**MINISTÉRIO DAS COMUNICAÇÕES**
Gabinete do Ministro

OFÍCIO Nº 3707/2020/MC

Brasília, 19 de agosto de 2020.

A Sua Excelência a Senhora

**Deputada SORAYA SANTOS**
Primeira-Secretária da Câmara dos Deputados
Brasília - DF

**Assunto: Requerimento de Informação nº 753/2020.**

Senhora Primeira Secretária,

Em atenção ao Ofício 1ªSec/RI/E/nº 1329 (SEI 5714141), que trata do Requerimento de Informação nº 753/2020, de autoria do Deputado Federal CAPITÃO ALBERTO NETO, e que solicita informações "*sobre o controle social das mídias digitais previsto no texto-base do Projeto de Lei das Fake News*", encaminho a Nota Informativa nº 134/2020/MC (SEI 5737587), do Departamento de Serviços de Telecomunicações deste Ministério, e que contempla o questionado no referido Requerimento.

Por oportuno e, conforme solicitado, informo que os demais Requerimentos de Informação encaminhados conjuntamente pelo Ofício 1ªSec/RI/E/nº 1329 (SEI 5714141), foram respondidos de forma separada.

Permanecemos à disposição para esclarecimentos adicionais, caso necessário.

Atenciosamente,

**FÁBIO FARIA**
Ministro

Documento assinado eletronicamente por **Fábio Salustino Mesquita de Faria, Ministro de Estado das Comunicações**, em 19/08/2020, às 20:38 (horário oficial de Brasília), com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **5802577** e o código CRC **35284635**.

Em caso de resposta a este Ofício, fazer referência expressa a: Ofício nº 3707/2020/MC - Processo nº 01245.000818/2020-74 - Nº SEI: 5802577

**MINISTÉRIO DAS COMUNICAÇÕES**
Secretaria de Telecomunicações
Departamento de Serviços de Telecomunicações

# NOTA INFORMATIVA Nº 134/2020/MC

| | |
|---|---|
| Nº do Processo: | **01245.000818/2020-74** |
| Documento de Referência: | **Correspondência Eletrônica nº 5724360** |
| Interessado: | **Deputado Capitão Alberto Neto.** |
| Nº de Referência: | **01245.000818/2020-74** |
| Assunto: | **Respostas ao Requerimento de Informação nº 753/2020** |

## SUMÁRIO EXECUTIVO

1. Trata-se do Requerimento de Informação nº 753/2020, formulado pelo Deputado Federal Capitão Alberto Neto, recebido pelo Ministério das Comunicações em 16 de julho de 2020, por meio do processo 01245.001681/2020-75, desmembrado no processo SEI nº 01245.000818/2020-74 e encaminhado à Secretaria de Telecomunicações.

## INFORMAÇÕES

2. Por meio do Requerimento de Informação em referência, são apresentados vários questionamentos referentes ao tema da divulgação de notícias falsa. Passa-se, a seguir, a apresentar as informações de competência deste Departamento.

**1) Existe algum planejamento no âmbito deste Ministério, para a criação ou fortalecimento de programas para valorizar e preservar direitos fundamentais como privacidade, segurança, proteção de dados, acesso à internet e liberdade de expressão, que aparentemente possam ser afetados com as regras contidas no PL 2630/2020?**

3. Quanto à primeira pergunta, cumpre recordar que o Ministério das Comunicações foi recentemente recriado, por meio da Medida Provisória nº 980, de 10 de Junho de 2020, e que no momento ainda aguarda a elaboração de decreto que estabelecerá de maneira mais detalhada quais as áreas de competências do Ministério das Comunicações, assim como os do Ministério da Ciência, Tecnologia e Inovações.

4. Assim, informamos que não existem, no presente momento, no âmbito da Secretaria de Telecomunicações, programas estruturados sobre os temas mencionados (privacidade, segurança, proteção de dados, acesso à internet e liberdade de expressão).

5. Sugere-se que a Secretaria de Comunicação Social se manifeste quanto ao tema, caso julgue pertinente.

**2) A divulgação de notícias falsas é um grande problema social que existe em qualquer forma de comunicação. Como evitar que a adição de um carimbo permanente em todas as mensagens privadas enviadas pelas pessoas através de meios digitais e o rastreamento dessas informações não ponham fim a privacidade das suas conversas particulares e nem sejam usadas contra a sociedade?**

6. A esse respeito, informa-se que, do ponto de vista técnico, a adição de um carimbo permanente em uma mensagem, como, por exemplo, uma assinatura *hash*, poderá ou não comprometer a privacidade das conversas particulares, a depender do modo e do fim para o qual este for utilizado.

7. Caso o objetivo seja o de comparar duas assinaturas para verificar se as mensagens são idênticas ou se houve alteração do conteúdo, não se vislumbra um risco imediato à privacidade dos indivíduos correspondentes. Esta técnica é utilizada em alguns contextos para moderação de conteúdo das plataformas digitais: ao identificar um conteúdo como ilícito (ex. uma imagem que contenha violência explícita) a plataforma compara o *hash* da mensagem enviada com um banco de dados que compara assinaturas de mensagens consideradas ilícitas, evitando que o conteúdo impróprio seja novamente publicado. Contudo, como pequenas variações no conteúdo (ex. adição de elementos extras a um texto, imagem ou vídeo) são capazes de alterar os *hash*, esta técnica por si só não consegue moderar conteúdo de forma eficiente (Link: https://gorwa.co.uk/publication/algomoderation/).

8. Uma segunda hipótese de aplicação de *hash* em uma mensagem é para a construção de uma cadeia de custódia de sua distribuição ao longo de um serviço de mensageria privada. Estes identificadores poderiam ser associados ao perfil do usuário que criou a mensagem, assim como de todos os usuários que vieram a compartilhar o mesmo *hash*, e essas associações seriam guardadas em registros para posterior custódia. Neste contexto, entende-se que esses registros podem eventualmente ensejar riscos à privacidade dos usuários, em razão da possibilidade de identificação dos perfis associados à criação e compartilhamento da mensagem, mediante acesso a essa tabela de registros sem observância de garantias procedimentais e do devido processo legal.

9. Nesse sentido, entende-se que deve ser examinada com cautela a previsão de regra nesse sentido constante do atual texto do PL 2630/2020.

**3) Quais os efeitos indesejados, no que se refere a liberdade de expressão, essa regulação de conteúdo online pode trazer para toda a sociedade?**

10. Entende-se que legislações sobre regulação de conteúdo online devem preferencialmente focar em regras que prevejam mais transparência para o ecossistema digital, permitindo que os usuários possam identificar mais facilmente contas inautênticas e *deep fakes* (ressalvadas as pseudonímias, humor e paródia), contas automatizadas ("bots") e contas que promovem impulsionamentos e anúncios.

11. Entende-se que a correta calibragem da regulação de conteúdo online deve buscar estabelecer um devido processo para a remoção de conteúdo infringente, com a identificação de critérios e procedimentos claros para tanto, evitando-se assim os riscos de esfriamento do debate público decorrente da insegurança jurídica associada ao risco de responsabilização por conteúdos de terceiros.

**4) Quais os riscos reais que se espera com o armazenamento de metadados de brasileiros e eventual acesso indevido ao conteúdo?**

12. Conforme é sabido, já existem, no ordenamento jurídico brasileiro, obrigações de armazenamento de metadados referentes à utilização da Internet. Nos termos do artigo 13 do Marco Civil da Internet, na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão (IP, data e hora), sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano. Além disso, nos termos do artigo 15, o provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet (IP, data e hora), sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses. O Marco Civil da Internet estabelece, ainda, critérios e procedimentos para a requisição judicial de tais registros, com o objetivo de formar conjunto probatório em processo judicial cível ou penal.

13. Entende-se que o estabelecimento de obrigações adicionais de guarda de metadados associadas ao uso da Internet deve ser avaliada à luz dos riscos de má utilização ou vazamento de tais dados, em particular quando estes se revelarem aptos a revelar a identidade dos usuários associados ao conteúdo por eles gerados ou compartilhados. Dentre os riscos associados a eventual acesso indevido a tal conteúdo, pode-se mencionar aqueles associados à formação de perfis, à perseguição

ou exposição indevida da intimidade de indivíduos; e à prática de fraudes, especialmente no caso de revelação de identificadores únicos como o RG e o CPF.

**5) Conforme a Lei Geral de Proteção de Dados, a coleta de dados deve se restringir ao necessário para a prestação do serviço, porém, de acordo com o texto, as plataformas terão que desenvolver mecanismos de detecção de fraudes no uso das contas. Será permitido que plataformas solicitem identidade ao usuário em casos de denúncias ou ações judiciais?**

14. A previsão do art. 7º do PL 2630/20 pode ir de encontro aos princípios da adequação e necessidade, estabelecidos no art. 6º, II e III, da LGPD, se cuidados necessários não forem estabelecidos. Isto porque, ao exigir a confirmação da identificação por meio de apresentação de documento de identidade, a plataforma deverá desenvolver mecanismos para assegurar que esses dados não serão utilizados para fins além dos exigidos em lei.

15. Deste modo, entende-se que, para manter harmonia com os princípios da LGPD, seria desejável que as informações sobre o documento de identidade do denunciado não sejam armazenadas por período além do necessário para conduzir a investigação da denúncia e garantir a segurança desse armazenamento, e que, ademais, é desejável restringir as hipóteses de exigência de identificação, reduzindo-se assim também o risco de mau uso ou vazamento de dados pessoais.

**6) Na visão deste Ministério, quem pagará pela adição de mecanismos para o controle de comunicação indicados pela proposta de Lei?**

16. Na forma como o PL 2630/20 se encontra estruturado, os custos da implementação dos mecanismos de moderação de conteúdo nele previstos devem ser suportados pelas empresas provedoras de aplicações da internet afetadas pelo escopo da PL, a saber, os provedores de redes sociais e de serviços de mensageria (art. 1º), excluídas as plataformas com menos de dois milhões de usuários registrados.

## CONCLUSÃO

Diante do exposto sugere-se o encaminhamento da presente nota informativa ao gabinete da Secretaria de Telecomunicações.

Brasília, 27 de julho de 2020.

Documento assinado eletronicamente por **Miriam Wimmer**, **Diretora do Departamento de Serviços de Telecomunicações**, em 30/07/2020, às 19:03 (horário oficial de Brasília), com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Thiago Moraes Guimarães**, **Analista**, em 30/07/2020, às 19:07 (horário oficial de Brasília), com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **5737587** e o código CRC **B83D8E7A**.

**Minutas e Anexos**

Não Possui.