„Thank you very much, your mail is perfectly fine“

Erik Tuchtfeld 2022-08-18T10:26:19

In May, the Commission presented its draft for a „Regulation laying down rules to prevent and combat child sexual abuse„. The introduction of the inspection of all digitally sent messages (discussed under the catchword „chat control“) led cryptography professor Matthew Green, among others, to assess the project as „the most sophisticated mass surveillance machinery ever deployed outside of China and the USSR„. The project, which evidently violates fundamental rights, is probably the largest state surveillance project in Europe since the end of the Cold War.

The Commission’s draft

The current proposal succeeds Regulation 2021/1232, which was adopted in record time last summer. After the European Electronic Communications Code (EECC) – probably by mistake – also placed digital communications via messenger and e-mail under the comprehensive protection of the secrecy of correspondence (cf. recitals 2, 9, 23 of Regulation 2021/1232), the operators of large unencrypted communication services such as Facebook Messenger noticed that this would also prohibit the previously common (server-side) scanning of communications for Child Sexual Abuse Material (CSAM). In response, Regulation 2021/1232 weakened confidentiality protections again and allowed these measures to resume in the short term. Even at that time, political unity was contrasted with considerable legal doubts. Even though this was not a matter of *imposing* inspection mechanisms, but only of *permitting* them, the former German ECJ judge Colneric, for example, considered the plan incompatible with fundamental rights.

What was yesterday a permission is now to become an obligation: Article 10(1) of the Commission’s current draft provides that both hosting providers (e.g. website hosts, social media platforms and similar services) and interpersonal communication services (i.e. messengers and email providers) must in future comply with „detection orders“. If such an order is issued, they will have to install and use software that is supposed to detect known and previously unknown images of child abuse as well as so-called „grooming“. „Grooming“ in this context describes the contacting of adults towards children for sexual purposes (Article 2 lit. o of the draft in conjunction with Article 6 of the Directive on Combating Sexual Abuse). For this purpose, the provider may either use its own software or software developed by a new EU Centre against child abuse to be established in The Hague (Article 10 para. 2; Articles 40 to 42). These „detection orders“ are issued by a court or an independent administrative authority at the request of a coordinating body (to be created) (Art. 25 to 32), if there is a significant risk that a service is used for online child abuse (Art. 7).

Since it is not a question of whether a service is used to a significant extent for child abuse, but whether there is a significant risk (regardless of the extent) of such use, almost all common, generally available digital means of communication are likely to be covered by this. For providers of unencrypted (or transport-only) communications services – as it is regularly the case with emails, for example, but also Facebook Messenger, Twitter direct messages, Instagram messages, etc. – this is likely to result in algorithms being used on the server side to detect CSAM and grooming messages. As soon as suspicious messages are detected (automatically), they will first be forwarded to the aforementioned EU Centre (Article 12) and then, if the suspicion is confirmed (whether by automated or manual procedures remains open), to Europol or national security authorities (Article 48).

The situation is more complex for providers of end-to-end encrypted communication (such as Signal, Threema or WhatsApp). They will be subject to the same obligation, but they have no technical ability to search the contents of the communication. The only possibility for them will be to check content prior to encryption, i.e. to build a mechanism into the respective app itself that checks the message before it is sent (and thus encrypted). Therefore, in its draft, the Commission continues to refer to end-to-end encryption as an „important tool to guarantee the security and confidentiality of the communications of users, including those of children“ (recital 26) – while this encryption is not banned, it simply becomes obsolete, making every messaging app a bug that is already active before encryption.

Compared to analog communication, server-side inspection corresponds to the mailman who opens every letter and package and takes a look at its contents, while inspection on the device side corresponds to the police officer who does not want to wait that long and already takes a look over the sender’s shoulder when writing.

Other critical aspects of the Commission’s draft, such as network blocking (Art. 16 to 18) or verification obligations (Art. 4 Par. 3, Art. 6 Par. 1 lit. c), can only be briefly mentioned here for the sake of space, without discussing them in detail. They each offer more than enough reason for independent contributions.

The essence of the Right to Privacy

Secrecy of correspondence is guaranteed in the European Union, in particular by Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights (CFR). Against the background of the comprehensive scanning of all digital communications, however, there are also likely to be considerable chilling effects on Freedom of expression and information (Article 11). Beyond the area of private life, particular attention must also be paid to the effects on professional secrecy holders such as journalists, lawyers and doctors, whose particularly protected communications with their informants/clients/patients will be screened (*La Quadrature du Net*, para. 118).

The case law of the ECJ on data retention, which only concerned the processing of metadata (e.g. information on the time of the communication and the parties involved), makes the obvious incompatibility of the current project with the

aforementioned fundamental rights clear. Interferences with the Right to Privacy must be „limited to what is strictly necessary“ (settled case-law, see *La Quadrature du Net*, para. 130). Furthermore, any interference must respect the essence of the right to privacy enshrined in Article 7 CFR, which is absolutely protected under Article 52 (1) sentence 1 CFR.

What is the essence, the core of this right to „respect for communication“? Most certainly that not every single piece of communication – be it automated or manual – is inspected for certain factors, but that in principle what is meant to be private remains private (on the distinction between private and public communication see also here). Admittedly, there is no principle without exceptions: For example, *case-specific* telecommunications surveillance, which in *individual* cases covers all communications, does not affect the essence of the right to secrecy of correspondence (but note also here the exception required under German constitutional law for communications that can be assigned to the core area of private life, § 100d StPO).

When it comes to the coverage of the “detection orders”, one can hardly think of a more exhaustive measure. It is only limited regarding its way of transport, since only digital—and not analog—communication is covered. The margin left for intensifying this act of surveillance would be to change the type of content the detection engine is looking for: Not only CSAM, but also terrorist content, organized crime, fake news —you name it. Accordingly, the ECJ has also rejected a violation of the essence of Article 7 CFR in the case of data retention directed at metadata only because „the directive does not permit the acquisition of knowledge of the content of the electronic communications as such“ (*Digital Rights*, para. 39). Conversely, the Commission’s plan, which relates precisely to the content of electronic communications, affects the essence of Article 7 CFR and thus must be considered unlawful.

No machine is error free

The unlawfulness of the draft would therefore have to be affirmed, even if one were to assume a perfect technology that would exclusively identify criminal content. However, the Commission itself assumes that around 12% of future messages would be *false positives*, i.e. would not concern criminal content (fn. 32 of the draft). As billions of messages are sent every day in the EU, a 12% false positive rate is likely to result in thousands of messages being leaked to public authorities every day without any substantive reason. Taking into account the type of content the technology is looking for, this is likely to primarily affect intimate chat messages that are exchanged consensually. In the future, there is a real risk that private photos, videos and text messages will end up on the desks of public officials.

The obligation to protect children

Of course, the Commission is aware of both the relevant case law and the actual problems. Surprisingly, it even refers – albeit highly selectively – to the case law on data retention when it emphasizes that Articles 7 and 8 CFR also give rise to positive

obligations for the European Union vis-à-vis children affected by abuse (footnote 27 of the draft with reference to para. 126 of *La Quadrature du Net*). However, it is precisely the existence of these obligations to protect that makes the draft a scandal: children have a right to be protected by the state. This is exactly what the ECJ also recognized in *La Quadrature du Net,* and yet found the laws on bulk data retention to be disproportionate. There is no indication that it would now come to a different conclusion. The Commission has thus produced a proposal that will attract a great deal of time, money and attention, only – if it gains political approval – to end up being declared null and void in court.

This does nothing to improve the urgently needed protection of children. Yet much could be done: At present, for example, some security authorities are not working to delete known images of child abuse because they lack the resources to do so – a flagrant violation of the fundamental obligation to protect those affected. Simply reviewing the existing material presents the police with considerable capacity problems. If the resources are already lacking for this, one can only paint a bleak scenario when it comes to the investigation of the perpetrators who directly harm the children.

The Commission should work with the member states to develop an effective, legally compliant plan of action to combat child abuse. This should include more personnel resources for the security authorities, improved reporting possibilities within the services, better media and sex education for children and an expansion of counselling and contact points for those affected. Dystopian total surveillance, on the other hand, should not be part of it.

This article is a translation of a previous text, „Vielen Dank, Ihre Post ist unbedenklich“.

(cc) BY-SA