Acerca da Anunciada Mudança de Política da Comissão Europeia Sobre a Utilização da Criptografia Ponto a Ponto

10 de Fevereiro de 2021

Análise da Direção do Capítulo Português da Internet Society da Anunciada Mudança de Política da Comissão Europeia Sobre a Utilização da Criptografia Ponto a Ponto

Lisboa, 10 de Fevereiro de 2021

Com o aparecimento e difusão da internet assistiu-se, nas últimas décadas, a um notável desenvolvimento das redes de comunicações digitais, um notável alargamento do âmbito de utilização destas redes e o consequente explodir de uma economia digital para lá das mais optimistas previsões. Pode-se dizer que quase nenhum aspecto da nossa vida social e profissional foi deixado incólume a esta verdadeira revolução tecnológica. Os cidadãos passaram a comunicar entre si, à distância, usando maioritariamente estes meios. Passaram, da mesma forma, a poder efectuar compras e vendas efectuando os respectivos pagamentos de forma digital. Passaram a relacionar-se como principais serviços do estado também usando redes de comunicações digitais. Podemos dizer que foram transpostas para este novo mundo virtual um grande conjunto de actividades humanas e com elas um significativo conjunto de prerrogativas de cidadania.

A transposição destes actividades, que sempre foram executadas até então de forma presencial, para este novo ambiente só foi possível pela introdução da Criptografia nos protocolos que as serve de suporte. A criptografia é usada, neste caso, não somente para manter informação somente acessível para um conjunto seleccionado de actores nessas actividades assim como para um conjunto muito maior de garantias para que tais acções se possam desenrolar sem as garantias que o facto de serem presenciais lhes confere automaticamente. São processos criptográficos que garantem a identidade dos intervenientes em cada acção realizada via internet, permitem que estes assinem documentos e mensagens, arbitram compras, asseguram que jogos decorrem segundo as regras estabelecidas, definem e garantem que os diversos papeis que cada um

desempenha em cada acção sejam respeitados. Portanto não é exagerado dizer que sem a criptografia que hoje é omnipresente na maioria dos protocolos em que a internet assenta, esta não poderia ter a importância que hoje lhe reconhecemos.

Argumentando que importa combater o crime organizado e a ameaça terrorista a CE afirma no seu comunicado de 9.12.2020[1] (mas que já havia sido referido em comunicado anterior sobre outro tema[2]) 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. Essa intenção, reafirmada no Q&A da CE sobre o primeiro comunicado, vai aliás na linha das declarações da comissária Ylva Johansson[3], no sentido de "encontrar uma solução para o problema da criptografia" e corresponde a iniciativas legislativas, no mesmo sentido apresentadas no senado dos USA[4]. Mesmo sem pôr em causa as intenções sobre que assenta tal decisão, esta comporta, em nossa opinião, riscos e erros de avaliação que importa considerar.

1. As primitivas criptográficas hoje disponíveis não permitem que sejam satisfeitos os objectivos referidos pela CE sem que sejam postos em causa as garantias que os actuais protocolos oferecem. Não é expectável que somente porque se deseja que os sistemas criptográficos passem a permitir que uma autoridade credenciada possa decifrar uma comunicação cifrada, seja possível criar tal sistema criptográfico mantendo este todas as outras características necessárias ao papel que desempenham nos diversos protocolos. Apesar de uma história de mais de um par de milénios, foi somente na década de 1970 que passamos a dispor de "criptografia de chave pública" sobre a qual assenta uma grande parte dos protocolos referidos.
2. Sem novas (e improváveis) primitivas criptográficas a única forma de satisfazer os propósitos expressos pela CE terá que passar pelo enfraquecimento dos sistemas criptográficos existentes. Ora o equilíbrio entre a capacidade de cifrar (da criptografia) e a capacidade de decifrar sem acesso à respectiva chave (criptoanálise) é muito frágil. Os sistemas criptográficos estão permanentemente sob o escrutínio dos estudiosos da matéria e por isso estão continuamente a ser descobertas novas fraquezas e vulnerabilidades que permitiriam quebrar as cifras e novas cifras a ser criadas ou robustecidas para tentar obstar tais ataques. Não é razoável esperar que tal enfraquecimento voluntário da criptografia usada não pudesse ser aproveitado para quebrar a sua utilização. Isso significaria que para se tentar dificultar um conjunto de crimes se estaria a facilitar um outro conjunto de acções criminosas. Para além do evidente absurdo, 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. Mas, seja qual for a solução para implementar tal possibilidade de escrutínio por parte das autoridades das comunicações digitais, seja por obtenção de novas primitivas criptográficas ou por enfraquecimento dos sistemas actuais, ela por si não resolve o problema. Não chega que existam sistemas criptográficos que tenham tal característica,

---

[1] Brussels, 9.12.2020 COM(2020) 795 final, "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond".

[2] Brussels, 24.7.2020 COM(2020) 607 final, "EU strategy for a more effective fight against child sexual abuse".

[3] Speech by Commissioner Johansson at a webinar on "Preventing and combating child sexual abuse & exploitation: towards an EU response", 9.6.2020.

[4] "Lawful Access to Encrypted Data Act'', GRAHAM, COTTON and BLACKBURN, 116th 2D Senate session.

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. Mas nem para o crime organizado nem para as organizações terroristas esta ilegalização vai constitui qualquer tipo de factor dissuasivo. As suas acções são intrinsecamente ilegais não será mais um regulamento de comunicações que constituirá obstáculo. Pelo contrário, será ao cidadão comum que se colocará o dilema de perder a protecção e garantias que a criptografia lhe deu, até esse momento, ou passar ele próprio a ser classificado de criminoso.

4. Qualquer "solução" que passe por, a montante da solução criptográfica, alterar o comportamento das peças de software (ou mesmo dos sistemas operativos) com vista aos mesmos objetivos (a criação de "backdoors), para além de ser impossível tornar universal, 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, como é o exemplo da relação médico/doente, advogado/cliente, jornalista/fonte, já para não referir o âmbito militar ou diplomático. Isso não obstou que fossem transpostas para o mundo digital as interacções dessas esferas. 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.

A ser prosseguida esta linha, agora ensejada, de regulamentar de forma canhestra o uso de criptografia, esta terá como consequência:

- 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.
- O risco de pôr em causa 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.

Monte da Caparica, 10/2/2020

A Direção do Capítulo Português da Internet Society

Assinado por delegação pelo Presidente da Direção

Associação ISOC Portugal Chapter
Departamento de Informática da FCT/UNLCampus da Caparica
2825-516 Monte da Caparica
https://isoc.pt **direcao@isoc.pt**