



**PL 2630/2020  
00126**

SENADO FEDERAL  
GABINETE DA SENADORA DANIELLA RIBEIRO

**EMENDA Nº      , DE 2020**  
(ao PL 2630, de 2020)

**Suprima-se o art. 10, do substitutivo ao Projeto de Lei nº 2630, de 2020:**

### **JUSTIFICAÇÃO**

O dispositivo é apresentado como um mecanismo de “rastreadibilidade” do fluxo de mensagens, suposto recurso necessário à apuração e responsabilização do conjunto de indivíduos que teriam participado da difusão de um determinado conteúdo considerado ilícito. A “inovação” legislativa é apresentada a partir de um argumento equivocados, segundo o qual essa seria a única forma de investigação diante de aplicativos calcados em tecnologias de criptografia.

A obrigatoriedade ataca frontalmente diretriz fundante da Lei Geral de Proteção de Dados (Lei No 13.709 de 2018), aprovada por unanimidade no Congresso Nacional, segundo a qual a coleta de dados deve ser a estritamente necessária para as finalidades de determinado serviço. Este dispositivo, inserido como espinha dorsal do modelo de proteção de dados no Brasil (e já consagrado no Marco Civil da Internet, Lei No 12.965 de 2014), vai ao encontro do adotado na maioria das leis de proteção de dados no mundo, como é o caso do Regulamento Geral de Proteção de Dados da União Europeia.

Ao instar a guarda esses dados a priori, o Artigo 10o inverte o princípio da presunção de inocência da Constituição Federal. Somada à identificação massiva, a obrigatoriedade da guarda desses dados sujeita o conjunto da população ao risco diante de políticas vigilantes, medidas de mau uso de seus dados pelas empresas e, ainda, vazamentos. Em um cenário de aumento dos abusos por autoridades e ofensiva sobre as liberdades e direitos, tais mecanismos impõem um risco ainda maior aos usuários e àqueles que desejem fazer uso de seu direito legítimo à crítica e ao questionamento de autoridades e grupos políticos e econômicos.

Some-se a isso o problema de potencialidade de responsabilização de todas as pessoas que, por razões legítimas ou involuntárias, participem das cadeias de compartilhamento de conteúdos, como jornalistas, pesquisadores, parlamentares e até cidadãos ao, eventualmente, repassar determinada mensagem. De acordo com o texto, os dados dessas cadeias poderão ser identificados pelas empresas e caberá às pessoas envolvidas terem que provar, a posteriori, sua não relação com as indústrias de disseminação de desinformação que o PL pretende atingir.



SF/20198.73999-52



SENADO FEDERAL  
GABINETE DA SENADORA DANIELLA RIBEIRO

Por fim, é importante destacar que a jurisprudência do STF já reconheceu os metadados como passíveis da mesma proteção constitucional que o conteúdo das mensagens, de maneira que não se justifica a obrigatoriedade de sua guarda generalizada. O dispositivo é apresentado como um mecanismo de “rastreadabilidade” do fluxo de mensagens, suposto recurso necessário à apuração e responsabilização do conjunto de indivíduos que teriam participado da difusão de um determinado conteúdo considerado ilícito. A “inovação” legislativa é apresentada a partir de um argumento equivocados, segundo o qual essa seria a única forma de investigação diante de aplicativos calcados em tecnologias de criptografia.

A obrigatoriedade ataca frontalmente diretriz fundante da Lei Geral de Proteção de Dados (Lei No 13.709 de 2018), aprovada por unanimidade no Congresso Nacional, segundo a qual a coleta de dados deve ser a estritamente necessária para as finalidades de determinado serviço. Este dispositivo, inserido como espinha dorsal do modelo de proteção de dados no Brasil (e já consagrado no Marco Civil da Internet, Lei No 12.965 de 2014), vai ao encontro do adotado na maioria das leis de proteção de dados no mundo, como é o caso do Regulamento Geral de Proteção de Dados da União Europeia.

Ao instar a guarda esses dados a priori, o Artigo 10º inverte o princípio da presunção de inocência da Constituição Federal. Somada à identificação massiva, a obrigatoriedade da guarda desses dados sujeita o conjunto da população ao risco diante de políticas vigilantes, medidas de mau uso de seus dados pelas empresas e, ainda, vazamentos. Em um cenário de aumento dos abusos por autoridades e ofensiva sobre as liberdades e direitos, tais mecanismos impõem um risco ainda maior aos usuários e àqueles que desejem fazer uso de seu direito legítimo à crítica e ao questionamento de autoridades e grupos políticos e econômicos.

Some-se a isso o problema de potencialidade de responsabilização de todas as pessoas que, por razões legítimas ou involuntárias, participem das cadeias de compartilhamento de conteúdos, como jornalistas, pesquisadores, parlamentares e até cidadãos ao, eventualmente, repassar determinada mensagem. De acordo com o texto, os dados dessas cadeias poderão ser identificados pelas empresas e caberá às pessoas envolvidas terem que provar, *a posteriori*, sua não relação com as indústrias de disseminação de desinformação que o PL pretende atingir.

Por fim, é importante destacar que a jurisprudência do STF já reconheceu os metadados como passíveis da mesma proteção constitucional que o conteúdo das mensagens, de maneira que não se justifica a obrigatoriedade de sua guarda generalizada.

Sala das Sessões,

**Senadora DANIELLA RIBEIRO**  
**Progressistas-PB**



SF/20198.73999-52