EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 22/2023, 15 May 2023
Tags: Data protection and digital governance
Topics: Platform regulation, child sexual abuse, personal data protection, privacy

'Voluntary detection orders' under the proposed EU Child Sexual Abuse Regulation violate EU (privacy) law

By Dr. Sabine K Witting & Dr. Gianclaudio Malgieri

Background

On 11 May 2022, the European Commission (Commission) published its proposed Regulation laying down rules to prevent and combat child sexual abuse (Child Sexual Abuse (CSA) Regulation). The proposed CSA Regulation aims to establish a clear and harmonized legal framework to better identify, protect, and support victims of CSA, notably through a clarification of the rules and responsibilities of online service providers when it comes to online CSA. It seeks to provide legal certainty to providers as to their responsibilities to assess and mitigate risks and, where necessary, to detect, report, and remove online CSA in a manner consistent with the fundamental rights laid down in the Charter of Fundamental Rights of the European Union and existing EU law.

The proposed CSA Regulation establishes a risk assessment and risk mitigation regime complementary to the Digital Services Act, specifically targeting risks associated with online CSA. If a so-called national 'Coordinating Authority', which oversees the risk assessment and risk mitigation measures undertaken by providers, identifies a significant risk of online CSA on a specific service, it can request a judicial or independent administrative authority to issue a detection order. If a provider receives a detection order, it is obliged to use technologies to detect and report specific types of online CSA to a newly established 'EU Centre'. If the company fails to comply, it can be fined up to 6% of its annual income or global turnover.

Despite these wide-ranging interventions proposed by the CSA Regulation, child protection organisations, some EU Member States and the Committee on Civil Liberties Justice and Home Affairs (LIBE) rapporteur, Javier Zarzalejos, are concerned that the mandatory detection regime alone is insufficient. They argue that it undermines the current voluntary efforts of many providers to proactively detect online CSA on their services – even if not being legally obliged to do so by a detection order (see further below).

This post analyses the complementarity of the voluntary detection regime with the mandatory detection regime in the proposed CSA Regulation and discusses whether such a regime is compatible with particular the General Data Protection Regulation (GDPR) and the e-Privacy Directive.

Moving from voluntary to mandatory detection regime under the CSA Regulation

To better understand the debate around the voluntary detection regime, it is important to travel back to a change in EU law which heavily affected the voluntary efforts of online providers in their fight against online CSA. Since the entry into force of the European Electronic Communications Code on 21 December 2020, the e-Privacy Directive also covers number-independent inter-personal communication services (NIICS) such as messaging services and email. Thus, the e-Privacy Directive prevented such NIICS from continuing their voluntary use of specific technologies to detect online CSA without authorization by national or EU legislation. To avoid such voluntary practices coming to a complete halt in the EU following 21 December 2020, a temporary derogation entered into force on 2 August 2021 enabling NIICS to continue the voluntary use of technologies for the processing of personal data and other data to the extent necessary to detect, report, and remove online CSA. However, the temporary derogation ceases to apply three years after its entry into force (on 3 August 2024) or alternatively, once the CSA Regulation enters into force (see section 89 of the proposed CSA Regulation).

As the CSA Regulation does not contain any legal provisions to continue the voluntary detection regime provided for in the temporary derogation, online providers will have to wait to receive a detection order until they can proactively search for online CSA. It is important to note that this consequence is not an oversight by the Commission, but a deliberate decision. Firstly, the Commission notices in its impact assessment report on the CSA Regulation that the temporary derogation did not create an explicit legal basis for processing personal data for the purpose of proactively detecting online CSA (p. 10). As the temporary derogation did not oblige providers to scan for online CSA but only gave them the option to do so, the 'compliance with a legal obligation' ground in Article 6(1)(c) GDPR does not apply. While the Commission notes that some providers evoked other legal bases under the GDPR (presumably 'legitimate interest' under Article 6(1)(f) GDPR), it also

acknowledges that the uncertainty regarding the legal basis deters some providers from taking voluntary action (p. 35). Secondly, the Commission argues that a voluntary detection regime leaves private companies to make fundamental decisions with significant impact on users and their rights (p. 29). Considering the complexities of regulating the detection of online CSA from a fundamental rights perspective, with the right to protection from violence, abuse and exploitation, freedom of expression, right to privacy and right to personal data protection affected amongst others, the Commission feels that it may not be appropriate to leave the decision on whether and how to detect content in private communications to providers.

Introduction of permanent 'voluntary detection regime' under LIBE Rapporteur

The decision of the Commission to abandon the voluntary detection regime altogether in the CSA Regulation was not welcomed by everyone. As mentioned, child protection organisations and some EU Member States are concerned that this shift might lead to detection gaps and unfairly slow down companies which are keen to continue voluntary detection and take an active role in the fight against online CSA. A recently leaked protocol on a meeting of the Council's Law Enforcement Working Party on 29 March 2023 demonstrates that several EU Member States – including France, Germany, Romania, Malta, Slovakia, Czech Republic, Estonia, Slovenia, and Latvia – agree that a detection gap needs to be avoided. Some expressed support for a limited extension of the voluntary detection regime under the temporary derogation, others argued for the establishment of a permanent legal basis for voluntary detection in the CSA Regulation, in addition to the mandatory detection regime.

The debate around the voluntary detection regime also heavily influenced the report of the LIBE Committee's Rapporteur on the CSA Regulation, Javier Zarzalejos. In his report, published on 29 April 2023, he proposes the introduction of a permanent legal basis for voluntary detection, called 'voluntary detection orders'. In his report, he argues that these orders will not only contribute to make mandatory detection orders a measure of last resort but will also cover a possible gap between the entry into force of the CSA Regulation.

According to the proposed amendments, the provider shall assess, in a separate section of its risk assessment, the voluntary use of specific technologies for the processing of personal and other data to the extent strictly necessary to detect, report, and remove online CSA from its services (see newly proposed Article 3(2)(a) CSA Regulation. As part of their risk mitigation measures, providers may request the national Coordinating Authorities to continue the use of specific technologies for the processing of personal and other data to the extent strictly necessary and proportionate. In such a case, the Coordinating Authority can request the competent judicial authority or administrative

authority to issue an order that authorizes the provider to maintain or implement mitigation measures that consist of using technology to process personal data for the purpose of detecting online CSA (see newly proposed Article 5(a) CSA Regulation).

Circumvention of fundamental rights safeguards through the voluntary detection regime?

As noted by the Commission, the decision whether to search private communications for online CSA is too sensitive for the protection of fundamental rights to be left to a company. By having the voluntary detection order signed off by a judicial or administrative authority, the LIBE Rapporteur creates an oversight mechanism, so that the decision does not solely lie with the company. While this is admittedly better than completely leaving this important decision to companies, the voluntary detection regime nonetheless significantly impacts the fundamental rights safeguards set by the CSA Regulation.

As mentioned above, companies need to assess the risks of their products and services associated with online CSA and take mitigation measures. The voluntary detection regime falls under the mitigation measures. If a significant risk remains despite the mitigation measures, Coordinating Authorities can request for the issuance of a detection order. However, the voluntary detection regime does not set the same fundamental rights safeguards as mandatory detection orders, such as the need for targeted, specific, and only strictly necessary measures with clear time limits (see Article 7(9) CSA Regulation). This means that if companies already deploy detection technologies as part of their mitigation measures, the voluntary regime circumvents the proportionality requirements introduced for mandatory detection orders, even though they have the exact same fundamental rights impact.

Further, it is important to note that a company which fails to mitigate the risk of online CSA through the voluntary detection regime does not immediately receive any penalties. The next step in the process is the issuance of a mandatory detection order before facing the risk of penalties (up to 6% of the annual income or global turnover). It is therefore likely that companies will strategically apply for the voluntary detection regime to avoid being issued a detection order which comes with the risk of penalties. The voluntary detection regime as proposed by the LIBE rapporteur hence incentivises companies to apply for voluntary detection orders and filter as much content as possible to avoid triggering a mandatory detection order with penalties attached to it. Combined with the lack of fundamental rights safeguards to minimize the impact on fundamental rights, this is a significant weakening of the arguably already weak fundamental rights safeguards in the current CSA Regulation.

Voluntary detection regime under existing EU Law

The data protection legal framework is key in this discourse. Considering that voluntary detection activities in private communications of users have the potential to seriously affect their fundamental right to privacy and data protection, we should take a closer look at the GDPR and at the e-Privacy Directive.

Looking at the GDPR, it is first necessary to clarify that the platform providers that want to carry out voluntary detection should find a lawful basis for processing such personal data. Among possible lawful bases at Article 6, we think consent is particularly hard to use both because it would jeopardize the voluntary detection activities and would probably be an invalid consent. Indeed, the effectiveness of these actions are based on their secrecy, but if a general consent is asked at the beginning of the data processing, it would not be specific enough and usually users would be in a position of information and power asymmetry that would impar the freedom of their consent provision.

Looking at the other lawful bases, we believe that also legal obligations might be problematic, because there is no real legal "obligation" to carry out a "voluntary" activity, even though they are authorized by a judicial body. Indeed, there is no explicit consequences (sanctions) in case such voluntary detections are not requested and performed.

As said above, also legitimate interest might be a slippery lawful basis, considering the necessary balancing test between the external interest (CSA detection) and the expectations/interests of data subjects and impacts on their privacy and data protection. This balancing test is particularly problematic due to the extremely high intrusiveness produced by a hidden access to private communications of data subjects and the risk that most of these detections are based on false positives. Public interest might be a more interesting lawful basis, however recital 45 of the proposed CSA regulation explains that the EU or national law should clarify whether this lawful basis can be used also by private entities (and not only by public entities and public officials). For what we know, the CSA regulation does not clarify this point.

There is an additional limit to the use of public interest and legitimate interest as lawful basis, since these private communications generally refer to sexually sensitive messages, they have a high potential to reveal the sexual orientation and/or sexual life of the data subject. Accordingly, these data would be a "special category of personal data" under Article 9(1) of the GDPR. This implies that stricter lawful bases (Article 9(2)) should apply, and "legitimate interest" and "public interest" would not be adequate justification for such data processing.

Looking at Article 9(2), the only lawful ground for processing sensitive data in this context appears to be letter (g), i.e., "reasons of substantial public interest, on the basis of Union

or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Here the question would be whether there are adequate safeguards to protect data subjects' rights under the CSA Regulation's mechanism for voluntary detection (as proposed by LIBE). In case voluntary detection is used as an *ex-ante* risk mitigation measure, it would be hard to prove proportionality and safeguards adequacy in practice.

However, since this would be an intrusion into private electronic communications, we would need to consider also the e-Privacy Directive. Article 5 prohibits the access to electronic communications. There are two exceptions: the consent of the user (whose problematic nature in this case are described above) and a specific legal authorisation (Article 15), provided that there are sufficient safeguards and that the principles of necessity and proportionality are respected. Actually, Article 15 (which the CJEU has already interpreted in a restrictive way, e.g., in *Tele2 Sverige*, *La Quadrature du Net*, and *Mircom*) refers only to authorisation in accordance with "Member States law", while the CSA Regulation would be an EU law. This means that the CSA Regulation would need national specifications in this regard, but that the CSA Regulation is not sufficient alone to avoid the lack of compliance with e-Privacy Directive. Interestingly, the Explanatory Memorandum of the European Commission proposal for the CSA Regulation affirms that, in case of "activities that are strictly necessary to execute detection orders" under the CSA Regulation, the exemption of Article 15(1) will apply "by analogy" (without any need of national implementation). We might wonder whether this interpretation is acceptable and whether it applies also to voluntary detections (which are not "orders", strictly speaking). However, even though one might judge the pre-authorisation model of voluntary detection in the CSA Regulation as an adequate legal basis under Article 15(1), other forms of voluntary detections, e.g., based on *ex-ante* risk mitigation strategies, would appear unacceptable.

Conclusion

In conclusion, the current structure of the voluntary detection regime circumvents the fundamental rights safeguards in the CSA Regulation Proposal. It also risks that companies are incentivized to over-filter at the risk mitigation stage to avoid the issuance of a mandatory detection order which comes with the risk of penalties.

Importantly, the voluntary detection regime does not solve the conflict with the GDPR. The lack of a lawful basis for processing personal data was already an issue for the temporary derogation. The voluntary detection regime proposed by the LIBE rapporteur, however, does not resolve this.

The voluntary detection regime hence perpetuates the legal concerns voiced about the temporary derogation, and, as set out by the Commission, undermines the mandatory detection regime under the CSA Regulation.