O Blog

Carta Aberta à Presidência da União Europeia

01/04/2021 Categoria: Criptografia

em Defesa da Liberdade de Utilização de Criptografia Segura

Publicada igualmente como artigo de opinião no jornal Público

À Presidência Portuguesa do Conselho da União Europeia em 2021

Caro Primeiro-Ministro, António Costa,

Escrevemos-lhe para partilhar as nossas preocupações sobre as consequências que poderão resultar do que parece ser uma nova orientação da União Europeia sobre a utilização da criptografia digital para fins civis, tanto no que respeita aos direitos e garantias dos cidadãos, como no retrocesso dos progressos feitos para uma transição digital, assim como nas suas consequências.

Sob o argumento que importa combater o crime organizado e a ameaça terrorista, o Conselho da União Europeia (CUE), na sua nota de 24.11.2020, assim como a Comissão Europeia (CE), no seu comunicado de 9.12.2020, afirmam a intenção de vir a regulamentar o uso de criptografia nas comunicações digitais com o objectivo de, quando para isso mandatados pela justiça poderem as autoridades policiais "ler" as comunicações cifradas. Ora importa ter presente os seguintes factos quando se considera tal intenção:

1. As primitivas criptográficas hoje disponíveis não permitem que sejam satisfeitos os objectivos referidos por CUE e CE sem que sejam postas em causa as garantias que os actuais protocolos oferecem.
2. Sem novas (e improváveis) primitivas criptográficas, a única forma de satisfazer os propósitos expressos por CUE e CE terá que passar pelo enfraquecimento dos sistemas criptográficos existentes. Não é razoável esperar que tal enfraquecimento voluntário da criptografia usada não pudesse ser aproveitado para quebrar a sua utilização, portanto facilitando um outro conjunto de acções criminosas. Isto iria abalar drasticamente a confiança pública na utilização da rede de comunicação digital o que poderia ter consequências dramáticas para uma economia, como a de hoje, fortemente assente nas transacções digitais.
3. Não chega que existam sistemas criptográficos que tenham tal característica, é necessário também que os actuais sistemas deixem de ser usados. A única forma de tal se alcançar seria a de proibir o uso de sistemas criptográficos tradicionais, o que afectará somente o cidadão comum, sem beliscar as práticas criminosas.
4. Qualquer "solução" que passe por alterar o comportamento das peças de software com vista aos mesmos objetivos (a criação de "backdoors") traduzir-se-á na constituição de ainda maiores vulnerabilidades e ainda piores resultados para a segurança dos sistemas e consequentemente factores para a diminuição da confiança dos utilizadores em meios digitais.
5. Há actos e contextos que o nosso edifício jurídico não admite que sejam escrutináveis, nem sob mandato judicial. Esta nova ordem criptográfica agora proposta teria, portanto, que classificar os cidadãos entre os que poderiam usar criptografia forte de forma legal e os outros que teriam que cometer um crime para o fazer.

Os subscritores alertam que, a ser prosseguida esta linha de regulamentar de forma canhestra o uso de criptografia, desta resultará:

- Não se ganhar qualquer eficácia no combate aos crimes que se diz querer evitar pois, como se viu, não é possível impedir a utilização de criptografia alternativa.
- A criminalização, em contrapartida, de um grande conjunto de acções até agora tomadas como legítimas e justificáveis.
- Atentar contra a confiança pública, entretanto construída nas comunicações digitais assim como o seu uso generalizado, pondo em risco o equilíbrio de uma economia digital cuja importância hoje é considerável.
- Uma dramática redução das garantias dadas ao cidadão comum acerca do seu direito à privacidade.
- A promoção duma situação que pode constituir terreno fértil ao desenvolvimento de regimes de forte controlo das populações em detrimento das suas liberdades democráticas.

Os signatários,

Eduardo Santos, Presidente da Associação D3 – Defesa dos Direitos Digitais

José Rebelo, Presidente da Associação de Estudos Comunicação e Jornalismo (AECJ)

Marcos Marado, Vice-Presidente da Associação Nacional para o Software Livre (ANSOL)

Maria Helena Monteiro, Presidente da Associação Para o Desenvolvimento da Sociedade da Informação (APDSI)

Ana Alves Pereira, Presidente da Associação Portuguesa de Bibliotecários, Arquivistas, Profissionais da Informação e Documentação

José Legatheaux Martins, Presidente do Capítulo Português da Internet Society (ISOC PT)

31/3/2021

PUBLICADO EM CRIPTOGRAFIA, ENCRYPTION, NEWS, PRIVACIDADE, PRIVACY