

17 de março de 2022

Prezada **Presidente da Comissão Europeia Ursula von der Leyen**,
Prezada **Vice-Presidente Executiva Margrethe Vestager**,
Prezado **Vice-Presidente Věra Jourová**,
Prezado **Vice-Presidente Dubravka Šuica**,
Prezada **Comissária Ylva Johansson**,
Prezado **Comissário Thierry Breton**,
Prezada **Comissária Margaritis Schinas**,

cc: Chefe de Gabinete Bjoern Seibert e Presidente da Comissão e Conselheiro Digital Anthony Whelan; Vice-Presidente Executivo Vestager Chefe de Gabinete Kim Jørgensen e Vice-Chefe de Gabinete Christiane Canenbley; Vice-Presidente Jourová Chefe de Gabinete Renate Nikolay e Vice-Chefe de Gabinete Daniel Braun; Vice-Presidente Šuica Chefe de Gabinete Colin Scicluna e Vice-Chefe de Gabinete Deša Srsen; Comissário Johansson Chefe de Gabinete Åsa Webber e Vice-Chefe de Gabinete Tom Snels; Comissário Breton Chefe de Gabinete Valère Moutarlier e Vice-Chefe de Gabinete Lucía Caldet; Comissária Schinas Chefe de Gabinete Despina Spanou e Vice-Chefe de Gabinete Natasha Bertaud.

Ref.: Proteção dos direitos e liberdades digitais na Legislação para combater eficazmente o abuso infantil

O combate à disseminação online de material sobre abuso e exploração sexual infantil (CSAM, “child sex abuse material” em inglês) é uma parte importante da extensa luta global para proteger jovens contra o abuso e exploração sexual. Em particular, esta luta exige uma abordagem abrangente por parte de governos e empresas para evitar tais crimes graves antes que eles aconteçam. No contexto da **iminente aprovação da legislação da União Europeia (UE) para combater eficazmente o abuso infantil**, instamos a Comissão para que garanta que a legislação seja elaborada sem prejudicar as comunicações privadas dos indivíduos.

Como os eventos chocantes das últimas três semanas enfatizaram, **privacidade e segurança são direitos que se reforçam mutuamente**. As pessoas sob ataque na Ucrânia dependem de tecnologias que preservam a privacidade para se comunicar com jornalistas, para coordenar a proteção de suas famílias e para lutar por sua segurança e direitos. Igualmente em tempos de paz, a capacidade das pessoas de comunicar-se sem intrusão injustificada - seja online ou offline - é vital para seus direitos e liberdades, bem como para o desenvolvimento de indústrias, associações e comunidades vibrantes e seguras.

Acreditamos firmemente que precisamos trabalhar juntos para encontrar soluções de longo prazo para enfrentar a disseminação de material sobre abuso e exploração sexual infantil no ambiente online, que sejam baseadas em evidências e respeitem todos os direitos fundamentais e o Estado de Direito. Acreditamos que recorrer a ‘soluções’ tecnológicas rápidas e ‘balas de prata’ não são apenas ineficazes, como também pode resultar em consequências indesejadas para a privacidade e o sigilo das comunicações de cada pessoa, incluindo as de crianças e sobreviventes de abuso.

Os especialistas concordam que não há como dar às autoridades policiais acesso excepcional às comunicações criptografadas de ponta a ponta sem criar vulnerabilidades

que podem ser exploradas por criminosos e governos repressivos¹. Como os recentes escândalos da Pegasus demonstraram, a varredura sem restrições dos dispositivos das pessoas representa enormes riscos para jornalistas, políticos, defensores dos direitos humanos e para a preservação de uma sociedade democrática.

Nós, as 39 organizações abaixo assinadas, pedimos, portanto, à Comissão Europeia que garanta que a próxima legislação respeite no mínimo um conjunto de 10 princípios de direitos humanos cumulativos,² dos quais gostaríamos de destacar o seguinte:

1. **Sem vigilância em massa:** Nunca deve haver a varredura generalizada e automatizada das comunicações privadas da população, pois esta é uma prática inerentemente desproporcional sob a legislação da UE. A legislação para combater eficazmente o abuso sexual infantil não deve obrigar os prestadores de serviços a tomar medidas ou garantir resultados que os forcem a conduzir tais práticas;
2. **As intervenções nas comunicações privadas da população devem ser direcionadas com base em suspeitas individuais:** Qualquer intromissão nas comunicações privadas deve ser feita com base em suspeitas específicas, razoáveis e individuais, conforme prescrito por lei e com supervisão judicial, para ser justificada;
3. **As medidas devem possuir menor grau de invasão possível à privacidade e limitar-se à detecção apenas de material sobre abuso e exploração sexual infantil:** Para garantir isso, o Comitê Europeu para a Proteção de Dados (CEPD) deve fornecer orientações sobre as tecnologias apropriadas. As medidas que quebram ou minam a criptografia (como a varredura do lado do cliente, "*client-side scanning*", em inglês); que são experimentais ou imprecisas; ou que criam riscos de cibersegurança, sempre criarão muito mais problemas do que podem resolver.

As organizações da sociedade civil ajudaram a moldar o Regulamento Geral sobre a Proteção de Dados (GDPR), a nova proposta de Regulamento ePrivacy, e a evitar regras ilegais de retenção de dados. Acreditamos, portanto, que uma colaboração mais estreita na próxima elaboração ajudaria a garantir uma legislação que seja eficaz, necessária e proporcional ao seu propósito. Isto também poderia ajudar a **evitar litígios que poderiam derrubar partes do futuro Regulamento, se obrigasse os prestadores de serviços a se intrometerem nas comunicações privadas das pessoas sem suspeitas justificáveis.**

Como defensores dos direitos humanos com experiência em tecnologia, reiteramos as limitações inerentes a qualquer "solução" tecnológica para problemas criminosos complexos como a disseminação de material sobre abuso e exploração sexual infantil, que exigem uma abordagem holística. Ao alcançar o objetivo de proteger as crianças, incluindo a prevenção da criação de material sobre abuso e exploração sexual infantil em primeiro lugar, sugerimos explorar intervenções sociais e humanas pelo menos tão intensamente quanto as baseadas na tecnologia.

Em uma sociedade que respeita a democracia e o Estado de Direito, os governos não

¹ Ver <https://arxiv.org/abs/2110.07450>.

² Ver <https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/>.

podem tomar medidas *a qualquer custo*. **E em um mundo em que cada aspecto de nossas vidas é cada vez mais digital, as medidas que põem em risco a privacidade e o sigilo das comunicações se tornarão cada vez mais perigosas.**

Esperamos que nossos comentários os ajudem nas etapas finais da preparação da legislação. Estamos à sua disposição para fornecer apoio e aconselhamento sobre este documento.

Assinado,

European Digital Rights (EDRi)
ApTI (Romênia)
Big Brother Watch (Reino Unido)
Bits of Freedom (Países Baixos)
Centre for Democracy & Technology (CDT) (Internacional)
Committee to Protect Journalists (CPJ) (Internacional)
Data Rights (Países Baixos / Europeu)
dataskydd.net (Suíça)
Defend Digital Me (Reino Unido)
Deutscher Anwaltverein (DAV) (Alemanha)
Deutsche Vereinigung für Datenschutz (DVD) (Alemanha)
Digitalcourage (Alemanha)
Digitale Gesellschaft (Alemanha)
Državljan D/Citizen D (Eslovênia)
Electronic Frontier Foundation (EFF) (Internacional)
Electronic Frontier Finland (Effi)
Entropia (Alemanha)
European Center for Not-for-Profit Law (ECNL)
European Sex Workers' Rights Alliance (ESWA)
Foundation for Information Policy Research (FIPR) (Reino Unido / Europeu)
Global Voices (Países Baixos / Internacional)
Homo Digitalis (Grécia)
Internet Society Catalan Chapter (ISOC-CAT) (Europeu)
ISOC Brazil - Brazil Chapter of the Internet Society (Brasil)
IT-Pol Denmark
LGBT Technology Partnership (Internacional)
Ligue des droits humains (Bélgica)
Mnemonic (Alemanha / Internacional)
Open Governance Network for Europe
Open Rights Group (ORG) (Reino Unido)
Privacy and Access Council of Canada
Privacy International (PI)
Ranking Digital Rights (Internacional)
Tech for Good Asia
Vrijdschrift.org (Países Baixos)