaration of Human Rights." *United Nations*, United Nations, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Voge, Callum. "European Commission Proposal to Prevent and Combat Child Sexual Abuse." *Internet Society*, 19 Aug. 2022, https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-eu-proposal-to-prevent-and-combat-child-sexual-abuse/.

We cannot risk that the EU becomes a safe haven for paedophiles and sexual predators online. Child Rights Manifesto. (2021, January 22). Retrieved from https://www.childrightsmanifesto.eu/we-cannot-allow-the-eu-to-become-a-safe-haven-for-paedophiles-and-sexual-predators-online/

"What Does Free Speech Mean?" *United States Courts*, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does.

"What is encryption? | Types of encryption". *CloudFlare*. https://www.cloudflare.com/en-gb/learning/ssl/what-is-encryption/

"What Is the Universal Declaration of Human Rights?" *The Australian Human Rights Commission*, https://humanrights.gov.au/our-work/what-universal-declaration-human-rights.

YouGov. *Poll: 72% of Citizens Oppose EU Plans to Search All Private Messages for Allegedly Illegal Material and Report to the Police*, 4 Nov. 2021, https://www.patrick-breyer.de/en/poll-72-of-citizens-oppose-eu-plans-to-search-all-private-messages-for-allegedly-illegal-material-and-report-to-the-police/

About the authors :

Stavroula (Stavrina) Chousou is a 1st year Master of Public Policy candidate specializing in Digital, New Technology and Public Policy. Upon graduating from the University of Piraeus, with an undergraduate degree in International and European Relation, she pursued a research traineeship at the Institute of International Affairs in Athens. There she mainly focused on the use and impact of technology in the unfolding Ukrainian War, as well as the rising state competition for technology supremacy in AI and Quantum Computing. At Sciences Po, Stavrina navigates new approaches combining technical and policy tools to balance ethical and security concerns in rising technologies.

Morgan Williams is a 1st year Master of Public Policy candidate specializing in Digital, New Technology and Public Policy. After completing a BA in Economics at the University of Maryland, Morgan spent two years as an OECD Young Associate where she contributed to multiple strands of the research programme on AI and Work, Innovation, Productivity and Skills (AI-WIPS), as well as research on the platform economy and domestic outsourcing. At Sciences Po, Morgan's primary interests lie in the intersection between technology, work and US & EU regulations.

Ludovica Pavoni is a 1st year Master of Public Policy candidate specializing in Digital, New Technology and Public Policy. Whilst pursuing her undergraduate degree in International Affairs at John Cabot University, Ludovica interned in a venture capital focusing on AI, VT, and AR. From this experience Ludovica's interests and research has focused on how to best approach technological advancement and how to best address big data application to the public sector.

Julia Magaud is a 1st year Master of Public Policy candidate specializing in Digital, New Technology and Public Policy. After completing her undergrad as a Political Humanities major at Sciences Po, Julia worked on a research project linking an AI company to London borough councils to improve urban planning. Julia is particularly interested in smart cities and the digitalization of the public sector to improve the delivery of public services.

About the Digital, governance and sovereignty Chair:

Sciences Po's Digital, Governance and Sovereignty Chair's mission is to foster a unique forum bringing together technical companies, academia, policymakers, civil societies stakeholders, public policy incubators as well as digital regulation experts. Hosted by the School of Public Affairs, the Chair adopts a multidisciplinary and holistic approach to research and analyze the economic, legal, social and institutional transformations brought by digital innovation. The Digital, Governance and Sovereignty Chair is chaired by **Florence G'sell**, Professor of Law at the Université de Lorraine, lecturer at the Sciences Po School of Public Affairs.

The Chair's activities are supported by: