DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Committee on Surveillance and Information Technology

on the Public Consultation of the European Commission on Fighting Child Sexual Abuse: Detection, Removal and Reporting of Illegal Content Online

Position Paper No.: 29/2021 Berlin/Brussels, April 2021

Members of the Committee Surveillance

- Rechtsanwältin Lea Voigt, Bremen (chair)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin (rapporteur)
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied)
- Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied)

In charge in the Berlin office

- Rechtsanwalt Max Gröning

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparency Register ID number:
87980341522-66

www.anwaltverein.de

Members of the Committee Information Technology

- Rechtsanwalt Dr. Helmut Redeker, Bonn (chair and rapporteur)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

In charge in the Berlin office

- Rechtsanwältin Nicole Narewski

Contact in Brussels

- Rechtsanwältin Eva Schriever, LL.M.
- Hannah Adzakpa, LL.M.

Mailing List:

Europe

- Europäische Kommission
    - Generaldirektion für Kommunikationsnetze, Inhalte und Technologien (CNECT)
    - Generaldirektion Migration und Inneres (HOME)
    - Binnenmarkt, Industrie, Unternehmertum und KMU (GROW)
- Europäisches Parlament
    - Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE)
    - Ausschuss für die Rechte der Frauen und die Gleichstellung der Geschlechter (FEMM)
- Rat der Europäischen Union
- Ständige Vertretung der Bundesrepublik Deutschland bei der EU
- Justizreferenten der Landesvertretungen
- Rat der Europäischen Anwaltschaften (CCBE)
- Bundesverband der Freien Berufe (BFB) Büro Brüssel
- Deutscher Steuerberaterverband (STVB) Büro Brüssel
- Bundesärztekammer (BAEK) Büro Brüssel

Germany

- Bundesministerium des Innern
- Bundesministerium der Justiz und für Verbraucherschutz
- Rechts- und Verbraucherschutzausschuss des Deutschen Bundestages
- Innenausschuss des Deutschen Bundestages
- Arbeitsgruppe Recht und Verbraucherschutz der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien
- Landesjustizministerien
- Rechts- und Innenausschüsse der Landtage
- Justizministerien und -senatsverwaltungen der Länder
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Bundesgerichtshof
- Bundesanwaltschaft
- Bundesrechtsanwaltskammer
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Europäische Kommission - Vertretung in Deutschland
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Vorstand und Landesverbände des DAV
- Vorsitzende der Gesetzgebungs-und Geschäftsführenden Ausschüsse des DAV
- Vorsitzende des FORUM Junge Anwaltschaft des DAV

Press

- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter
- Jur
- PCNetzpolitik.org
- Heise
- LTO
- EDRI
- Agence Europe

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising more than 62.000 German lawyers and lawyer-notaries in 252 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level.

I. Summary

The public consultation on *Fighting child sexual abuse: Detection, removal and reporting of illegal content online* stems from the Strategy of the European Commission for a more effective fight against child sexual abuse, which was published on July 24th, 2020. In September 2020, the Commission presented a proposal for a Regulation (COM(2020) 568 final) on a temporary derogation from certain provisions of Directive 2002/58/EC (e-Privacy-Directive) as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online (hereinafter: Interim Regulation). The European Electronic Communications Code has become fully applicable to Over-Top-Services on December 21st, 2020. Hence, certain online communication services, such as webmail, messaging and internet calls now fall under the scope of the E-Privacy-Directive. However, the E-Privacy-Directive does not contain an explicit legal basis for voluntary scanning measures to detect child sexual abuse materials (CSAM). The proposed Interim Regulation is intended to fill this legislative gap by allowing online communication service providers to implement voluntary measures for the automated analysis of communication data (content, traffic and location data) and to report identified cases of sexual abuse to authorities.

The German Bar Association (DAV) has already voiced its concern about the Interim Regulation in Position Paper 25/2021. In the interinstitutional negotiations it has become apparent, that professional secrecy will not be protected. However, professional secrecy is indispensable in a state governed by the rule of law. It is necessary to realise the right to a fair trial including a defence (Art. 6 ECHR), the right to an effective remedy including advice, defence and representation (Art. 47 CFR). In particular in cases where lawyers represent victims of child abuse or defend those

accused of such acts, the proposed Interim Regulation would inevitably lead to interference with the confidentiality of client relationships. Such an outcome would be unacceptable not only to protect the rights of lawyers and their clients, but to protect the rule of law in general. Hence, the DAV holds that in any future regulation, the use and exploitation of protected content which is subject to professional secrecy must be prevented (cf. §§ 100 d para. 5, 160a paras 2-3 of the German Code of Criminal Procedure - StPO).

The CJEU held that due to the particular intensity of interference, an automated analysis of traffic and location data is only justified when being confronted ‘with a serious threat (…) to national security which is shown to be genuine and present or foreseeable‘, or if there is ‘a reasonable suspicion of participation in terrorist offences‘. In order to combat serious crime, the court also requires a restriction to an objectively and non-discriminatorily determined group of persons or to a specific geographical region (*La Quadrature du Net*, C-511/18, C-512/18, and C-520/18).

Effective judicial or administrative control must be ensured and clear guarantees are required that the rules of data protection law are observed when processing the data. This demands appropriate technical and organizational measures to protect the data subjects. These general principles are also applicable to instances of *voluntary* data processing by private parties. From the point of view of the affected individuals, it makes no difference whether data processing by a service provider takes place on the basis of a legal obligation or not. Indeed, the intensity of infringements on fundamental rights and hence the users’ need for protection does not change depending on whether a measure is voluntary or mandatory.

The mass analysis of *content* data of all communication users without any reason and its subsequent reporting to the authorities is a particularly serious interference with the confidentiality of communications which goes considerably beyond the data retention measures discussed so far. Indeed, the analysis of content data without any reason and its comprehensive transmission to state authorities in the case of real or alleged ‘hits’ ultimately leads to a complete removal of the confidentiality of electronic communication. The analysis of the content of communication data, irrespective of its subsequent transmission to third parties, already consists of a considerable infringement on fundamental rights that requires justification.

It seems as if the Interim Regulation, which was designed merely as a temporary Regulation to enable voluntary measures, will be used in the future as a blueprint for corresponding permanent and potentially mandatory regulation. The DAV demands that any automated or manual analysis of communications data for the purpose of preventing and prosecuting criminal offenses must be measured against the requirements of the General Data Protection Regulation without exception. Hence, the DAV's answers to the targeted public consultation are closely connected to Position Paper 25/2021.

II. Answers to Selected Questions of the Public Consultation

Legislation to tackle child sexual abuse online effectively

Issue: what is the current situation and where are the gaps?

In your experience, what types of child sexual abuse online and related activities are most concerning and should be tackled in priority?

- o Distribution of **known** child sexual abuse material by uploading it to the open web (e.g. by posting it in social media or other websites, uploading it to image lockers, etc)
- o Distribution of **known** child sexual abuse material via messaging applications and e-mails
- o Distribution of **known** child sexual abuse material via darknets
- o Distribution **known** of child sexual abuse material in peer-to-peer networks
- o Distribution of **new** child sexual abuse material by uploading it to the open web (e.g. by posting it in social media or other websites, uploading it to image lockers, etc).
- o Distribution of **new** child sexual abuse material via messaging applications and e-mails
- o Distribution of **new** child sexual abuse material via darknets
- o Distribution of **new** child sexual abuse material in peer-to-peer networks
- o Online grooming of children
- o Children distributing self-generated material
- **X Other**

Please specify:

500 character(s) maximum

What is most concerning is the fact that adults are abusing children in the first place. The question about how and in which forms materials get distributed is secondary. Instead of trusting solely in a technological solution to prevent distribution, what is needed is prevention in the early stages, coupled with effective victim support. The focus solely on supply and distribution channels does not solve the root problem of demand for CSAM.

Why do you consider the above activities most concerning? Please explain, also taking into account the current measures in place that you are aware of to tackle the above activities.

2000 character(s) maximum

It is very concerning that the present debate on the Interim Regulation (COM(2020) 568 final) does not consider the root problem of high demand for CSAM. There is no evidence that introducing the scanning of all communications would make perpetrators stop their activities. Rather, there is a real risk that they would switch their activities to darknets or hide them with the help of external encryption software such as PGP (Pretty Good Privacy). The CJEU held that due to the particular intensity of interference, an automated analysis of traffic and location data is only justified when being confronted ‘with a serious threat (…) to national security which is shown to be genuine and present or foreseeable‘, or if there is ‘a reasonable suspicion of participation in terrorist offences‘. In both cases, effective judicial or administrative control must be ensured. In order to combat serious crime, the court also requires a restriction to an objectively and non-discriminatorily determined group of persons or to a specific geographical region (*La Quadrature du Net*, C-511/18, C-512/18, and C-520/18). In addition, clear guarantees are required that the rules of data protection law are observed when processing the data. This demands appropriate technical and organizational measures to protect the data subjects. The mass analysis of *content* data of all communication users without any reason and its subsequent reporting to the authorities is a particularly serious interference with the confidentiality of communications which goes considerably beyond the data retention measures discussed so far. The DAV therefore demands that any automated or manual analysis of communications data for the purpose of preventing and prosecuting criminal offenses must be measured against the requirements of the General Data Protection Regulation without exception.

Considering the current gaps in the fight against child sexual abuse online that in your view exist, which of the following outcomes should the new legislation aim to achieve in priority with regard to child sexual material and online grooming?

- o Reduce the amount of **known** child sexual abuse material uploaded in the open web
- o Reduce the amount of **known** child sexual abuse material distributed via messaging applications and emails
- o Reduce the amount of **known** child sexual abuse material distributed via darknets
- o Reduce the amount of **known** child sexual abuse material distributed via peer-to-peer networks
- o Reduce the amount of **new** child sexual abuse material uploaded in the open web
- o Reduce the amount of **new** child sexual abuse material distributed via messaging applications and emails
- o Reduce the amount of **new** child sexual abuse material distributed via darknets
- o Reduce the amount of **new** child sexual abuse material distributed via peer-to-peer networks
- o Reduce the amount of sexual material self-generated by children distributed online
- o Enable a swift takedown of child sexual abuse material after reporting
- o Ensure that child sexual abuse material stays down (i.e. that it is not redistributed online)
- o Reduce the number of instances of Online grooming of children
- **X Other**

Please specify:

500 character(s) maximum

Mandatory reporting of known CSAM (hashing-technology) would be helpful. Hashing technology has been continuously improved, and is based on previously identified pictures of CSAM. While these technologies are still prone to errors, the risks are much

less than with previously unknown CSAM, which relies on the automated analysis of content data. Mandatory reporting of known CSAM would hence be less invasive.

Considering the current gaps in the fight against child sexual abuse online that in your view exist, which of the following outcomes should the new legislation aim to achieve in priority with regard to tackling child sexual abuse in general, including prevention and victim support aspects?

- o Provide legal certainty for all stakeholders involved in the fight against child sexual abuse online (e.g. service providers, law enforcement and child protection organisations)
- o Enable a swift start and development of investigations
- o Improve transparency and accountability of the measures to fight against child sexual abuse online
- o Ensure that the legislation is future proof, i.e. that it remains effective despite future technological developments
- o Ensure a victim-centric approach in investigations, taking the best interests of the child as a primary consideration
- **X Improve prevention of child sexual abuse**
- **X Improve assistance to victims of child sexual abuse**
- o Other

Please specify:

500 character(s) maximum

The best interests of the child also include their right to confidentiality. This is particularly important in situations where lawyers represent victims of child abuse. In cases where lawyers represent victims of child abuse or defend those accused of such acts, the proposed Interim Regulation (COM(2020) 568 final) would inevitably lead to interference with the confidentiality of client relationships. Such an outcome would be unacceptable.

Do you consider that the activities of service providers are sufficiently supervised by public authorities? Please provide a reasoning for your response and provide concrete examples of supervisory measures.

2000 character(s) maximum

Any comprehensive monitoring of all communication participants requires an intensive monitoring of service providers by the competent authorities. This monitoring includes on the one hand an assessment of the criteria used to decide when any identified material contains CSAM. On the other hand, it also includes an assessment of the effectiveness of the technical and organisational measures taken. This task can only be performed by the data protection authorities. Hence, they must be provided for as supervisory authorities. This means that they must be adequately equipped, both with regards to personnel and with regards to material and financial resources. Their duties must also include the examination of the monitoring software used.

Do you have any other comments in relation to the current situation and challenges in your actions to fight against child sexual abuse online?

The DAV represents the voices of more than 62.000 German lawyers. While the DAV does not directly cooperate with law enforcement authorities, lawyers represent people accused of possessing or distributing CSAM, but also the victims of child sexual abuse online. Regarding the question whether current efforts to tackle child sexual abuse online strike an appropriate balance between the rights of victims and the rights of all users (e.g. privacy of communications), the DAV repeats its criticism on the proposed Interim Regulation (COM(2020) 568 final) . An adoption of this Interim Regulation would allow the automated mass analysis of content data, which would ultimately lead to a complete removal of the confidentiality of electronic communication. Irrespective of its subsequent transmission to third parties, this already consists of a considerable infringement on fundamental rights that requires justification. Although combating child abuse is undoubtedly a legitimate and very important regulatory purpose, the indiscriminate analysis of all communication content data as regulated in Article 3 of the Interim Regulation clearly exceeds the limits of proportionality. In cases where lawyers represent victims of child abuse or defend those accused of such acts, the proposed Interim Regulation would inevitably lead to interference with the confidentiality of client relationships. Hence, the Interim Regulation should not become a blueprint for future regulatory efforts.

Legislative solution: what should it include to tackle the above gaps effectively?

Scope

If online service providers were to be subject to a legal obligation to detect, remove and report child sexual abuse online in their services, providers of which of the following services should be subject to that legal obligation?

- o Instant messaging
- o Text-based chat (other than instant messaging)
- o Webmail
- o Voice chat
- o Video chat
- o Video streaming
- o Audio streaming
- o Web hosting
- o Image hosting
- o Social media
- o Online gaming
- o Cloud infrastructure
- o Message boards
- **X No service provider should be subject to such legal obligation**
- o Other

Please specify:

500 character(s) maximum

If the proposed Interim Regulation (COM(2020) 568 final) entered into force, it would allow the automated mass analysis of content data on a voluntary basis. This would allow blatantly disproportionate infringements on the fundamental rights of all users of the internet and ultimately lead to a complete removal of the confidentiality of electronic communication.To introduce a legal obligation for service providers to engage in serious fundamental rights infringements is absolutely unacceptable.

If legislation were to explicitly allow online service providers to take voluntary measures to detect, remove and report child sexual abuse online in their services, providers of which of the following services should be included?

- o Instant messaging
- o Text-based chat (other than instant messaging)
- o Webmail
- o Voice chat
- o Video chat
- o Video streaming
- o Audio streaming
- o Web hosting
- o Image hosting
- o Social media
- o Online gaming
- o Cloud infrastructure
- o Message boards
- **X No service provider should be legally enabled to take such voluntary measures**
- o Other

Please specify:

500 character(s) maximum

The proposed Interim Regulation would allow the automated mass analysis of content data on a voluntary basis, which would allow blatantly disproportionate infringements on the fundamental rights of all users of the internet and ultimately lead to a complete removal of the confidentiality of electronic communication. From the point of view of the affected individuals, it makes no difference whether data processing by a service provider takes place on the basis of a legal obligation or not.

If legislation was to either allow or oblige relevant online service providers to detect, remove and report child sexual abuse online in their services, should the legislation apply to service providers that offer services within the EU, even when the providers themselves are located outside the EU?

o Yes

X No

Comments

1000 character(s) maximum

If the proposed Interim Regulation (COM(2020) 568 final) entered into force, it would enable the automated mass analysis of content data by service providers. The mass analysis of *content* data without any reason and its subsequent reporting to the authorities is a particularly serious interference with the confidentiality of communications which goes considerably beyond the data retention measures discussed so far. These general principles are also applicable to instances of *voluntary* data processing by private parties. From their point of view, it makes no difference whether data processing by a service provider takes place on the basis of a legal obligation or not. Additional dangers for the potentially monitored users arise from the fact that service providers from third countries offering their services in the EU collect personal data beyond the purpose of combating child sexual abuse online.

Which types of child sexual abuse online should the possible legislation cover and how?

	Mandatory detection and removal	Mandatory reporting	Voluntary detection and removal	Voluntary reporting	No need to cover this in the legislation
Known child sexual abuse material (i.e. material previously confirmed as constituting child sexual abuse)	○	○	◉	○	○
New (unknown) child sexual abuse material	○	○	○	◉	○
Online grooming	○	○	○	◉	○
Live-streaming of child sexual abuse	○	○	○	◉	○

Comments

2000 character(s) maximum

The types of CSAM to be covered in future legislation all depend on the precise functioning of the software and algorithms. At the moment, the only software that is well-advanced is the hashing-technology for known images. In any case, the software needs to be further improved to reduce the error rate. The algorithms and filters used have to be made transparent, as to minimise the risks that users are reported falsely.

Before its use, the suitability and accuracy of the software - as well as its training data - must be checked by the responsible supervisory authority or certified bodies, such as the data protection authority, before it is used. It is also extremely important to develop the software further to be able to protect professional secrecy, such as between lawyers and their clients. Professional secrecy must already be protected effectively at the level of data collection, whenever content data is analysed. It has been argued that content data which is subject to professional secrecy cannot be identified for technical reasons. This argument does not hold since the questions in this questionnaire assume at the same time that it is technically possible to identify certain incriminated content by using artificial intelligence. Hence it should also be technically possible to identify legally privileged content. If it is not technically possible for analysis software to reliably separate out communications content that needs to be protected for reasons of professional secrecy, this does call the necessity of professional secrecy into question. Rather, such a technical 'impossibility' reveals the fact that the analysis software is not able to ensure a legally unobjectionable evaluation of the identified contents. Irrespective of this, the use and exploitation of protected content which is subject to professional secrecy must be prevented (cf. §§ 100 d para. 5, 160a paras 2-3 of the German Code of Criminal Procedure - StPO).

Some of the current tools that service providers use to voluntarily detect, report and remove child sexual abuse online do not work on encrypted environments. If online service providers were to be subject to a legal obligation to detect, remove and report child sexual abuse online in their services, should this obligation apply regardless of whether these services use encryption?

- o Yes
- **X No**

Comments

2000 character(s) maximum

If a mandatory obligation to detect, report and remove CSAM entered into force which provides an exception for encrypted environments, it would be very easy for perpetrators to simply switch to encrypted communication channels. At the same time, even if the encryption could be broken to detect CSAM, perpetrators could switch their

activities to the darknet. Hence, the proposal would not achieve its desired effect: to reduce the amount of CSAM distributed via the internet.
At the same time, making it mandatory for private service providers to scan all communication contents allow blatantly disproportionate infringements on the fundamental rights of users of internet-based communication services, without providing for sufficient procedural safeguards for those affected. Moreover, in some cases it also contradicts obligations under data protection legislation.
In particular, breaking encryption would threaten the professional secrecy of lawyers. Especially in cases where lawyers represent victims of child abuse or defend those accused of such acts, the proposed Interim Regulation would inevitably lead to interference with the confidentiality of client relationships. Hence, breaking encryption in the permanent legislation would not benefit the victims of CSAM either.

Safeguards

To be able to detect, remove and report child sexual abuse online, service providers need to carry out a series of actions. To what extent do you agree that the following actions are proportionate, when subject to all the necessary safeguards?

	Fully agree	Partially agree	Partially disagree	Fully disagree	No opinion
To check whether images or videos **uploaded online** (e.g. to a social media platform, or a file hosting service) are copies of known child sexual abuse material	○	◉	○	○	○
To assess whether images or videos **uploaded online** (e.g. to a social media platform, or a file hosting service) constitute **new** (previously unknown) child sexual abuse material	○	○	◉	○	○
To check whether images or videos sent in a **private communication** are copies of **known** child sexual abuse material	○	◉	○	○	○
To assess whether the images or videos sent in a **private communication** constitute **new** child sexual abuse material	○	○	◉	○	○
To assess whether the contents of a **text-based communication** constitute **grooming**	○	○	◉	○	○
To assess, based on data **other than content data** (e.g. metadata), whether the user may be abusing the online service for the purpose of child sexual abuse	○	◉	○	○	○

The actions to detect, remove and report child sexual abuse online may require safeguards to ensure the respect of fundamental rights of all users, prevent abuses,

and ensure proportionality. To what extent do you agree that the legislation should put in place safeguards to ensure the following:

	Fully agree	Partially agree	Partially disagree	Fully disagree	No opinion
The tools used to detect, report and remove child sexual abuse online reduce the **error rate** to the maximum extent possible	◉	○	○	○	○
The tools used to detect, report and remove child sexual abuse online are the **least privacy intrusive**	◉	○	○	○	○
The tools used to detect, report and remove child sexual abuse online comply with the **data minimisation principle** and rely on anonymised data, where this is possible	◉	○	○	○	○
The tools used to detect, report and remove child sexual abuse online comply with the **purpose limitation principle**, and use the data exclusively for the purpose of detecting, reporting and removing child sexual abuse online	◉	○	○	○	○
The tools used to detect, report and remove child sexual abuse online comply with the **storage limitation principle**, and delete personal data as soon as the purpose is fulfilled	◉	○	○	○	○
The online service provider conducts a **data protection impact assessment and consults the supervisory authority**, if necessary	◉	○	○	○	○
Online service providers are subject to the oversight of a **supervisory body** to assess their compliance with legal requirements	◉	○	○	○	○
Reports containing **new material or grooming** are **systematically** subject to **human review** before the reports are sent to law enforcement or organisations acting in the public interest against child sexual abuse	◉	○	○	○	○
All reports (including those containing **only previously known** child sexual abuse material) are **systematically** subject to **human review** before the reports are sent to law enforcement or organisations acting in the public interest against child sexual abuse	◉	○	○	○	○
A clear **complaint mechanism** is available to users	◉	○	○	○	○
Effective remedies should be available to users that have been erroneously affected by the actions of the service provider to detect, report and remove child sexual abuse online	◉	○	○	○	○
Providers should make clear in the **Terms and Conditions** that they are taking measures to detect, report and remove child sexual abuse online	◉	○	○	○	○

Other (please specify):

2000 character(s) maximum

It is extremely important to adopt all safeguards in any future legislation. The CJEU has set strict limits on the storage of traffic and location data by telecommunication providers without any reason. It is only allowed by way of exception under specific conditions and if sufficient procedural safeguards are guaranteed. Relevant legislation must ensure - through clear and precise rules - that the storage of the data in question complies with any applicable substantive and procedural conditions applicable and that those affected have effective safeguards to protect them from risks of abuse. The CJEU held in addition that due to the particular intensity of interference, an automated analysis of traffic and location data is only justified when being confronted ‘with a serious threat (…) to national security which is shown to be genuine and present or foreseeable‘, or if there is ‘a reasonable suspicion of participation in terrorist offences‘. In both cases, effective judicial or administrative control must be ensured. In order to combat serious crime, the court also requires a restriction to an objectively and non-discriminatorily determined group of persons or to a specific geographical region (*La Quadrature du Net*, C-511/18, C-512/18, and C-520/18). These general principles are also applicable to instances of *voluntary* data processing by private parties. From the point of view of the affected individuals, it makes no difference whether data processing by a service provider takes place on the basis of a legal obligation or not. Indeed, the intensity of infringements on fundamental rights and hence the users’ need for protection does not change depending on whether a measure is voluntary or mandatory. The DAV therefore demands that any automated or manual analysis of communications data for the purpose of preventing and prosecuting criminal offenses must be measured against the requirements of the GDPR without exception.

Sanctions

To what extent do you agree with the following statements, in the context of possible future legislation allowing/obliging relevant online service providers to detect, report and remove child sexual abuse online in their services:

	Fully agree	Partially agree	Partially disagree	Fully disagree	No opinion
Companies should be subject to **financial sanctions** if they fail meet the legal obligations (including safeguards) related to the detection, reporting and removal of child sexual abuse online	○	○	○	○	○
Companies should be subject to **criminal sanctions** if they fail meet the legal obligations (including safeguards) related to the detection, reporting and removal of child sexual abuse online	○	○	○	○	○
Companies that erroneously detect, remove or report child sexual abuse online **in good faith** should not be subject to the relevant sanctions	○	○	○	○	○
There should be **no sanctions** for failure to meet the legal obligations (including safeguards) related to the detection, reporting and removal of child sexual abuse online	○	○	○	○	○

Other (please specify):

2000 character(s) maximum

The appropriateness of which type of sanctions all depends on how well the software and algorithms function. At the moment, the only software that is well-advanced is the hashing-technology for known images. Hence, sanctions in cases of non-compliance with reporting obligations could be useful. However, the software needs to be further improved to include less false positives. There has to be transparency about the algorithms and filters used, as to minimise the risks to the users to be reported falsely. It is also extremely important for victims to further develop the software so that it is able to protect professional secrecy, for example between lawyers and their clients, but also from others such as counselling centres, psychologists, psychiatrists and clergy. Professional secrecy must already be protected effectively at the level of data collection, whenever content data is analysed. It has been argued that content data which is subject to professional secrecy cannot be identified for technical reasons. This argument does not hold since the questions in this questionnaire assume at the same

time that it is technically possible to identify certain incriminated content by using artificial intelligence. Hence it should also be technically possible to identify legally privileged content. If it is not technically possible for analysis software to reliably separate out communications content that needs to be protected for reasons of professional secrecy, this does call the necessity of professional secrecy into question. Rather, such a technical 'impossibility' reveals the fact that the analysis software is not able to ensure a legally unobjectionable evaluation of the identified contents. Irrespective of this, the use and exploitation of protected content which is subject to professional secrecy must be prevented (cf. §§ 100 d para. 5, 160a paras 2-3 of the German Code of Criminal Procedure - StPO).

Transparency and accountability

Transparency reports *could refer to periodic reports by service providers on the measures they take to detect, report and remove child sexual abuse online.*
These transparency reports should be:

	Yes	No	No opinion
Obligatory to ensure transparency and accountability	◉	○	○
Voluntary: an obligation would incur an additional burden on the online service providers, especially when they are small and medium enterprises	○	◉	○
Evaluated by an independent entity	◉	○	○
Standardised, to provide uniform quantitative and qualitative information to improve the understanding of the effectiveness of the technologies used as well as the scale of child sexual abuse online	◉	○	○

Transparency reports *should include the following information:*

- o Number of reports of instances of child sexual abuse online reported by type of service
- o Number of child sexual abuse material images and videos reported by type of service
- o Time required to take down child sexual abuse material after it has been flagged to/by the service provider

X Types of data processed to detect, report and remove child sexual abuse online

X Legal basis for the processing to detect, report and remove child sexual abuse online

X Whether data are shared with any third party and on which legal basis

X Number of complaints made by users through the available mechanisms and the outcome of those proceedings

X Number and ratio of false positives (an online event is mistakenly flagged as child sexual abuse online) of the different technologies used

o Measures applied to remove online child sexual abuse material in line with the online service provider's policy (e.g. number of accounts blocked)

X Policies on retention of data processed for the detecting, reporting and removal of child sexual abuse online and data protection safeguards applied

o Other

Please specify:

1000 character(s) maximum

Transparency reports are an important tool to evaluate the effectiveness and reliability of the software used to detect CSAM. Therefore, they should contain all the necessary information to determine the quality of the software, in particular with regard to the ratio of false positives and data security. Irrespective of this, the use and exploitation of protected content which is subject to professional secrecy must be prevented (cf. §§ 100 d para. 5, 160a paras 2-3 of the German Code of Criminal Procedure - StPO).

Performance indicators

Which indicators should be monitored to measure the success of the possible legislation?

o Number of reports of child sexual abuse online reported by company and type of service

o Number of child sexual abuse material images and videos reported by company and type of service

o Time required to take down child sexual abuse material after it has been flagged to/by the service provider

X Number of children identified and rescued as a result of a report, by company and type of service

- o Number of perpetrators investigated and prosecuted as a result of a report, by company and type of service
- o Number of related user complaints as a result of a report, by company and type of service

X Other

Please specify:

1000 character(s) maximum

It is extremely important to develop a suitable tool for evaluating the effectiveness and reliability of the software used to detect CSAM. Hence, it is important to report on the ratio of false positives on the one hand, and the number of children identified and rescued as a result of a report on the other hand. At the moment, no publicly available data as to the reliability of the software exist, and it is hence not possible to conclude that the measures are effective. If any legislation entered into force which makes it mandatory for private parties to report CSAM, there should be a way to evaluate these reports objectively.