GESELLSCHAFT FÜR FREIHEITSRECHTE

22 FEBRUARY 2023 | EXPERT OPINION TO THE DIGITAL AFFAIRS COMMITTEE OF THE GERMAN BUNDESTAG

CHAT CONTROL

THE EU COMMISSION'S DRAFT REGULATION ON CHAT CONTROL AND ITS INCOMPATIBILITY WITH THE EUROPEAN CHARTER OF FUNDAMENTAL RIGHTS

CONTENT

INTRODUCTION

The EU Commission's draft regulation[1] (Chat Control Regulation) raises significant fundamental rights concerns. The fight against sexual violence against children is an objective that is essential for the protection of children and their rights and can justify restrictions of other fundamental rights. However, there are considerable doubts about the suitability, effectiveness and proportionality of the proposed measures. We are convinced that the draft violates the EU Charter of Fundamental Rights at crucial points.

The five most important fundamental rights objections to the chat control proposal are summarised in this expert opinion.

The EU Commission's proposal is based on Article 114 TFEU[2], the harmonisation of the European internal market. By choosing this legal basis, the EU Commission commits itself to countering sexual violence against children by means of economic regulation. The draft proposes a catalogue of obligations for online services such as interpersonal communication services, hosting services, app stores and internet access providers. These categories are defined very broadly, so that many different service providers will be required to take measures that impact fundamental rights:

Interpersonal communication services are, for example, **e-mail services such as Gmail** or **instant messaging services such as WhatsApp**. These enable private communication via the internet, with numerous services offering end-to-end encryption. The obligations for interpersonal communication services under the chat control draft also apply to encrypted services where the provider has no means of accessing the contents of users' private communication. Hosting includes all services that store content on behalf of their users. It does not matter whether this content is made accessible to third parties. A **private cloud storage service such as Dropbox** is equally affected by the hosting obligations of the chat control proposal as a public **social media network such as Instagram** or a **non-commercial discussion forum**. App stores are service providers that mediate between software developers and users when apps are downloaded. An app store is usually required to install apps on modern smartphones. The rules of the chat control proposal apply not only to the powerful **app stores of Google and Apple**, which are pre-installed on Android devices and iPhones respectively, but also to **open-source alternatives such as f-droid**.

The proliferation of depictions of sexual violence against children via economic actors on the internet, or the misuse of these online services to perpetrate sexual violence against children, is one facet of a serious problem that requires a holistic societal response. Around three quarters of the cases take place in the child's immediate social environment or family.[3] In the last section of this opinion, we therefore point to

[1] **European Commission,** Proposal for a regulation by the European Parliament and the Council laying down rules to prevent and combat child sexual abuse, 2022, COM(2022) 209, 2022/0155/COD.
[2] Treaty on the Functioning of the European Union.
[3] **German Federal Ministry for Family Affairs, Senior Citizens, Women and Youth**, „Schieb den Gedanken nicht weg!" Kampagne für ein Umdenken bei sexueller Gewalt gegen Kinder gestartet, 17.11.2022.

alternative, effective, fundamental rights-compliant approaches which the legislature should pursue in order to fulfil its duty to protect children from sexual violence. However, without a change of the legal basis Art. 114 TFEU and a completely new conception of the draft, the European legislator cannot take up these important measures, as they go far beyond economic regulation. The Chat Control Regulation thus threatens to do a disservice to child protection by narrowing the political debate to monitoring and blocking obligations that would not hold up in court due to blatant violations of the EU Charter of Fundamental Rights.

1. CHAT CONTROL VIOLATES THE RIGHT TO PRIVACY

The EU Commission's proposal provides for a whole range of obligations for online services such as internet access providers, app stores, hosting platforms and interpersonal communications services. Interpersonal communications services are, for example, email services such as Gmail or instant messaging services such as WhatsApp. The term "chat control" is often used colloquially to refer to the EU Commission's draft regulation as a whole. Chat control in the narrower sense is the part of the draft according to which **authorities can oblige providers of communications services such as WhatsApp or Signal to monitor their users' private communications**. This is a particularly serious restriction on rights to privacy and the protection of personal data (Arts. 7 and 8 of the EU Charter of Fundamental Rights): The monitoring is not limited to persons specifically suspected of having committed a crime. Additionally, unlike data retention, which is also incompatible with the Charter but is limited to metadata – i.e. information about who communicated with whom at what time – chat control includes the surveillance of the contents of private messages, which is even more invasive.

Authorities can impose so-called "detection orders" against providers of interpersonal communications services. This means that authorities can, for example, oblige messenger services **to monitor the communications of all their users**. It is sufficient that the authority has identified a significant risk that the service in question is being used for the dissemination of depictions of sexual violence against children. Detection orders are not targeted, i.e. they do not have to be limited to monitoring the communications of specific users who are under suspicion. Instead, authorities can order that the content of all communications of all users of the service be monitored preventatively. This is therefore a form of mass surveillance without probable cause.[4]

Such a detection order can oblige service providers to filter content for known as well as unknown depictions of sexual violence against children. In addition, they can include an obligation to automatically detect attempts by adults to solicit minors (grooming). Content detected in this way must be forwarded by the service providers to a newly-created EU centre, which will pass the information on to the law enforcement authorities of the member states after a superficial plausibility check. Even the suitability of this measure to effectively counter the spread of depictions of sexual violence against children on the internet is doubtful. Successful investigations by German law enforcement agencies in the past have shown that criminals often only exchange the keys to files stored in encrypted form on hosting providers via

[4] See **Bäcker/Burmeyer**, My spy is always with me: Comments on the planned obligations of Internet service providers to combat sexualized violence against children (so-called "chat control" regulation), Verfassungsblog 2022.

interpersonal communication services. The links to these files are in turn exchanged in darknet forums. If criminals proceeded in this way, as in the case of "Boystown",[5] for example, chat control would be completely moot because neither the automatic filtering of interpersonal communication services nor of hosting services could detect the content exchanged.

Although service providers are free to choose which technologies to use to comply with the detection order, these technologies must in any case be able to analyse the contents of communications. This obligation comes with the inherent risk that even legal intimate communications between users will be viewed by the staff of the technology companies, forwarded to the authorities and, in the worst case, even passed on to criminals through data leaks. Talk of "technological neutrality" in the context of the Chat Control Regulation is misleading, because no technologies exist or are conceivable that can fulfil the requirements of the draft regulation while guaranteeing the confidentiality of legal communications.

In order to detect known depictions of sexual violence against children ('known CSAM'), an automated comparison of sent media files with a reference database may be sufficient. **To detect unknown depictions of sexual violence ('new CSAM') and grooming ('solicitation'), machine learning must be used** to analyse the semantic content of chats, as well as the meaning of audio and video communications. These methods are particularly prone to error: they only make an assumption about the meaning of the content based on patterns in the analysed communication - without actually understanding the content or the context of the conversation. There are no known technologies capable of reliably distinguishing unknown illegal content from legal communications.

In its case law on data retention, the European Court of Justice has indicated that indiscriminate mass surveillance of the contents of communications would violate the essence of the right to privacy.[6] **Indiscriminate mass surveillance is incompatible with the fundamental rights to privacy and data protection under the EU Charter**, whether it involves encrypted or unencrypted communications. At the centre of public criticism of chat control, however, is the fact that the draft regulation does not exempt end-to-end encrypted communication services from detection orders. These services ensure that only the people involved in a private conversation can read the communication content – neither the service provider nor third parties can decrypt it. More and more people are specifically choosing end-to-end encrypted messengers to protect themselves. If the provider of such a messenger receives a detection order, it cannot reject it on the grounds that the service provider cannot access the contents of its users' communications. The EU Commission's draft pays lip service to the importance of end-to-end encryption. However, it states that service providers may only choose between technologies that allow them to detect illegal content in private communications. In other words, service providers who offer end-to-end encryption without backdoors will not be able to implement any detection orders they may receive from authorities and thus will come into conflict with the law. This attack on end-to-end encryption increases the intensity of the restriction of fundamental rights caused by the Regulation's proposed indiscriminate mass surveillance.

---

5 **Der Spiegel**, Mutmaßliche »Boystown«-Administratoren: Vier Männer stehen wegen Missbrauchsseite vor Gericht, 14.09.2022.

6 "So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, ***it is not such as to adversely affect the essence of those rights given that***, as follows from Article 1(2) of the directive**, *the directive does not permit the acquisition of knowledge of the content of the electronic communications as such***", Court of Justice of the European Union, judgment of 8 April 2014, *Digital Rights Ireland*, joint cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 39, emphasis by the author. See also **Tuchtfeld**, "Thank you very much, your mail is perfectly fine" - How the European Commission wants to abolish the secrecy of correspondence in the digital sphere, Verfassungsblog 2022.

2. THREAT OF CHILLING EFFECTS FOR COMMUNICATION FREEDOMS

The European Court of Justice has already warned on several occasions that **indiscriminate mass surveillance has an indirect negative impact on freedom of expression** (Article 11 of the EU Charter of Fundamental Rights): communication participants are prevented from freely expressing their opinions if they cannot be sure of the confidentiality of their communications.[7] This particularly affects professional secrecy holders, such as journalists communicating with their sources, but also whistleblowers, opposition activists or people in war zones. In Ukraine, for example, the download of encrypted messaging app Signal rose by over 1000% compared to previous months in the two months following the start of Russia's war of aggression against Ukraine.[8] The danger of so-called **"chilling effects", i.e. a deterrent effect for the exercise of the fundamental right to freedom of expression and information**, will be exacerbated if the **Chat Control Regulation, as proposed by the EU Commission, attacks the end-to-end encryption of messenger services**. The aforementioned groups of people use such messengers for good reason. If this possibility is taken away from them because service providers have to weaken end-to-end encryption, considerable chilling effects can be expected.

This effect occurs regardless of whether service providers monitor the contents of private communications through a backdoor in the encryption technology or by scanning the content on the user's device before it is encrypted (client-side scanning). The communication participants expect their communication to remain confidential from the moment when they enter a message into the chat programme on their mobile phone – not only at the moment when this message is delivered to its addressee. The decisive factor is that the expectation of confidentiality and integrity of the communication process is shaken to such an extent that those affected feel compelled to restrict the exercise of their freedom of communication themselves.

The Chat Control Regulation threatens to provoke chilling effects far beyond the borders of the European Union. Once implemented in technology, security vulnerabilities can be exploited by intelligence agencies or criminals around the world. Moreover, if providers in the EU must make adjustments to their interpersonal communications services to weaken encryption, there is a high likelihood that they will roll out these changes globally - whether for business reasons or due to pressure from third countries. **Authoritarian regimes like to take advantage of the "Brussels Effect,"** that is, the tendency of European regulation to set global standards. They can expect less criticism for repressive laws on the international stage if the European Union has already moved ahead with similar surveillance measures.

Children, too, the intended beneficiaries of the Chat Control Regulation, have a right to privacy and could be particularly negatively affected by these chilling effects. As minors get older, private internet use plays an increasingly important role in the development of their personality. If children and adolescents are affected by sexual violence in their personal environment, confidential communication via the internet can be a way

7 Court of Justice of the European Union, Judgment of 6 October 2020, *La Quadrature du Net i.a.*, C-511/18, ECLI:EU:C:2020:791.
8 **Report of the Office of the United Nations High Commissioner for Human Rights**, The Right to Privacy in the Digital Age, 04. August 2022.

to access help services. The expectation that private communication content will be monitored can therefore prevent those affected from making use of such resources.

3. DE FACTO FILTERING OBLIGATIONS FOR HOSTING PROVIDERS WITHOUT SAFEGUARDS

Public criticism of the proposal has concentrated on the phrase "chat control", which highlights the planned obligations on messengers to scan private chats. But the planned obligations for hosting services that store third-party content on behalf of their users do not stand up to fundamental rights scrutiny either. Hosting services include those that make third-party content publicly available (platforms such as YouTube, hosting services of public websites) as well as those that offer their customers private cloud storage (Dropbox, iCloud Drive). They also include services where content is only accessible to a certain closed group of people (private accounts on Twitter, closed groups on Facebook, hosting providers of company websites with restricted access). Insofar as the planned obligations for hosting providers relate to non-public content, **the threats to privacy and freedom of expression described under sections 1. and 2. of this paper are also relevant for hosting services.** In addition, there are specific problems: many of the envisaged procedural fundamental rights safeguards for detection orders may end up being evaded entirely in the case of hosting services. This is due to the different privacy rules for communications on messengers on the one hand, and hosting services on the other.

Hosting services (including private cloud storage providers such as Google Drive or Dropbox) can not only be required to scan private content under the Chat Control Regulation, but they may also scan content voluntarily. The Chat Control Regulation stipulates that all service providers must first carry out their own risk analysis as to whether their services pose a risk of being abused for sexual violence against children. Only if, in the view of the authorities, a service provider responds to this risk analysis with insufficient voluntary measures, will they impose a detection order. The risk mitigation measures taken by hosting services are therefore not truly voluntary, but serve the purpose of avoiding an official order. However, by giving the hosting services only vague guidelines as to what these risk mitigation measures should look like, the EU Commission is undermining the effective protection of fundamental rights: In the context of these self-selected measures, **hosting service providers may resort to error-prone filters to monitor private user uploads**. In this scenario, none of the fundamental rights safeguards for detection orders included in the draft regulation will be applied to those risk mitigation measures.

In this respect, hosting services differ from messenger services: Messenger and email programmes such as WhatsApp, Signal or Proton Mail fall under the e-Privacy Directive, which in principle prohibits these service providers from monitoring the private communication content of their users. The temporary derogation from this prohibition, which itself raises serious fundamental rights concerns,[9] is to be replaced by the Chat Control Regulation. After the Chat Control Regulation comes into force, messengers and email service providers may only access the contents of private communications based on a detection order.

[9] **Colneric,** Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament, 2021.

For hosting providers such as private cloud storage, on the other hand, the e-Privacy Directive with its ban on monitoring private communications does not apply.

For hosting providers, it will regularly be attractive to avoid a looming detection order through "voluntary" measures. In this way, the companies retain more control – also over the costs. There is a **strong incentive to avoid costly measures to protect users' fundamental rights**.

Before imposing a detection order, an authority must weigh the risk posed by the service against the interference with the users' fundamental rights. In this regard, the European Court of Justice has set narrow limits for the mandatory use of filtering systems.[10] These are only compatible with the EU prohibition of general monitoring obligations if the filters function so faultlessly that the service providers do not have to perform an "independent assessment of the content" in order to rule out false positives. At least **in the case of unknown depictions of sexual violence against children and grooming, the filter systems are incapable of meeting the Court's standards**. If a hosting service "voluntarily" filters content as part of its duty to minimise risk, there is no public assessment of **whether the filtering systems are compatible with users' fundamental rights**.

As a result, large amounts of private content, such as consensually shared intimate photos on adults' smartphones that are automatically stored in the cloud would be automatically identified and inspected by service providers. Data leaks or untrustworthy employees sifting through the data on behalf of the companies can cause this information to become public. Such false positives can also lead to innocent users being inadvertently locked out of their accounts or even falsely reported to law enforcement authorities.[11] Those affected can then suddenly no longer access their files and are not compensated for the resulting loss of business or negative consequences for their personal lives.

4. WEBSITE BLOCKING OBLIGATIONS REQUIRE SURVEILLANCE OF INTERNET USERS

The draft regulation provides for blocking obligations on internet access providers relating to individual websites (URLs). Before an authority issues a blocking order, it must require internet access providers to provide the authority with information about users' access to the URL in question. To be able to collect the necessary information about the access to individual URLs and pass it on to the authorities**, internet access providers would have to monitor the surfing behaviour of all their customers preventively and comprehensively**. However, such surveillance would **be incompatible with the prohibition on general monitoring obligations and with the fundamental right to privacy**. Additionally, this information is technically inaccessible to the internet access providers if the URL is encrypted using the https protocol.

[10] Court of Justice of the European Union, Judgement of 26 April 2022, *Poland v Parliament and Council*, C-401/19, ECLI:EU:C:2022:297.
[11] **The New York Times**, A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal, 21.08.2022.

Almost all websites now use https to ensure that, for example, address or credit card data that users enter into web forms is transmitted in encrypted form. The widespread use of https is recommended by the Federal Office for Information Security.[12]

The targeted blocking of individual URLs is equally impossible for internet access providers without abandoning https encryption[13] and monitoring the contents of their users' online activities. DNS-based website blocking is not suitable for the planned blocking of individual URLs, because DNS blocking always affects entire domains. A DNS block directed against an individual file on a share hosting platform would also affect all other content hosted by the same share hoster and would thus not meet the requirement of the European Court of Justice that website blocking must be strictly targeted.[14] In practice, therefore, there is a **considerable danger that internet access providers will either over-comply with the blocking orders to the detriment of users' freedom of expression and information** by using DNS blocking to block access to an entire domain. Or they will attempt to implement prima facie targeted blocking and therefore monitor the surfing behaviour of their customers, while sacrificing the security of online communications via https encryption in the process.

5. AGE VERIFICATION ENDANGERS FREEDOM OF COMMUNICATION

The draft regulation stipulates that all providers of interpersonal communications or hosting services that are at risk of being used for grooming must **verify the age of their users**. The risk identified does not have to be significant – the obligation to implement age verification would therefore apply in principle to all email and messaging services that enable communication between minors and adults. Only service providers that can completely rule out any risk that their services may be used for grooming are exempt from the age verification obligation. However, to completely rule out the possibility of adults communicating with children via a service, a service provider must know the age of its users, so *de facto* the age verification obligation applies to all providers of interpersonal communication services or hosting services.

In addition, the age verification obligation also applies to all app store providers. They must also prevent underage users from downloading apps that pose a significant risk of being used for grooming. **This measure severely restricts the fundamental communication rights of minors**, especially teenagers. App stores would have to categorically block them from installing certain apps, without any assessment of their rights to freedom of expression and information against the risk the app poses to underage users. Of course, the grooming risk of an app is greatest when it is popular with both minors and adults. Regardless of their individual level of development, all minors would be completely excluded from these apps.

12 See **Federal Office for Information Security**, Basic IT security tips.
13 See **European Data Protection Board**, Proposal to combat child sexual abuse online presents serious risks for fundamental rights, 29.07.2022.
14 Court of Justice of the European Union, Judgement of 27 April 2014, *UPC Telekabel Wien*, C-314/12, ECLI:EU:C:2014:192.

Due to the strong market concentration in this area,[15] the possibilities to switch to an alternative app store are limited if a market leader attributes a significant grooming risk to a certain app and unjustifiably blocks underage users from downloading it. Even the few alternatives to Apple and Google on the app store market, such as the open-source project f-droid for Android devices, will be affected by the age verification requirement.[16] As a result, the Chat Control Regulation threatens the very existence of those open-source alternatives. Due to their decentralised nature, these projects are unable to implement a centralised age verification system and thus comply with the app store obligations from the draft regulation. Thus, the proposal threatens to exacerbate the very market concentration in the app store market that the EU is currently trying to alleviate with another regulation, the Digital Markets Act[17].

Service providers may choose between age assessment methods (for example, AI-based facial analysis, as already used by Instagram[18]) and age verification methods (using an identity document or digital proof of identity). **Both procedures are extremely intrusive for users**.

Age verification via identity documents comes close to abolishing the right to anonymous internet use, which the German government has promised to uphold in its coalition agreement. All signs indicate that the planned European ID wallet will not support data minimisation when verifying a person's age of majority either. Neither the EU Commission's draft regulation on the European digital identity[19] (EIDAS) reform, nor the Council's negotiating mandate,[20] prevent companies that query the age of majority using the digital identity mechanism from accessing personal data such as a person's date of birth or their legal name.[21] There is therefore no technical solution for age verification on the horizon that would be compatible with anonymous internet use.

AI-supported facial analysis, on the other hand, is often outsourced by service providers to external companies, leaving users with little control over the handling of this particularly sensitive personal data. If the technology makes a wrong assessment, **young-looking adults can also be excluded from using certain apps**. Those who do not possess identification documents or do not want to entrust their sensitive biometric data to a company are excluded from crucial communication technologies. Using a modern smartphone without an app store becomes practically impossible. Doing without messenger services is also unreasonable, especially for people who, for good reason, attach particular importance to anonymous internet use (whistleblowers, victims of stalking, politically persecuted people). In contrast to service providers, **users cannot always choose between different age verification procedures**.

15 See **Gesellschaft für Freiheitsrechte e.V.**, Fundamental Rights Obligations of Digital Corporations, 2022.
16 **Elina Eickstädt. Netzpolitik**, Chatkontrolle: Akute Gefahr für offene Software, 27.12.2022.
17 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector.
18 See **Instagram**, Introducing New Ways to Verify Age on Instagram, 23.06.2022.
19 **European Commission**, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 2021. COM(2021) 281, 2021/0136/COD.
20 **Council of the European Union**, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity – general approach, 25.11.2022, 14959/22. https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/en/pdf
21 The European Parliament has yet to adopt its negotiating mandate.

6. FUNDAMENTAL RIGHTS-PRESERVING ALTERNATIVES

By choosing Article 114 TFEU as the legal basis for its proposal, the European Commission has committed itself to countering sexual violence against children by regulating economic actors. The European Commission justifies its legislative competence by claiming that "barriers to the Digital Single Market for Services have started to emerge following the introduction by some Member States of diverging national rules to prevent and combat online child sexual abuse."[22] Purportedly, the draft regulation would thus serve to remove these barriers to the internal market and prevent the emergence of new barriers to the cross-border provision of online services.

This justification is not convincing. All of the services covered by the draft Chat Control Regulation also fall within the scope of the recently adopted Digital Services Act. The Digital Services Act has fully harmonised the obligations of these service providers to combat the dissemination of illegal content by their users. The danger invoked by the European Commission that national legislation to combat sexual violence against children on the internet would promote fragmentation of the European internal market therefore does not exist.

This does not mean that online services should be free from any responsibility for the protection of children. However, the justification for such requirements should be the state's duty to protect the fundamental rights of all those affected, not the harmonisation of the European internal market. In fact, sexual violence against children is also a serious problem on the internet, and combating it is essential for the protection of children and their rights. The dissemination of depictions of sexual violence against children via the Internet contributes to the constant re-traumatisation of those affected, and the use of online services by criminals for grooming purposes also requires appropriate, effective, and proportionate countermeasures.

Within the legal basis chosen by the European Commission, proposals for alternative, fundamental rights-preserving measures to protect children must be directed at online services. The rapporteur of the European Parliament's Internal Market Committee seeks to make the most of this very narrow framework. In his recently published draft opinion,[23] he plans to eliminate some particularly serious violations of fundamental rights such as client-side scanning, age verification, and the automatic detection of unknown depictions of sexual violence or grooming. Instead, he wants to require interpersonal communications services and hosting services to protect children through particularly privacy-friendly default settings (privacy by design and by default), easy-to-find and age-appropriate information about risks of the service and counseling resources, as well as child-friendly and expedited reporting channels for suspicious content. While these proposals must be subject to a proportionality assessment with regard to the additional personnel costs for the services concerned, we believe that they are fundamentally better suited to ensure the necessary balance between the various fundamental rights affected than the Commission's empty promises of technical solutions.

However, even such a fundamental reorientation of the obligations for online service providers falls short of effectively combating sexual violence against children. We welcome the fact that the German government is taking

22 **European Commission**, Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse, 2022, COM(2022) 209, 2022/0155/COD, Explanatory Memorandum, Legal Basis, Subsidiarity and Proportionality, p. 7.

23 **European Parliament**, Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. 08.02.2023.

account of the particular danger of sexual violence in the home life of children and young people through measures such as the campaign "Don't push the idea away!" of the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth. However, the recognition of this danger is not yet sufficiently reflected in public support for prevention and assistance services. As an illustrative example, we would like to refer to the inadequate telephone hours of the Sexual Abuse Help Line of the Independent Commissioner on Child Sexual Abuse.[24]

We also hope that the debate on chat control will increase legislators' awareness of the inadequacies of law enforcement in the digital public sphere. Recommendations for improving law enforcement should be based on an analysis of previous successful investigations against criminal structures on the internet, such as the "Boystown" case. In these cases, undercover investigators played a central role. They must be supported by training and fair working conditions in view of their particularly psychologically demanding tasks.

Instead, the chat control proposal threatens to keep law enforcement agencies busy with numerous reports of false positives. There is also a danger that reports of consensual sexting among youth will increase. Since such content may well fulfill the criminal offense of § 184c, the authorities are obligated to follow up on such reports and prosecute those minors. Such proceedings can divert much-needed human resources from undercover investigations against adult offenders. A review of § 184b with a view to correcting the sentencing framework in order to allow public prosecutors to refrain from prosecution in certain cases, as recently decided by the 93rd Conference of Ministers of Justice of the German states, would also be advisable with a view to better prioritising limited law enforcement resources.

We hope that this selection of more appropriate, fundamental rights-preserving alternatives to chat control illustrates that the state's options for preventing and effectively combating sexual violence against children are far from exhausted. A rejection of the draft Chat Control Regulation should be accompanied by a package of measures that accounts for the particular seriousness of these crimes, without creating a false dichotomy between child protection and the protection of confidential communications.

[24] Monday, Wednesday and Friday from 9 to 14, Tuesday and Thursday from 15 to 20, not on federal holidays, on 24 or 31 December. Hilfe-Portal Sexueller Missbrauch. Ein Angebot der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs. Accessed on 21.02.2023.