DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Surveillance Committee

on the Trilogue Negotiations concerning the proposed Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC 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 (COM(2020) 568 final

Position Paper No.: 25/2021 Berlin/Brussels, March 2021

Members of the Surveillance Committee

- Rechtsanwältin Lea Voigt, Bremen (Chair)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin (Rapporteur)
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Rechtsanwältin Prof. Dr. Annika Dießner, Berlin
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt
- Rechtsanwalt Prof. Dr. Mark A. Zöller, München
- Prof. Dr. Annika Dießner, Berlin (permanent guest member of the Committee)
- Prof. Dr. Mark A. Zöller, München (permanent guest member of the Committee)

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

Contact in Brussels:

- Rechtsanwältin Eva Schriever, LL.M.,

Mailing List

Europe

- European Commission
    - Directorate-General on Communication Networks, Content and Technology
    - Directorate-General on Justice and Consumers
    - Directorate General on Migration and Home Affairs
- European Parliament
    - Committee on Civil Liberties, Justice and Home Affairs
- Council of the European Union
- Permanent Representation of the Federal Republic of Germany to the European Union
- Officers of the Länder
- Council of Bars and Law Societies of Europe (CCBE)
- Bundesverband der Freien Berufe (BFB)

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

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

On September 10th, 2020, the Commission presented a proposal for a Regulation 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 Interim Regulation is intended to allow 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 DAV is explicitly in favour of combating the preparation and commission of child sexual abuse and its dissemination via the internet through effective measures at EU-level. However, the Interim Regulation proposed by the Commission would allow blatantly disproportionate infringements on the fundamental rights of users of internet-based communication services. Furthermore, the proposed Interim Regulation lacks sufficient procedural safeguards for those affected. This is why the legislative proposal should be rejected as a whole.

The DAV demands that any automated or manual analysis of communications data for the purpose of preventing and prosecuting criminal offences must be measured against the requirements of the General Data Protection Regulation (GDPR) without exception. The DAV explicitly joins the recommendations of the European Parliamentary Research Service's substitute impact assessment in this regard, which was published on February 5th, 2021.

Should the Interim Regulation be adopted despite these fundamental concerns, the DAV demands that the protection of professional secrecy should be expressly included in the enacting part of the Interim Regulation. This could be achieved by adopting

Amendment 28 of the LIBE report. 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 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.

II. Background

The proposed Interim Regulation stems from the Commission's Strategy for a more effective fight against child sexual abuse, which was published on July 24th, 2020. 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.

Some telecommunications providers have so far taken voluntary measures to detect CSAM on the internet. However, the e-Privacy Directive does not contain an **explicit legal basis** for processing content or traffic data for the purpose of detecting child sexual abuse on the internet. With full applicability of the European Electronic Communications Code, these voluntary activities are now no longer possible unless member states take specific national measures. The Interim Regulation is intended to create a limited exception to the applicability of Article 5(1) and Article 6 of the e-Privacy Directive, which regulate the protection of the confidentiality of communications and traffic data.

Article 3 of the Interim Regulation intends to allow online communication service providers to implement voluntary measures for the automated analysis of communication data (content, traffic and location data) using ‘relevant key indicators,

such as keywords and objectively identified risk factors' and to report identified cases of sexual abuse to authorities.

III. General rejection of the proposed Interim Regulation

The DAV is explicitly in favour of combating the preparation and commission of child sexual abuse and its dissemination via the internet through effective measures at European level. However, the Interim Regulation proposed by the Commission would allow blatantly disproportionate infringements on the fundamental rights of users of internet-based communication services. Furthermore, the proposed Interim Regulation lacks sufficient procedural safeguards for those affected. The legislative proposal should therefore be rejected as a whole.

According to Article 15 (1) E-Privacy-Directive, Member States may enact legislation to restrict the rights and obligations under Article 5 (Confidentiality of Communications) and Article 6 (Traffic Data), if it is a necessary, appropriate and proportionate measure for the prevention, investigation, detection and prosecution of criminal offences. Recital 11 of the E-Privacy-Directive clarifies that such a measure must be 'strictly' proportionate to the intended purpose.

The CJEU has set **strict limits** on the storage of traffic and location data by telecommunication providers without any reason. In its case law on data retention, the CJEU held that general and indiscriminate retention of such data is in principle impermissible. 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 (*La Quadrature du Net*, C-511/18, C-512/18, and C-520/18)

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 (*La*

Quadrature du Net, C-511/18, C-512/18, and C-520/18). The Interim Regulation does not account for these safeguards and therefore falls far short of the CJEU's requirements on data retention.

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 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. Although combating child abuse is undoubtedly a legitimate 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,.

The interference with fundamental rights is further intensified by the fact that the Interim Regulation foresees data analysis by service providers using **artificial intelligence**. This type of analysis poses special risks for those affected, since the accuracy of the analysis results depends on the design of the analysis software, in particular the designation of indicators. There are considerable doubts as to whether Article 3 of the proposed Interim Regulation ensures that the service providers use sufficiently reliable software. The specifications here remain conceivably vague ('well-established technology', 'sufficiently reliable', 'relevant key indicators, such as keywords and objectively identified risk factors').

Furthermore, the Interim Regulation contains insufficient and unclear rules regarding **the processing of data**. For example, service providers would be entitled to transfer identified content to ’law enforcement and other relevant public authorities"’, while it is completely unclear which entities would fall under the latter category.

Furthermore, it is to be feared that 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 mandatory regulations**. The Commission is currently conducting a public consultation in this regard and plans to present a draft regulation in the second quarter of 2021. 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. In this matter, the DAV expressly endorses the recommendations made by the European Parliament's Scientific Service in its Targeted Substitute Impact Assessment, published on February 5th, 2021.

IV. The Protection of Professional Secrecy is Non-Negotiable

Professional secrecy is **indispensable** in a state governed by the rule of law. It serves to realise the right to a fair trial including the right to defend himself in person or through legal assistance of his own choosing (Art 6 ECHR), the right to an effective remedy including advice, defence and representation (Art. 47 CFR), the implementation of the rule of law, the realisation of the right to be heard and the right to respect for private and family life (Art 8 ECHR. Art 7 CFR).

The Interim Regulation threatens the professional secrecy of lawyers in three specific cases: when lawyers represent the victims of child abuse, when lawyers provide abstract legal advice to protect against child abuse; and when lawyers defend accused persons in this area.

In all three cases, breaches **of confidentiality** would occur on a regular basis if the Interim Regulation were to enter into force. Nowadays, communication in client relationships takes place in a variety of ways. Clients use e-mail services such as Gmail, messenger services such as WhatsApp, video conferencing services such as

Microsoft Teams and a variety of other digital channels for correspondence with their lawyers. Since the planned Interim Regulation does not provide for an exception for encrypted communication content, even the use of "crypto-messengers" would not be a suitable means of preserving the protection of professional secrecy.

Therefore, professional secrecy must already be protected effectively at the level of **data collection, whenever content data is analysed**. The reason is that the analysis of content data already consists of an interference with fundamental rights. This interference is intensified in the transmission of ‘hits’ to authorities and other third parties. The fact that that the data analysis is not carried out by government agencies but rather by companies in the private sector does not preclude the need for adequate protection mechanisms. Indeed, the intention of the Interim Regulation is to enable telecommunications providers to implement their own measures to prevent and prosecute crimes on the internet and to transmit identified ‘hits’ to authorities. This can be seen as yet another instance of ‘outsourcing’ of government tasks to private companies. While this corresponds to the trend of the times, it is all the more necessary to implement sufficient safeguards already at the level of purpose-oriented data collection by any private bodies concerned.

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 Interim Regulation assumes 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.

Should the Interim Regulation be adopted despite these fundamental concerns, the DAV demands that provisions on the protection of professional secrecy should be expressly included in the enacting part of the Regulation, for example in the form of Amendment 28 of the LIBE report:

Amendment 28: Article 3, paragraph 1, lit. xiii (new)

there is **no interference with any communication protected by professional secrecy**, such as between doctors and their patients, journalists and their sources or **lawyers and their clients.**