LEWIATAN

Warszawa, 22 września 2023 r.
KL/363/172/ET/2023

Pan
Łukasz Wojewoda
Dyrektor
Departament Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

Szanowny Panie Dyrektorze,

W związku z trwającymi pracami nad projektem Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie, Konfederacja Lewiatan w załączeniu, przesyła stanowisko do projektu dyrektywy.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Załącznik: Stanowisko Konfederacji Lewiatan do projektu Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

Remarks of the Polish Confederation Lewiatan on the proposal of Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (CSAM)

We support the European Commission's goal to create a comprehensive legislative framework to ensure better protection of children against sexual abuse and exploitation. However, we believe the Regulation should be modified to become more effective from a child safety perspective, and less intrusive from a privacy perspective. In this note, we specifically focus on detection orders as a particularly concerning element of the proposal.

In this note, we specifically focus on detection orders as a particularly concerning element of the proposal.

Prevention

Child sexual abuse is a complex societal problem and combating it requires a holistic approach that looks at preventing harm from happening in the first place, empowering people to stay safe, responding to potentially harmful situations and supporting victims. The European Commission's draft proposal focuses almost exclusively on content detection but we believe that, in order to truly meet its objective of preventing and combating child sexual abuse online, the text should adopt a broader approach and focus on outcomes such as preventing harmful contact from happening and illegal content from being created and tackling the distribution of such content.

We do not oppose the idea of having a mechanism that would ensure that providers would be mandated to take action against Child Sexual Abuse Material (CSAM) and grooming, if they were found - through the risk assessment procedure - to have failed to take sufficient steps to meaningfully reduce risk of harm. However, such a mandatory regime should not focus on detection measures only (as the concept of the "detection order" suggests), but take a broader view of combating CSAM and grooming by explicitly including a reference that such orders concern measures combating and preventing those heinous crimes. Without such reference, the mandatory regime is likely to fall short of effectively addressing the range of risks involved.

End-to-end encryption

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

A mandatory obligation to detect and report CSAM and grooming in encrypted communications would undermine people's privacy and security by effectively requiring companies to access all users' text messages, photos and videos at all times for evidence of nudity, sexual activity and potentially suspicious combinations of words. We do not believe this is a safe, effective or proportionate approach to tackling CSAM and grooming.

A detection order mandating access to private communications is incompatible with EU law, including the prohibition on general monitoring enshrined in the DSA. The current proposal does not meaningfully outline how detection orders meet strict requirements of necessity and proportionality or provide for safeguards, such as those included in the Interim CSAM Derogation regarding permissible technologies. Such safeguards should be stipulated by law to ensure lawfulness and consistency in application across the EU.

Furthermore, we are seriously concerned that the proposal fails to exclude end-to-end encrypted messaging services from an obligation to scan message contents. Such a requirement is fundamentally incompatible with what users expect from an end-to-end encrypted messaging service: namely that no one – including any government or the messaging service itself – other than the sender and the recipient of a message can access its contents. Encrypted messaging services should be permitted to meet their obligations to tackle CSAM and grooming without accessing message contents: for example, through product design, user reporting and other privacy-preserving techniques.

End-to-end encryption protects people from serious crimes like hacking, fraud and identity theft; it enables secure communications for journalists, government officials, activists and individuals who may be targeted by authoritarian or illiberal regimes; and empowers people who may be subjected to domestic violence or hate crimes. In the context of increasing cybercrime and digital authoritarianism, encryption keeps people and their most sensitive information safe and private.

In its impact assessment[1], the European Commission has shown a worrying preference for widely-disputed detection technologies such as 'client-side scanning'. Experts[2] [3] [4] [5] [6]agree that it is not possible to deploy these technologies without breaking the fundamental promise of end-to-end encryption. Even a well-intentioned effort to build a system that

[1] Impact Assessment Report: Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse
[2] Internet Society: Fact Sheet: Client Side Scanning
[3] OHCHR Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (2015)
[4] Open letter on the position of scientists and researchers on the EU's proposed Child Sexual Abuse Regulation
[5] BSR: Human Rights Impact Assessment on Meta's Expansion of End-to-End Encryption
[6] Susan Landau et al: Bugs in Our Pockets: The Risks of Client-Side Scanning

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

scans messages for illegal activity would open the door to broader abuses by hackers and other hostile actors, creating an intolerable risk to all users' security.

The European Commission has not outlined in its proposal or assessment the limitations of such detection technologies or how risks of unintended consequences to privacy and security will be avoided. The European Data Protection Supervisor (EDPS) had already warned of the risks of breaking encryption in the fight against child abuse in its opinion on the Interim Derogation[7] and in its joint opinion with the European Data Protection Board (EDPB) on the draft Regulation[8].

Other safeguards

Finally, while we welcome the safeguards attached to detection orders, including judicial review, they must be proportionate and effectively protect the privacy of all users. Detection orders must also be consistent with the recently reconfirmed principle in the DSA that prohibits general monitoring obligations.

KL/363/172/ET/2023

[7] EDPS: On the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online
[8] EDPB - EDPS joint opinion n 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy