COMO PROTEGER A PRIVACIDADE DO CONSUMIDOR E A SEGURANÇA DE DADOS NA ERA DO 5G?[1]

Mikołaj Barczentewicz[2] and Fred Roeder[3]

SUMÁRIO

Esta proposta de política pública analisa os atuais riscos relacionados à privacidade dos consumidores europeus, expõe como as normas atuais são insuficientes para proteger a privacidade dos consumidores na era de tecnologias 5G e examina soluções legais e políticas que minimizem a exposição dos consumidores a vazamentos de dados e a violações de privacidade.

O escopo desta análise

• Os principais interesses dos consumidores incluem não apenas preços baixos e a rápida adoção de novas tecnologias, mas também privacidade e proteção de dados.

• Ações governamentais e privadas que enfraqueçam a privacidade e a proteção de dados expõem os consumidores a risco de danos significativos (por exemplo: crime financeiro, roubo de identidade).

• Concentramo-nos no problema da vulnerabilidade de dispositivos e de softwares a interferências maliciosas (proteção de dados). Focamos nossa proposta em produtos e serviços de consumo, bem como em infraestrutura eletrônica.

---

[1] Tradução de Pedro Gonet Branco (Editor-chefe da RED|UnB. Graduando em Direito pela Universidade de Brasília. Visiting student na UC Berkeley).

[2] Mikołaj Barczentewicz é Professor Assistente da Faculdade de Direito da Universidade de Surrey, Pesquisador Associado da Universidade de Oxford, e Privacy Fellow no Consumer Choice Center, onde atua principalmente com questões jurídicas e éticas associadas às novas tecnologias. Estudou Direito e Filosofia nas Universidade de Oxford e de Varsóvia. Antes de estudar em Oxford, era advogado especializado em direito Europeu e regulamentação no escritório de Varsóvia da DZP, e um especialista em Direito e Política na Fundação FOR (uma ONG polaca fundada pelo Professor Leszek Balcerowicz). Notoriamente, Mikołaj liderou uma campanha para aumentar o escopo da liberdade de informações na Polônia e, nessa campanha, processou com sucesso o Presidente da Polônia em um caso perante os mais altos tribunais polacos.

[3] Fred Roeder é Economista de Saúde e Diretor Administrativo do Consumer Choice Center. Atua na área consultiva (para governos, ONGs e setor privado) sobre reformas econômicas em dezenas de países, com foco em mercados emergentes e países pós-comunistas. Além da saúde, suas áreas de pesquisa são transporte, telecomunicações e tecnologias digitais. É membro do conselho de diversas empresas de tecnologia na Europa e na América do Norte e em conselhos consultivos de empresas e organizações sem fins lucrativos.

Recomendações

• Os consumidores são mais bem servidos por políticas focadas em resultados e baseadas em evidências. Medidas extremas como proibições totais baseadas no país de origem devem ser tidas como último recurso.

• Recomendamos a atribuição de responsabilidade legal a operadores e revendedores de software e de dispositivos que exponham os consumidores a riscos de interferência maliciosa e ilegal. Outra possível medida é a responsabilização pessoal dos diretores das empresas.

• A responsabilização legal deve ter o apoio da certificação de segurança de software e de dispositivos (conforme proposto na Lei de Segurança Cibernética da União Europeia[4]). A abordagem proposta pela Comissão da União Europeia em sua nova recomendação sobre segurança de redes 5G é condizente com nossas recomendações.

• A promoção de rígidos protocolos de criptografia e de métodos seguros de autenticação devem ser parte significativa do esforço empreendido na proteção dos interesses do consumidor.

INTRODUÇÃO

Os consumidores estão expostos a novos e significativos riscos devidos à dependência de softwares e dispositivos conectados à Internet. Essa dependência deve crescer cada vez mais com a adoção de redes 5G e de dispositivos com sistema de conexão à Internet das Coisas

Novos casos de roubos de identidade, crimes financeiros e outras formas de ataques e interferência maliciosa são descobertos diariamente. Recentemente foi revelado um ataque de hackers ao servidor de atualização de software de um dos principais fabricantes de hardware do mundo, o que permitiu aos invasores instalar *backdoors* em milhares de computadores[5]. A situação se agravou com a divulgação de notícia na imprensa de que a fabricante demorou para reagir ao alerta de segurança, permitindo, assim, que os ataques continuassem. Por outro lado, há governos que almejam estabelecer métodos de acesso a dados pessoais que não dependam do consentimento dos usuários (por exemplo, colocando pressão sobre os fabricantes para que incluam *backdoors* em seus dispositivos), o que prejudica a segurança de produtos e serviços digitais.

Tais incidentes são evidência de que a proteção de dados do consumidor e, consequentemente, a própria privacidade do consumidor,

[4] European Union's "Cybersecurity Act"

[5] Kim Zetter, 'Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers' (Motherboard, 25 de março de 2019) <https://motherboard.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates- to-install-backdoors-on-thousands-of-computers >

não estão sendo tratadas com a devida seriedade. Alguns fabricantes e desenvolvedores de software tendem a dar excessiva importância a características que os clientes percebem à primeira vista, como preços baixos, e se esquecem que os consumidores também têm interesse por privacidade e proteção de dados. Acreditamos na necessidade de uma resposta política inteligente que incentive os agentes do mercado a darem valor à proteção de dados dos usuários, mas que não promova distorções indevidas no mercado, nem limite o poder de escolha do consumidor.

Neste documento, concentramo-nos em soluções políticas que salvaguardem os interesses dos consumidores. Nossa preocupação maior não é com os limites que devem existir nas medidas de segurança pública adotadas pelos governos, mas ressaltamos que os métodos que minam a proteção de dados podem tornar-se ferramentas para qualquer ator suficientemente motivado e competente. Em outras palavras, os *backdoors* instalados por governos democráticos liberais podem ser usados por criminosos ou governos estrangeiros.

POSSÍVEIS SOLUÇÕES

Apresentamos três possíveis políticas públicas que podem resolver o problema: responsabilidade legal, certificação e proibições baseadas no país de origem. Elas não são mutuamente exclusivas – em princípio, todas podem contribuir para uma política abrangente que proteja a privacidade do consumidor e a segurança dos seus dados. Todas elas possuem algum grau de desvantagem do ponto de vista do consumidor. Acreditamos, no entanto, que as **regras de responsabilidade** são as mais capazes de alcançar o melhor equilíbrio entre fornecer segurança aos consumidores e o custo de fazê-lo. Não estamos convencidos de que as proibições baseadas no país de origem devam ser implementadas no contexto atual.

É bem-vinda a nova Recomendação da Comissão Europeia sobre Segurança Cibernética de redes 5G, dado que a abordagem adotada é consistente com a nossa recomendação e estabelece o equilíbrio ideal entre os custos potenciais para os consumidores e os benefícios que os consumidores terão do aumento da segurança dos dados[6].

Algumas das suposições que fizemos ao oferecer as recomendações:

• Não existe uma única solução para proteger a privacidade do consumidor e a segurança dos dados. Precisamos de uma combinação de soluções e essa combinação provavelmente mudará com o tempo.

• A competição saudável entre diferentes jurisdições e entre empresas privadas é o melhor mecanismo para a descoberta das ferramentas certas.

[6] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks <http://europa.eu/rapid/press-release_IP-19-1832_en.htm?locale=en>.

Todos que trabalham em soluções para questões de cibersegurança, no entanto, devem dar maior importância aos interesses do consumidor.

• Não nos posicionamos sobre quais são as melhores soluções tecnológicas e, portanto, adotamos a neutralidade tecnológica.

• As normas atuais (por exemplo, o art. 32 da GDPR[7]) não fornecem clareza suficiente quanto ao padrão de segurança nas cadeias de suprimento exigido.

RESPONSABILIDADE

É recomendável que a lei influencie empresas privadas (como fabricantes e importadoras de dispositivos digitais, operadoras de telecomunicações) ao adotar de regras de responsabilidade para os que utilizam ou revendem software ou dispositivos com vulnerabilidades que tragam riscos para a privacidade do consumidor e para a segurança de dados. Isso deve pressionar os fornecedores não-europeus a adotarem o conceito de *security-by-design* e a se esforçarem para comprovar que o fizeram.

Em certa medida, tais regras de responsabilidade (e outros mecanismos de coerção) já existem, dado que a proteção de dados e de comunicações é prevista em lei no âmbito da União Europeia (por exemplo, Art. 32 GDPR e Art. 16 da Diretiva NIS[8]) e em âmbito nacional. Novas normas deverão ser criadas, no entanto, para que se possa responsabilizar legalmente as fabricantes e as importadoras de *hardware* que vendam produtos com falhas de segurança.

Também recomendamos a responsabilização pessoal de diretores de empresas que falhem em proteger os elementos aqui discutidos.

Independentemente da existência ou não de regras de responsabilidade geral, há manifesta necessidade de orientação oficial mais específica, ou mesmo de novas normas, sobre o padrão apropriado de segurança para software e hardware. Tanto as normas de segurança digital da União Europeia quanto as dos Estados-membros tendem a exigir apenas que as "medidas adequadas" sejam tomadas.

A Agência da União Europeia para Segurança de Redes e Informações (ENISA), por exemplo, em suas diretrizes para Pequenas e Médias Empresas, restringe-se a determinar que apenas aqueles que processam

[7] Art. 32 of the General Data Protection Regulation <https://gdpr.eu/article-32-security-of-processing/ >.

[8] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union" <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ :L:2016:194:TOC>

dados pessoais devem garantir que "software e hardware são obtidos por fornecedores confiáveis, seguindo procedimentos contratuais formais"[9]. Considerando a grande preocupação em relação aos ataques a cadeias de suprimentos (de que é exemplo o ataque ao servidor de atualização de software mencionado anteriormente) e até mesmo as falhas de segurança inseridas propositadamente pelos fabricantes, essa diretriz falha em fornecer uma base legal efetiva e adequada para os problemas postos.

Para resolver o problema da falta de clareza e eficácia das normas de proteção de dados (e, consequentemente, do padrão de responsabilidade), deve-se levar em conta o seguinte:

- Os padrões técnicos devem ser os mais tecnologicamente neutros possível. Especificamente, não se deve exigir a adoção de equipamentos específicos, pois isso poderá se tornar uma barreira à entrada de novas empresas no mercado e ao desenvolvimento tecnológico.
- Em vez disso, as regras devem focar em resultados e ser tão gerais quanto possível, na medida em que forneçam orientação suficiente para regular o tema.
- Os padrões devem ser de fácil identificação e adoção não apenas pelos maiores agentes do mercado, que podem facilmente dedicar recursos significativos ao cumprimento da norma.

Esses objetivos são difíceis de se alcançar por meio de normas gerais, como a GDPR. Uma possível solução complementar é a adoção de sistemas certificação.

CERTIFICAÇÃO DE SOFTWARE E DISPOSITIVOS

A responsabilidade por vulnerabilidades poderia ser excluída ou reduzida se o dispositivo ou serviço em questão fosse certificado como seguro. Alguns países da União Europeia operam sistemas de certificação de segurança, mas, conforme as razões apresentadas na proposta da Lei de Segurança Cibernética da União Europeia, a proteção é insuficiente[10].

O sistema de certificação proposto na lei – dependendo de como for implementado – poderá contribuir significativamente para assegurar a proteção dos dados do consumidor. Espera-se, no entanto, que os padrões de certificação sejam adequados, dada a existência de perigos potenciais,

[9] ENISA, "Guidelines for SMEs on the security of personal data processing" (December 2016), <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-proces sing>

[10] "Proposal of a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')" <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477R(02)&qid=1553611735328&from=EN>.

como a exigência governamental de que fabricantes implementem *backdoors* em seus produtos.

Recomendamos que os sistemas de certificação a serem desenvolvidos conforme a Lei de Segurança Cibernética da União Europeia exijam as seguintes exigências nos produtos e serviços direcionados aos consumidores ou que lidem com dados de consumidores:

- Criptografia. Criptografia de ponta-a-ponta das comunicações e criptografia de dados em repouso aumentam significativamente o nível de proteção contra interferência maliciosa. Acreditamos que quanto menor a qualidade da criptografia adotada, maior deve ser a probabilidade de responsabilização (e maiores devem ser as penas) pelos problemas decorrentes de vulnerabilidades no sistema ou de violações de segurança.
- Autenticação. Os consumidores devem ter a opção de usar exclusivamente o método de autenticação mais seguro disponível para determinado produto ou serviço (isto é, sem a necessidade da utilização forçada de métodos menos seguros, como SMS). Para serviços on-line, isso significa aceitar o padrão W3C WebAuthn (permitindo *login* a partir de dispositivos físicos, como o YubiKey, da Yubico, ou o Titan, da Google).

PROIBIÇÕES BASEADAS NO PAÍS DE ORIGEM

Há razões para se acreditar que alguns governos exigem, legal ou informalmente, que empresas privadas incluam certas vulnerabilidades em seus *softwares* e dispositivos para que elas possam ser exploradas por agentes do Estado ou com a cooperação do fabricante. Isso tem sido usado como justificativa para que se proíba a venda por atacado de produtos e serviços com base no país de origem deles. **Tais proibições dificilmente são do interesse do consumidor**.

A proibição de venda por atacado supostamente motivada por questões de segurança produz os mesmos efeitos que uma restrição ao comércio no contexto de guerra comercial. A primeira vítima de qualquer conflito comercial são os consumidores do país que impõem barreiras tarifárias e não-tarifárias ao comércio. A menos que não haja outra solução viável e que haja manifesta evidência de risco de segurança, essa solução não deve ser adotada.

Os consumidores são melhor atendidos por políticas focadas em resultados e baseadas em evidências. Instrumentos extremos, como a proibição total baseada no país de origem, devem ser vistos como último recurso.