O conflito entre a defesa da privacidade e a luta contra o abuso sexual de crianças na União Europeia

Nuno M. Guimarães (guimaraesn@acm.org), Nuno T. Castro (teixeiracastro81@gmail.com)
Internet Society Portugal (isoc.pt)

Os anos recentes têm tornado evidente a preocupação com a explosão de conteúdos digitais nocivos (*harmful content*) em particular os associados ao abuso sexual de crianças[1] (*child sexual abuse*). No quadro da estratégia de luta contra o abuso sexual de crianças de 2020[2], foi recentemente anunciada pela Comissão Europeia (CE) uma proposta de regulação das regras de prevenção e combate a esse crime[3,4]. A proposta é especialmente dedicada ao espaço digital (*online*) e inclui um conjunto de prescrições aos agentes, utilizadores e fornecedores de serviços desse espaço a que chamamos a "*internet*".

A proposta, de 11 de Maio de 2022, e que fará agora o caminho legislativo entre o Parlamento Europeu e o Conselho Europeu[5] (órgão que reúne os chefes de governo da EU), tem sido considerada um ataque sério à privacidade nas comunicações interpessoais, pelo facto de induzir a eliminação do mecanismo básico de garantia da privacidade, a criptografia ponto-a-ponto (*end-to-end encryption, infra* E2EE).

Apresentamos aqui a nossa visão sobre o problema, para suscitar análise crítica e tomadas de posição da sociedade civil. Referimos sumariamente a proposta da CE, um contexto de análise das consequências, um quadro tecnológico e enquadramento jurídico e legislativo. Nas conclusões explicitamos o que antevemos como riscos desta proposta.

1. A proposta da Comissão Europeia

A proposta da CE[3] pretende impor regras, operadas pelo Centro Europeu de Abuso Sexual de Crianças, essencialmente dirigidas aos operadores de serviços de alojamento de informação (*hosting*) e comunicações interpessoais (*infra* designados de operadores). As regras obrigarão a: (1) avaliação e mitigação de risco relativo a conteúdos nocivos e aliciamento (*solicitation/grooming*); (2) possibilidade de emissão de ordens de deteção obrigatória de conteúdos nocivos ou de aliciamento, por autoridade nacional ou tribunal; (3) aplicação de salvaguardas na execução dessas ordens de deteção, minimizando a invasão de privacidade e taxas de erro (falsos positivos); (4) reporte ao Centro Europeu por parte dos operadores; (5) remoção compulsiva de material nocivo ou bloqueio de acesso no caso do seu alojamento em jurisdições não cooperantes (aqui a ordem dirige-se aos fornecedores de acesso básico à internet); (6) impossibilidade de download de apps promotoras de aliciamento de crianças; (7) emissão de ordens de deteção por parte de tribunais ou autoridades nacionais independentes.

O texto da proposta[4] detalha este conjunto de regras até ao artigo 9º, introduz de seguida um artigo específico relativo a tecnologias e salvaguardas, artigo 10º. O capítulo II especifica obrigações dos fornecedores. Não são aqui relevantes as disposições dos capítulos III e seguintes, sobre estruturas de coordenação e supervisão, ou a especificação administrativa do Centro EU.

Duas conclusões óbvias extraímos da proposta: (1) os destinatários principais são os operadores; (2) a eliminação da E2EE não é explicitamente proposta (legislação hábil) mas pode ser a consequência inevitável. Esta seria a perspetiva pessimista.

2. Consequências da quebra de segurança nas comunicações interpessoais

A quebra das condições de segurança nas comunicações interpessoais, nomeadamente no que se refere à confidencialidade relativamente ao seu conteúdo, é um ataque direto e essencial à privacidade dos cidadãos e até das empresas e organizações.

A privacidade é, obviamente a par com a dignidade humana em causa no crime de abuso sexual de crianças, um direito fundamental para uma cidadania completa, consagrado na generalidade dos textos constitucionais

---

[1] O Código Penal português, Decreto Lei 48/95, artigos 171º e ss, considera a distinção entre crianças – até 14 anos e menores – entre 14 e 18. Nas diretivas europeias encontramos "abuso sexual de crianças". Usamos esta terminologia.
[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12433-EU-strategy-to-fight-child-sexual-abuse_en
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472
[5] https://www.consilium.europa.eu/en/

das sociedades livres e abertas, desde a Declaração Universal dos Direitos do Homem (artigo 12º), Convenção Europeia dos Direitos Humanos (artigo 8º), Constituição da República Federativa do Brasil (artigo 5º) ou Constituição da República Portuguesa (onde funda o princípio como estruturante do Estado de direito democrático, no seu artigo 2º, e igualmente desenvolvido, por exemplo, no artigo 26º).

A privacidade é essencial ao estado de direito democrático. Ao cidadão comum, permite-lhe o seu livre desenvolvimento da personalidade, consagrando-lhe, por exemplo, o direito à solidão, intimidade, auto-reflexão e reserva, condições para autonomia pessoal e liberdade[6]. A privacidade é uma expressão da segurança individual e coletiva[7] e é condição de sustentabilidade de uma sociedade e cultura. A sua defesa no espaço digital é por isso um imperativo de sobrevivência de uma sociedade democrática, livre e aberta.

A garantia da confidencialidade na comunicação interpessoal na internet, suportada na E2EE, é o equivalente da defesa constitucionalmente consagrada da correspondência ou comunicações telefónicas. Não deve ser posta em causa de forma generalizada, fora de um quadro judicialmente bem determinado. Mais ainda, qualquer retrocesso na confiança dos utilizadores nos meios digitais, contraria as necessidades de transição digital e põe em causa a estabilidade da economia digital.

3. Estado da arte tecnológico

A E2EE é uma tecnologia central nas aplicações de comunicação interpessoal, p.e. Whatsapp (aprox 2bi utilizadores[8]), Telegram (500m[9]) ou SIgnal (40m[10]). As tecnologias de criptografia utilizadas são em geral baseadas em chaves simétricas. Por exemplo no caso do Whatsapp[11] é usada a técnica AES-256 para codificação de mensagem e HMAC-SHA256 para autenticação. Sem mais detalhes técnicos, a consequência da aplicação destas técnicas é a impossibilidade prática de uma terceira parte (não envolvida na comunicação) descodificar a mensagem.

Uma questão importante sobre a privacidade destes sistemas é a proteção dos metadados, informação que descreve a mensagem e o contexto da comunicação. Esta proteção não está relacionada com a E2EE e tem sido publicamente contestada[12]. A privacidade dos metadados das comunicações interpessoais é um tema vivo na Europa e até recentemente em Portugal como mencionamos *infra*.

Em alternativa à eliminação da E2EE como requisito para deteção e moderação de conteúdos nocivos, têm vindo, a ser propostos métodos de moderação de conteúdos compatíveis com a defesa da privacidade, suportando reporte de utilizadores, deteção de conteúdos conhecidos, deteção baseada em classificadores privados, rastreamento de conteúdos e análise de popularidade de conteúdos (ver p.ex.[13,14]).

Como nota final, recordamos que, mesmo impondo requisitos a operadores, a tecnologia de comunicações seguras e indecifráveis continua disponível e simples. Por exemplo, um sistema de correio eletrónico com PGP (Pretty Good Privacy)[15], garantindo privacidade e confidencialidade das comunicações, sem operador centralizado, é facilmente concretizável. A tecnologia atual permite a criação, por todos, inclusive e sobretudo por organizações criminosas, de mecanismos de comunicação protegidos e inacessíveis. Em consequência, contrariamente ao que é a filosofia do combate ao grande crime organizado, medidas deste tipo arriscam-se a afetar somente criminosos individuais, com perfil de "amador" ou "consumidor". As grandes redes criminosas podem cifrar as suas comunicações sem a ajuda sistemas de mensagens convencionais.

---

[6] Alan Westin, Privacy and Freedom, 1967
[7] James H. Moor, Towards a Theory of Privacy in the Information Age, Computers and Society, September1997
[8] https://www.thinkimpact.com/whatsapp-statistics/
[9] https://www.businessofapps.com/data/telegram-statistics/
[10] https://www.businessofapps.com/data/signal-statistics/
[11] https://www.whatsapp.com/security
[12] https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users
[13] Jonathan Mayer, Content Moderation for End-to-End Encrypted Messaging
https://www.cs.princeton.edu/~jrmayer/papers/Content_Moderation_for_End-to-End_Encrypted_Messaging.pdf
[14] Kulshrestha, A. and Mayer, J. Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation, https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha
Proceedings of the 30th USENIX Security Symposium, August 11–13, 2021, 978-1-939133-24-3
[15] https://www.openpgp.org

4. Enquadramento legislativo e jurídico

A proposta da CE não determina expressamente a eliminação da E2EE e é aliás muito cuidadosa nas referências à quebra da criptografia. A experiência anterior da CE relativamente a diretivas[16] na área do controlo e acesso a informação sobre comunicações pessoais constitui decerto um referencial de prudência.

Um exemplo importante na UE foi a decisão do Tribunal de Justiça Europeu (ECJ) de 2014 – caso *Digital Rights Ireland Ltd*[17] - que invalidou os termos da diretiva comunitária (95/46/EC) sobre proteção dos direitos individuais face ao processamento de dados pessoais e ao livre movimento desses dados, em particular no que se refere ao armazenamento, por parte das operadoras, dos metadados das comunicações interpessoais para fins de investigação criminal. Essa decisão do ECJ foi incluída na fundamentação recente (04-2022) da declaração de inconstitucionalidade, pelo Tribunal Constitucional Português[18], da respetiva transposição portuguesa, invocando questões relacionadas com a localização/jurisdição do armazenamento dos dados, o princípio jurídico da proporcionalidade e as garantias de proteção e recurso.

A aprovação e posterior eficácia da proposta de lei que aqui referimos poderá assim ser questionada pelos órgãos judiciais europeus se conduzir, de forma explícita, na letra da diretiva, ou implícita, na sua aplicação, a soluções de condicionamento desproporcional e desprotegido das garantias de privacidade dos cidadãos. No caso da abordagem desta diretiva, este questionamento é mais complexo de efetivar *a priori* dado que a diretiva em si mesma delega as soluções para os operadores e não determina *de jure*, apenas potencialmente *de facto*, a eliminação da E2EE.

Uma análise mais elaborada das potenciais consequências da proposta, e que aqui não apresentamos, requer a consideração de outras normas europeias, p.e. Digital Markets Act e Digital Services Act, em fase final de promulgação, do próprio Regulamento Geral de Proteção de Dados (RGPD/GDPR) e das normas relativas a fluxos e armazenamento de dados, p.e. para equacionar o impacto das jurisdições não cooperantes.

5. Conclusões

Com o quadro que descrevemos, podemos, nesta fase, apresentar as seguintes conclusões:

(1) **Tecnicamente**, a proposta da CE é omissa quanto à defesa da criptografia, nomeadamente E2EE, como fundamento técnico para garantia do direito fundamental e constitucional à privacidade. Ao tornar os operadores responsáveis pela deteção de conteúdos nocivos, obriga implicitamente ao acesso destes às comunicações e à quebra da confidencialidade e privacidade. Os métodos e algoritmos utilizados numa análise automática introduzem ainda no espaço das comunicações interpessoais o problema dos enviesamentos (*bias*) e induzem indiretamente concentração da oferta, dado que pequenos operadores não possuem dados em escala para uma automatização fiável. Em geral, a passagem de prerrogativas públicas para a esfera privada dos operadores (poucos grandes gigantes mundiais) reforça a oportunidade para o uso de modelos de funcionamento cada vez menos transparentes e que afastam o espaço digital do ideal de rede aberta que a ISOC defende.

(2) **Constitucionalmente**, ao remeter para os operadores a responsabilidade de concretização técnica da deteção de conteúdos nocivos, a CE protege-se do eventual recurso para proteção de direitos fundamentais junto do ECJ ou do Tribunal Europeu dos Direitos do Homem. No caso do Brasil, no imediato, a questão europeia aqui em foco não se coloca. Por sua vez, no caso português, vingando a tese da CE - da erosão da privacidade (por troca com um aparente maior sentimento de segurança) - o ordenamento jurídico-constitucional português não tutela, propriamente, uma figura efetiva de proteção de direitos, liberdades e garantias. À falta de uma queixa de constitucionalidade (próxima das figuras

[16] As normas europeias manifestam-se de variadas formas: no caso, as diretivas, de acordo com os quadros constitucionais de cada Estado membro, são posteriormente objeto de transposição para leis nacionais pelos órgãos legislativos competentes – parlamentos e/ou governos - de cada país.
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62012CA0293
[18] https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

germânicas) ou recurso de amparo (das hispânicas), o acesso à justiça constitucional, em Portugal simplesmente não existe, comprometendo a defesa da pessoa contra o Estado (ou mesmo contra privados),

(3) **Economicamente/do ponto de vista do mercado**, as decisões regulatórias impulsivas e generalizadas, que contrariam necessidades e valores fundamentais dos utilizadores podem conduzir a médio prazo a uma reconfiguração das soluções tecnológicas que continuam a demonstrar capacidade de inovação incontrolável, e acabam por não resolver o problema original, no caso, o controlo de material nocivo,

(4) **Eticamente**, sendo o abuso sexual de crianças um atentado intolerável à dignidade humana e que deve ser combatido por todos os meios possíveis e razoáveis, a proposta da CE pode ser usada como um caso de referência para qualquer domínio – substituamos literalmente a expressão "*abuso sexual de crianças*" por "*ofensa à moral pública*" ou "*desrespeito pelo Estado*". Apesar de, no quadro da cultura europeia, essa substituição parecer um absurdo, temos de ter consciência de que podemos estar a criar mecanismos de referência, técnicos e jurídicos, para o controlo dos cidadãos. E a Europa de hoje não pode dizer que isso nunca acontecerá dentro das suas fronteiras, sendo a distância curta entre o atual capitalismo da vigilância[19] e Estado totalitário.

As pulsões securitárias são uma enfermidade do estado de direito democrático. A diluição da fundamentalidade dos direitos basilares, como a troca da liberdade por segurança, é um caminho de simples justificação, mas perigoso para todos, individual e coletivamente e é uma porta de entrada para espaços totalitários.

Os dilemas colocados pelo crescimento da sociedade digital, não são mais complexos que outros desafios tecnológicos e sociais e devem ser resolvidos com serenidade e maturidade sem colocar em causa o valor fundamental da liberdade digital, e real, dos cidadãos.

Lisboa, 31 de Maio de 2022. Os nossos agradecimentos aos Professore José Legatheaux Martins e Rogério Reis pelos comentários ao texto e ao Observatório da Criptografia, projeto do IP.Rec (Instituto de Pesquisa em Direito e Tecnologia do Recife) pelo convite à sua publicação.

[19] Shoshana Zuboff, The Age of Surveillance Capitalism, 2019, Public Affairs