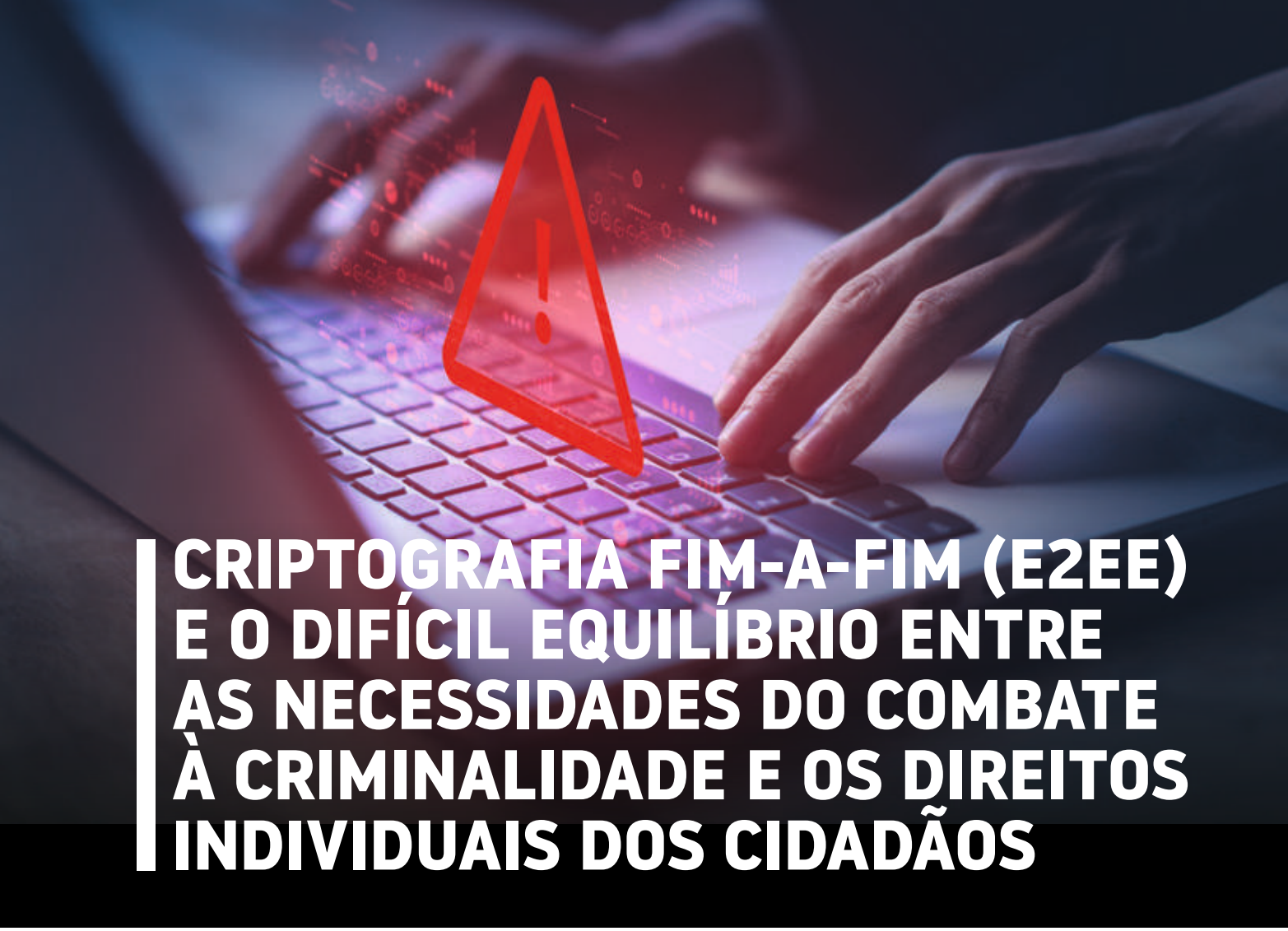

CRIPTOGRAFIA FIM-A-FIM (E2EE) E O DIFÍCIL EQUILÍBRIO ENTRE AS NECESSIDADES DO COMBATE À CRIMINALIDADE E OS DIREITOS INDIVIDUAIS DOS CIDADÃOS

JOSÉ LEGATHEAUX MARTINS
PROFESSOR JUBILADO DA FACULDADE DE CIÊNCIAS E TECNOLOGIA DA UNIVERSIDADE NOVA DE LISBOA
PRESIDENTE DO CAPÍTULO PORTUGUÊS DA INTERNET SOCIETY DE 2017 A 2021

A criptografia [1] é usada pelos exércitos e os estados pelo menos desde o tempo de Júlio César. Até ao final da II Guerra Mundial, a sociedade civil fazia um uso reduzido da criptografia, mas com a generalização das comunicações telefónicas e, posteriormente, a generalização de comunicações digitais via Internet, a utilização civil da criptografia vulgarizou-se, estando atualmente na base da segurança e confiabilidade do novo mundo digital.

Com a invenção de algoritmos de cifra simétrica (invioláveis sempre que usam chaves de dimensão adequada), e sobretudo após a invenção da criptografia de chave pública, a utilização pelas aplicações de criptografia fim-a-fim, isto é, E2EE – End-to-End Encryption, tornou-se dominante. Com estes novos métodos e protocolos, cuja implementação está disponível em código aberto, de utilização sem restrições por qualquer ator, as chaves de cifra usadas são apenas conhecidas das partes em comunicação – os operadores da rede, as plataformas e os serviços de vigilância dos estados não conseguem ter acesso ao conteúdo das comunicações depois destas serem cifradas. Só antes ou depois de terem sido cifradas [2].

O conceito do direito à privacidade e a sua cada vez maior relevância foi crescendo ao longo dos séculos. No século XX, com a sua inscrição na Declaração Universal dos Direitos Humanos [3] e na legislação dos países que adotam o modelo de Estado de Direito, a privacidade é um direito bem reconhecido. Nos outros estados esse direito está vedado sempre que entra em conflito com as necessidades dos agentes do poder, decisão essa tomada pelos próprios, sem qualquer intervenção de tribunais independentes.

A privacidade tem também custos sociais negativos e por isso não é um direito absoluto. Por exemplo, a privacidade permite esconder crimes públicos, como os de violência doméstica. A criptografia fornece, portanto, uma arma suplementar a quem pretende infringir a lei, pois esconde comunicações que poderiam permitir detetar e provar os crimes. Nas sociedades regidas pelas regras dos Estados de Direito introduziram-se mecanismos que tentam equilibrar os direitos dos cidadãos com as necessidades da aplicação da lei.

Por exemplo, a polícia pode solicitar a gravação e acesso a comunicações telefónicas de indivíduos, desde que tal seja autorizado pelo juiz de instrução do processo. A implementação

deste preceito jurídico particular é realista dado existir um pequeno número de operadores telefónicos licenciados e as comunicações telefónicas não usarem criptografia E2EE. Daqui resulta que as conversações telefónicas de suspeitos podem ser conhecidas da polícia, mas proíbe-se, simultaneamente, pelo menos em teoria, que todas as comunicações da sociedade civil estejam sujeitas a devassa generalizada. Desta forma, procura-se um equilíbrio, em teoria razoável, entre as necessidades de combater o crime e a proteção da privacidade dos cidadãos e das empresas.

A evolução recente da Internet veio alterar este quadro. Por um lado, o uso de E2EE é acessível a todos: cidadãos honestos e desonestos. Por outro lado, as aplicações que usam E2EE são comuns e variadas. Mesmo que essas aplicações fossem proibidas é fácil implementar alternativas. Daqui resulta um novo quadro, no qual os métodos de vigilância anteriormente descritos e usados na rede telefónica deixaram de ser possíveis. De facto, cada vez mais comunicações de voz e vídeo transitaram para aplicações que fazem uso de E2EE, como por exemplo: WhatsApp, Signal, Proton Mail, etc.

Recentemente, muitos estados ocidentais decidiram introduzir legislações para atacarem este problema, como por exemplo a "Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual de crianças" [4], muitas vezes também designadas propostas anti CSAM ("Child Sexual Abuse Material"). A norma jurídica proposta pretende introduzir uma nova abordagem ao combate às atividades ilegais na Internet e tem, entre outros, o objetivo de permitir à polícia e aos reguladores acederem em claro às mensagens trocadas entre utilizadores na Internet, para detetarem atividades suspeitas de pedofilia ou terrorismo.

Há um debate aceso sobre como este acesso poderia ser implementado nos casos em que é utilizada E2EE. No entanto, a comunidade científica perita em criptografia assinalou o que é óbvio. Só há duas formas de implementar esse acesso: ou proibir na prática o uso de E2EE ou introduzir aquilo que se designa por "Client-Side Scanning" (CSS), isto é, captar o conteúdo antes (na origem) ou depois (no destino) de este ser cifrado.

Com efeito, a introdução de chaves de cifra só acessíveis à polícia ou aos reguladores só seria tecnicamente possível usando métodos que, por definição, não são E2EE. Mesmo assim, o registo dessas chaves pelas autoridades criaria um gigantesco problema de segurança, pois as mesmas nunca poderiam cair nas mãos erradas. O outro método consiste em aceder às comunicações antes de estas serem cifradas ou depois de serem decifradas. Isto é, a polícia, ou os operadores das aplicações, teriam de ter acesso completo aos dispositivos dos utilizadores. Tal como no caso anterior, a monitorização dos dispositivos é sujeita a *hacks* e *bugs* que permitiriam aos espiões, criminosos e outros agentes malignos terem acesso não autorizado aos dispositivos das pessoas e aos conteúdos dos mesmos. Estes métodos são desmontados num recente artigo publicado por reputados especialistas internacionais em segurança [5].

Adicionalmente, a grande maioria das novas propostas legislativas de combate a CSAM torna as plataformas, em particular as de suporte das redes sociais, parcialmente responsáveis pelo combate a publicações ilegais ou que possam ser usadas para fins ilegais. Isso parece ser implementado exportando para as plataformas parte do papel dos reguladores. Como é natural, estas vão implementar esses controlos recorrendo a aprendizagem automática, uma tecnologia com falsos positivos, que só podem ser evitados através de curadoria manual, normalmente deficientemente implementada devido ao seu elevado custo.

Na prática, os estados estariam a exportar para as plataformas parte do papel de vigilância e por extensão a responsabilidade pelas garantias e direitos dos cidadãos, o que é barato na aparência, mas reforça a centralidade e o papel de plataformas que funcionam com base na recolha de dados privados e um modelo económico que já foi designado "Capitalismo de Vigilância" [6]. A regulação estaria assim a dar-lhes armas de reforço do seu modelo de atuação, sem contribuir para combater os seus efeitos negativos mais gerais.

Felizmente que alguns governos reconhecem que a solução para os novos problemas colocados às autoridades policiais pelo complexo novo mundo digital não deve passar pela generalização da análise massiva das comunicações privadas entre pessoas. Por exemplo, a legislação proposta pelo Governo do Canadá para combate à pedofilia [7] coloca explicitamente fora da sua alçada as plataformas de mensagens, usem ou não E2EE. Os desafios colocados por este novo contexto ao combate ao crime não podem ser resolvidos por formas desproporcionadas, como reconhecem pareceres dos serviços jurídicos do Conselho da União Europeia [8]. Temos de ser mais inventivos. |

[1] Fernando Boavida e Mário Bernardes, "Introdução à Criptografia," FCA, 2019

[2] "Reflections on Ten Years Past the Snowden Revelations," RFC 9446 - IETF, 2013 - Ver especialmente o Capítulo 5

[3] "Declaração Universal dos Direitos Humanos," Nações Unidas, 1948 - Ver o Artigo 12º

[4] Consultar a proposta "COM (2022) 209 final" em https://eur-lex.europa.eu, maio 2022

[5] Harold Abelson et al., "Bugs in your pockets: the risk of client-side scanning," Journal of Cybersecurity, Volume 10, Issue 1, 2024

[6] Shoshana Zuboff, "A Era do Capitalismo de Vigilância," Relógio de Água, Lisboa 2019

[7] House of Commons of Canada, "Online Harms Act - Bill C-63," fevereiro de 2024

[8] Legal Service of the Council of the European Union, "Advice 8787/23 on proposal COM (2022) 209 final. Advice on detection orders in interpersonal communications – Right to privacy and protection of personal data – proportionality"

INGENIUM
A ENGENHARIA PORTUGUESA EM REVISTA

SÉRIE II | N.º 184 | ABRIL.MAIO.JUNHO 2024

Propriedade **Ordem dos Engenheiros**
Diretor **Fernando Manuel de Almeida Santos**
Diretores-adjuntos **Lídia Manuela Duarte Santiago, Jorge Manuel Pais Marçal Liça**

Editor
Ordem dos Engenheiros
Av. António Augusto de Aguiar, 3 D, 1069-030 Lisboa
NIPC 500 839 166

Conselho Editorial
Fernando Manuel de Almeida Santos, Lídia Manuela Duarte Santiago, Jorge Manuel Pais Marçal Liça, António Gonçalves da Silva, José Maria Mendes Ribeiro de Freitas Albuquerque, Isabel Cristina Gaspar Pestana da Lança, Nelson Artur Carmelo Jerónimo, Nuno Miguel Tomás, Pedro Venâncio

Sede, Administração, Redação, Publicidade e Produção
Revista INGENIUM
Av. António Augusto de Aguiar, 3 D, 1069-030 Lisboa
T 213 132 600 | F 213 524 630 | E ingenium@oep.pt
www.ordemengenheiros.pt/pt/centro-de-informacao/ingenium

Coordenação Geral **Nuno Miguel Tomás** CPJ 4100
Edição **Nuno Miguel Tomás** CPJ 4100
Redação **Pedro Venâncio** CPJ 7733
Colégios e Especializações **Alice Freitas**
Publicidade e Marketing **ingenium@oep.pt**
Produção, Circulação e Assinaturas **ingenium@oep.pt**
Projeto Gráfico e Paginação **Sofia Pavia Saraiva** (For Yesterday Projects, Lda.)
Impressão **Lidergraf – Sustainable Printing**, Rua do Galhano, 15 – 4480-089 Vila do Conde
Publicação **Trimestral** | Tiragem **41.500 exemplares**
ERC 105659 | API 4074 | Depósito Legal 2679/86 | ISSN 0870-5968 | INPI 485958
Estatuto Editorial **www.ordemengenheiros.pt/pt/centro-de-informacao/ingenium**

ORDEM DOS ENGENHEIROS

2024 IGUALDADE DE GÉNERO NA ENGENHARIA

ORDEM DOS ENGENHEIROS
Bastonário **Fernando Manuel de Almeida Santos**
Vice-presidentes Nacionais **Lídia Manuela Duarte Santiago, Jorge Manuel Pais Marçal Liça**

CONSELHO DIRETIVO NACIONAL
Fernando Manuel de Almeida Santos, Lídia Manuela Duarte Santiago, Jorge Manuel Pais Marçal Liça, Bento Adriano de Machado Aires e Aires, José Manuel Reis Lima Freitas, Isabel Cristina Gaspar Pestana da Lança, Luís Filipe da Costa Neves, António José Vieira Alves Carias de Sousa, Jorge Manuel Gamito Pereira, José Miguel Brazão Andrade da Silva Branco, Teresa Maria Soares Costa

CONSELHO DE ADMISSÃO E QUALIFICAÇÃO
Rosa Maria Guimarães Vaz Costa (Civil), Luís Manuel Coelho Guerreiro (Civil), Isabel Maria de Almeida Ribeiro de Oliveira (Eletrotécnica), Catarina Maria Ribeiro Pinto Marques (Eletrotécnica), António José Coelho dos Santos (Mecânica), Manuel Carlos Gameiro da Silva (Mecânica), Carlos Alberto Esteves Leitão (Geológica e de Minas), Maria Luísa Pontes da Silva Ferreira de Matos (Geológica e de Minas), Luís Alberto Pereira de Araújo (Química e Biológica), Cristina Maria dos Santos Gaudêncio Baptista (Química e Biológica), Bento Manuel Domingues (Naval), Victor Manuel Gonçalves de Brito (Naval), Maria Teresa de Vasconcelos e Sá Pereira (Geográfica), Octávio Magalhães Borges Alexandrino (Geográfica), António Augusto Fontainhas Fernandes (Agronómica), Maria Rosário da Conceição Cameira (Agronómica), Cláudia Marisa Viliotis (Florestal), Ana Paula Soares Marques de Carvalho (Florestal), Maria de Fátima Reis Vaz (Materiais), Rodrigo Ferrão de Paiva Martins (Materiais), Ricardo Jorge Silvério Magalhães Machado (Informática), Alberto Manuel Rodrigues Silva (Informática), Carlos Alberto Diogo Soares Borrego (Ambiente), António João Carvalho de Albuquerque (Ambiente)

PRESIDENTES DOS CONSELHOS NACIONAIS DE COLÉGIOS
Humberto Salazar Amorim Varum (Civil), Manuel de Matos Fernandes (Eletrotécnica), Carlos Alberto Sousa Duarte Neves (Mecânica), Joaquim Eduardo Sousa Góis (Geológica e de Minas), António Gonçalves da Silva (Química e Biológica), Dina Maria Correia Santos Paz Dimas (Naval), João Manuel Agria Torres (Geográfica), Raul da Fonseca Fernandes Jorge (Agronómica), João Carlos Lobão Tello da Gama Amaral (Florestal), José Maria Mendes Ribeiro de Freitas Albuquerque (Materiais), Vasco Miguel Moreira do Amaral (Informática), João Pedro Cortez Moraes Rodrigues (Ambiente)

REGIÃO NORTE **Conselho Diretivo** Bento Adriano de Machado Aires e Aires (Presidente), Maria João de Sousa Teles Brochado Correia (Vice-presidente), José Manuel Reis Lima Freitas (Secretário), Ana Cláudia Moreira Teodoro (Tesoureira), José António Silva de Carvalho Campos e Matos (Vogal), Ana Carina Vila Pouca Quintas (Vogal), Vítor António Pereira Lopes de Lima (Vogal)
REGIÃO CENTRO **Conselho Diretivo** Isabel Cristina Gaspar Pestana da Lança (Presidente), Ricardo José Leal Duarte (Vice-presidente), Luís Filipe da Costa Neves (Secretário), Virgínia Clara Macedo Elói Fernandes Manta (Tesoureira), Jorge Miguel Sá Silva (Vogal), Pedro Jorge Gonçalves Carreira (Vogal), Maria Isabel Rodrigues Quintaneiro (Vogal)
REGIÃO SUL **Conselho Diretivo** António José Vieira Alves Carias de Sousa (Presidente), Rita Maria Diogo de Carvalho de Moura (Vice-presidente), Jorge Manuel Gamito Pereira (Secretário), Pedro Manuel da Hora Santos Coelho (Tesoureiro), Carla Patricia Cunha Melfe de Figueiredo (Vogal), Daniel Vaz Silva (Vogal), Susana Antas Serôdio (Vogal)
REGIÃO MADEIRA **Conselho Diretivo** José Miguel Brazão Andrade da Silva Branco (Presidente), Beatriz Rodrigues Jardim (Vice-presidente), Bernardo Oliveira Melvill de Araújo (Secretário), Luísa Filipa Mendonça Rodrigues (Tesoureira), Higino José Vasconcelos Lemos Silva (Vogal), Luísa Maria Gouveia (Vogal), Roberto da Silva de Jesus (Vogal)
REGIÃO AÇORES **Conselho Diretivo** Teresa Maria Soares Costa (Presidente), André do Canto Brandão Cabral (Vice-presidente), Luís Gonzaga Pereira (Secretário), José António Silva Brum (Tesoureiro), Délia Margarida Silva Carvalho (Vogal), Miguel Pironet San-Bento Almeida (Vogal), Sandra Micaela Ferreira Cabral (Vogal)

www.ordemengenheiros.pt

NESTA EDIÇÃO