

# Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática

**Autor(a):** Daniel Sarmento

**Publicado em:** 14 de maio de 2020

**Publicação:** jota\_import

**Link JurisTube:** <https://juristube.com.br/colunistas/daniel-sarmiento/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica>

**Fonte original:** <https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-e-m-tempos-de-erosao-democratica>

**Identificador citável:** [juristube.com.br/colunistas/daniel-sarmiento/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica#ep-66bbe4af](https://juristube.com.br/colunistas/daniel-sarmiento/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica#ep-66bbe4af)

## Resumo

*Duas ações no Supremo discutem a possibilidade de suspensão do funcionamento de aplicativos de mensagem*

## Texto integral

Está na pauta do STF do dia 20 de maio o julgamento da ADI 5527 e da ADPF 403, que discutem a possibilidade de suspensão do funcionamento de aplicativos de mensagem – como WhatsApp, Telegram, Signal e Messenger –, em caso de descumprimento de decisão judicial que determine a quebra do sigilo das comunicações entre usuários do serviço. Na ADI 5527, da relatoria da ministra Rosa Weber, objetiva-se a declaração de inconstitucionalidade de preceitos do Marco Civil da Internet, que supostamente permitiriam, nessa hipótese, a suspensão do funcionamento dos aplicativos. Já na ADPF 403, relatada pelo ministro Edson Fachin, foram questionadas decisões judiciais que determinaram a suspensão do funcionamento do WhatsApp, com pedido de proibição de novas decisões da mesma natureza, por violarem as liberdades de expressão e comunicação e o princípio da proporcionalidade. A impossibilidade de suspensão judicial de aplicativos de mensagem é reconhecida de modo praticamente unânime, e foi afirmada na medida liminar concedida pelo STF na ADPF 403. Afinal, parece absolutamente despropositado atribuir a todo e qualquer juiz brasileiro a possibilidade de suspender nacionalmente um serviço que hoje talvez constitua o principal instrumento de comunicação cotidiana para a maior parte da população brasileira – só o WhatsApp tem atualmente mais de 120 milhões de usuários no país. Tais suspensões judiciais violam claramente os princípios constitucionais da proporcionalidade e da liberdade de comunicação e expressão. Contudo, outra questão mais delicada vem sendo debatida no âmbito dos referidos processos, e talvez o STF venha a decidi-la no julgamento conjunto das ações. A questão é a seguinte: os aplicativos de comunicação mais utilizados no Brasil se utilizam de tecnologia conhecida como “criptografia de ponta-a-ponta”. Através dela, apenas as próprias pessoas que se comunicam têm acesso às mensagens umas das outras. O conteúdo dessas mensagens permanece absolutamente inacessível, não apenas para terceiros, como também para o próprio aplicativo. Trata-se de mecanismo que robustece a proteção da privacidade e da segurança nas comunicações para todos os usuários do serviço. A tecnologia usada pelos principais aplicativos de mensagem – pelo menos este é o caso do WhatsApp – não permite que a criptografia de ponta-a-ponta seja

afastada, mesmo temporariamente, para usuários específicos. Esse ponto foi esclarecido por inúmeros especialistas, na audiência pública conjunta realizada pelo STF na ADPF 403 e ADI 5527. Com isso, torna-se tecnicamente inviável o cumprimento de decisões judiciais que decretem a interceptação ou a quebra do sigilo das comunicações realizadas por meio de tais aplicativos. Essa quebra de sigilo demandaria a modificação da própria tecnologia utilizada, com a introdução de uma vulnerabilidade no sistema de criptografia, por vezes chamada de backdoor , por meio da qual a operadora do aplicativo pudesse acessar o conteúdo das mensagens dos seus usuários, ou viabilizar esse acesso por autoridades públicas. Muito embora inexista qualquer norma legal impondo aos aplicativos a criação da backdoor, há quem sustente que o STF deveria decretar essa obrigação. O argumento é que, sem isso, dificulta-se a investigação de crimes, já que os órgãos estatais competentes ficam impossibilitados de monitorar as conversas de suspeitos e acusados quando travadas por meio de aplicativos, mesmo com a devida ordem judicial. O argumento é sedutor, mas não procede. É que, se a tecnologia fosse efetivamente alterada para permitir a quebra do sigilo das mensagens, certamente essa vulnerabilidade do sistema de criptografia também poderia ser utilizada por terceiros ou pelo próprio Estado, fora das hipóteses legalmente admitidas. Na prática, seria impossível limitar o uso da backdoor, impedindo a sua utilização, por exemplo, por hackers, para as mais diversas finalidades escusas; por autoridades estatais, fora dos casos juridicamente permitidos – em desvios ou arroubos autoritários –; ou mesmo por funcionários inescrupulosos dos próprios aplicativos. Em outras palavras, a imposição de mudança na tecnologia dos aplicativos de mensagem, com a criação da backdoor, não atingiria apenas os suspeitos de crime, mas toda a população que se utiliza dos respectivos serviços, quase sempre de modo lícito e inocente. Do ponto de vista jurídico, isso significa dizer que a ponderação subjacente ao caso não é entre, de um lado, a privacidade de possíveis criminosos, e, do outro, a segurança pública de toda a sociedade. Trata-se, na verdade, de colisão entre os direitos fundamentais de todos os usuários dos aplicativos de mensagem e o interesse público no aperfeiçoamento de investigações criminais. Os usuários desses aplicativos – vale dizer, a grande maioria da população brasileira – seriam atingidos de várias formas. A sua privacidade seria gravemente afetada, pois as comunicações, que hoje eles podem travar com segurança, estariam permanentemente expostas ao risco de invasões por terceiros. A sua liberdade de expressão também seria ameaçada. Com o risco permanente de bisbilhotice e de monitoramentos ilícitos, as pessoas tenderiam a se abster de falar o que desejam, ou a alterar o conteúdo das suas mensagens. Afinal, como falar com liberdade, se nossas conversas puderem estar sendo captadas por hackers, criminosos ou por arapongas? A segurança de muitas das atividades pessoais e profissionais das pessoas, cada vez mais realizadas através de aplicativos, também seria seriamente comprometida. Como ficariam as conversas íntimas entre casais e parceiros amorosos, diante do risco permanente de invasões ilícitas? E os bate-papos entre amigos e familiares, sempre marcados pela espontaneidade? Como profissionais e empresas poderiam tratar com segurança dos seus negócios, em conversas on-line ? E quanto às próprias autoridades públicas, inclusive judiciais, que também usam aplicativos de mensagem para o desempenho das suas funções? Por perceberem que a fragilização da criptografia nas comunicações on-line viola direitos da população, diversas entidades voltadas à proteção de direitos humanos vêm condenando as tentativas de imposição de criação de backdoors . Nessa linha, a Anistia Internacional, por exemplo, registrou que a criptografia é questão de direitos humanos, e que obrigação de criação de backdoors, por atingir a liberdade de expressão e a privacidade de todos os usuários, é inerentemente desproporcional e contrária ao direito internacional dos direitos humanos.

[1] Na mesma direção, a relatoria sobre liberdade de expressão da ONU afirmou que “ falhas

intencionais (nos sistemas de criptografia) invariavelmente prejudicam a segurança de todos os usuários on-line, uma vez que as backdoors, mesmo quando criadas apenas para o acesso de autoridades públicas, podem ser acessadas por entidades não autorizadas, como outros estados ou atores não estatais. Diante do seu impacto amplo e indiscriminado, as backdoors afetam desproporcionalmente todos os usuários” [2] . Essas preocupações agravam-se ainda mais no contexto de erosão da democracia, vivenciado atualmente em diversos países, como o Brasil. No atual cenário, em que somos governados por presidente da República que celebra abertamente a ditadura militar, ataca diariamente os direitos humanos e busca aparelhar as instituições republicanas, é preciso adotar precauções adicionais diante dos riscos de arbítrio e de autoritarismo estatal. Diante desse quadro, será que vale impor mudança tecnológica aos aplicativos de mensagem que pode potencializar a vigilância estatal sobre a vida dos cidadãos – especialmente dos críticos e adversários dos governantes de plantão? Vale baixar a guarda e facilitar, quem sabe, o advento de um distópico Big Brother – o de George Orwell e não o transmitido pela Rede Globo – que possa espionar as conversas cotidianas das pessoas? A resposta é muito clara. Agora, mais do que nunca, cabe ao Supremo proteger nossas liberdades. [1] Veja-se < <https://www.eff.org/deeplinks/2016/03/amnesty-international-encryption-human-rights-issue> >. No documento consta: “as medidas que obriguem as empresas a criar backdoors para a criptografia usada em seus produtos ou serviços (afetando todos os usuários) constituem uma significativa interferência nos direitos dos usuários à privacidade e à liberdade de expressão. Como essas medidas afetam de modo indiscriminado a privacidade on line de todos os usuários, prejudicando a segurança de suas comunicações eletrônicas e dados privados, a Anistia Internacional acredita que elas sejam inerentemente desproporcionais, e assim ilegítimas perante o direito internacional dos direitos humanos” (tradução livre). [2] Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the human right to freedom of expression, David Kaye, 22/05/2015, p. 15. Disponível em < <https://www.ohchr.org/en/issues/freedomofexpression/pages/callforsubmission.aspx> >.

## Como citar este documento

As citações abaixo seguem os padrões ABNT NBR 6023:2018, APA 7ª edição, Chicago Author-Date (17ª ed.) e BibTeX (LaTeX). Copie o formato exigido pelo periódico ou gerenciador bibliográfico (Zotero, Mendeley, EndNote).

### ABNT (NBR 6023:2018)

SARMENTO, Daniel. Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática. *jota\_import*, 14 maio 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica>. Acesso via: JurisTube — Acervo Digital de Direito. Disponível em: <https://juristube.com.br/colunistas/daniel-sarmiento/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica>. Acesso em: 31 ago. 2026.

### APA 7ª edição

Sarmiento, D. (2020, May 14). Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática. *\*jota\_import\**. <https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica>

### Chicago Author-Date (17ª ed.)

SARMENTO, Daniel. 2020. “Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática.” *\*jota\_import\**, May 14. <https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica>

### BibTeX

```
@article{daniel-sarmiento-aplicativos-criptografia-e-direitos-fund-2020,  
  author = {Sarmiento, Daniel},  
  title = {Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática},  
  journal = {jota_import},  
  year = {2020},  
  url = {https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica},  
  urldate = {2020-05-14}  
}
```



#### Licença de Uso — CC BY-NC-SA 4.0

Este conteúdo está licenciado sob a licença Creative Commons Atribuição-NãoComercial-Compartilhalguar 4.0 Internacional (CC BY-NC-SA 4.0). O uso para fins acadêmicos e educacionais é permitido, desde que citada a fonte original (JurisTube) conforme as normas técnicas indicadas neste documento.

*Termos completos:*

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt-br>

JurisTube — Acervo Digital de Direito

<https://juristube.com.br/colunistas/daniel-sarmiento/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica>

PDF gerado em 2026-08-31 03:56 UTC