ARTIGOS ACEITOS PARA PUBLICAÇÃO
DIREITO DIGITAL E SETOR PÚBLICO - 2020.2

ITS RIO

Pós-Graduação em Direito Digital

CEPED UERJ ITS

COMENTÁRIOS AO PL N° 2.630/2020, O "PL DAS FAKE NEWS" – CONTAS INAUTÊNTICAS, IDENTIFICAÇÃO DE USUÁRIOS E RASTREABILIDADE DE MENSAGENS

Adalthon de Paula Souza

COMENTÁRIOS AO PL N° 2.630/2020, O "PL DAS *FAKE NEWS*" – CONTAS INAUTÊNTICAS, IDENTIFICAÇÃO DE USUÁRIOS E RASTREABILIDADE DE MENSAGENS

Adalthon de Paula Souza[1]
Pós-Graduação em Direito Digital (ITS/UERJ)
Avaliação referente ao Módulo I: Direito Digital e Inovação no Setor Público
Disciplina de referência: Desinformação, Discurso de Ódio e Regulação da Internet

INTRODUÇÃO

Em 30/06/2020, o Senado Federal aprovou o texto-base do controverso Projeto de Lei nº 2.630/2020 ("PL nº 2630/2020"), que busca instituir a "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet". Embora não seja esse o seu único objetivo, o projeto de lei foi, até o momento, a iniciativa de maior êxito dentre todas as proposições legislativas que, em tese, intentam combater o fenômeno da desinformação e, justamente por isso, ficou popularmente conhecido como "PL das *Fake News*".

As instituições responsáveis pela movimentação do processo legislativo no Brasil são conhecidas por serem altamente influenciadas pelo noticiário e pelo debate público contemporâneo às proposições normativas. A aprovação de novas leis é frequentemente estimulada ou desacelerada a depender da exposição do tema na mídia[2]. E não foi diferente com o PL nº 2.630/2020.

O trâmite do projeto no Senado Federal foi estimulado não apenas pela proximidade do período eleitoral do ano de 2020, mas, sobretudo, devido ao destaque adquirido pelo tema na imprensa, principalmente após ter sido impulsionado pelo Inquérito 4.781 (frequentemente referido como "Inquérito das *Fake News*"), que apura a divulgação de notícias fraudulentas,

[1] Bacharel em direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP), atendeu ao Curso de Extensão em Proteção de Dados Pessoais e Privacidade promovido pelo Data Privacy Brasil, atualmente cursa a Pós-Graduação em Direito Digital promovida pela Universidade do Estado do Rio de Janeiro (UERJ), o Instituto de Tecnologia e Sociedade (ITS Rio) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED), e é advogado no escritório Pinheiro Neto Advogados, em São Paulo/SP.

[2] Senado Federal. **Marco Civil da Internet foi reação brasileira a denúncias de Snowden**. Disponível em: https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/propostas-senadores-querem-inteligencia-forte/marco-civil-da-internet-foi-reacao-brasileira-a-denuncias-de-snowden. Acesso em: 12 dez. 2020..

falsas comunicações de crimes, denunciações caluniosas e ameaças aos ministros do STF (Supremo Tribunal Federal)[3].

Devido à pressa para a sua aprovação, o PL das *Fake News* não foi suficientemente discutido e apreciado pelos diversos atores da sociedade que poderiam contribuir para a edição de norma legal referente a um tema tão caro ao ambiente democrático.

A desconsideração da participação da sociedade no processo legislativo representa uma ruptura em relação à elaboração de marcos legais tangentes a temas de tecnologia no Brasil, que vem de experiências bem-sucedidas como a Lei 12.965/2014 (Marco Civil da Internet) e a Lei 13.709/2018 (Lei Geral de Proteção de Dados), das quais diversos membros da sociedade civil puderam participar ativamente da construção, e que, consequentemente, hoje são reconhecidas internacionalmente como legislações modernas e referência em relação aos seus respectivos temas.

O PL nº 2.630/2020, por outro lado, tramitou e foi aprovado no Senado em apenas 48 (quarenta e oito) dias. O texto surgiu originalmente do PL 1.429/2020[4], proposto pelos deputados Felipe Rigoni (PSB/ES) e Tabata Amaral (PDT/SP) na Câmara dos Deputados, e, paralelamente, foi proposto com redação similar no Senado, pelo Senador Alessandro Vieira (Cidadania/SE), tendo sido registrado como PL 1.358/2020[5] nesta casa. O texto original já era problemático, pois nasceu com a proposta de encarregar as plataformas a identificar "*conteúdos potencialmente desinformativos*" e de contratar "*verificadores de fatos independentes*", que iriam determinar a veracidade de conteúdos, tendo os provedores "*no máximo 12 (doze) horas para a adoção das providências*".

O projeto em trâmite na Câmara chegou a ser colocado em Consulta Pública com prazo inicial de duração prevista para irrisórios 10 (dez) dias, posteriormente estendida por mais um mês. A Consulta Pública, no entanto, se mostrou inócua, uma vez que apenas 5 (cinco) dias após o seu início, o Senador Alessandro Vieira retirou o PL 1.358/2020 na mesma data em que propôs o PL 2.630/2020[6] no Senado Federal com algumas alterações. A manobra tirou o foco do projeto em trâmite na Câmara dos Deputados, que foi retirado de tramitação e arquivado mediante requerimento de seus autores.

---

[3] Supremo Tribunal Federal. **Nota do Gabinete do Ministro Alexandre de Moraes.** 2020. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444198&ori=1. Acesso em: 12 dez. 2020.

[4] Câmara dos Deputados. **Projeto de Lei 1429/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242713. Acesso em: 12 dez. 2020.

[5] Senado Federal. **Projeto de Lei 1358/2020.** Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141372. Acesso em: 12 dez. 2020.

[6] Senado Federal. **Projeto de Lei 2630/2020**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 12 dez. 2020..

No Senado, o PL nº 2.630/2020 passou a tramitar rapidamente e o texto original foi sucessivamente desidratado. O projeto passou a ser alvo de críticas de diversos atores da sociedade e especialistas, como a Human Rights Watch, a ONU, Anistia Internacional, a Artigo 19, o Instituto de Tecnologia e Sociedade (ITS), a Coalizão Direitos na Rede e diversos outros órgãos. O PL das *Fake News* também foi objeto de diversos requerimentos de retirada da pauta e de impressionantes 152 (cento e cinquenta e duas) propostas de emendas. Ainda assim, na noite de 30/06/2020, o PL foi aprovado por 44 votos a 32 no Senado.

Independentemente se o PL se tornará lei ou não, se será sancionado com o texto da forma como aprovado no Senado ou se sofrerá alterações após o trâmite integral, que ainda conta com a análise da Câmara dos Deputados, é decepcionante identificar como o processo legislativo em relação a um tema tão relevante tenha sido conduzido de forma tão equivocada que, não por outra razão, produziu um texto deficiente em diversos aspectos técnicos, conceituais e práticos, conforme pretende demonstrar este artigo.

A desinformação é, de fato, um grave problema e que se mostrou um grande risco para sociedades, se tornando especialmente danosa naquelas que buscam calcar-se em preceitos democráticos. No entanto, qualquer tentativa de buscar soluções para a questão não pode ignorar o amplo debate e passar por cima de avanços históricos em relação a liberdades individuais, sob o risco de, além de não dirimir os seus efeitos nocivos, violar direitos e garantias já conquistados.

Embora o projeto aprovado no Senado Federal tenha diversos pontos problemáticos, este trabalho foca a sua análise nos dispositivos que tratam especificamente de contas inautênticas, identificação de usuários e rastreabilidade de mensagens (arts. 6º, 7º, 8º e 10), tendo como objetivo demonstrar que, se for sancionado com redação igual ou com o texto semelhante àquele remetido para a análise da Câmara dos Deputados, o PL 2630/2020 representará verdadeiro retrocesso em aspectos como proteção de dados, segurança, privacidade e liberdade de expressão.

CONTAS INAUTÊNTICAS E IDENTIFICAÇÃO DE USUÁRIOS

Em seu art. 5º, II, o PL 2360/2020 define como conta inautêntica a "*conta criada ou usada com o propósito de assumir ou simular identidade de terceiros para enganar o público*". Em seguida, dque estão "*ressalvados o direito ao uso de nome social e à pseudonímia nos termos desta Lei, bem como o explícito ânimo humorístico ou de paródia*". Adiante, em seu art. 6º, é estabelecido que os provedores de redes sociais e de serviços de

mensageria privada deverão adotar medidas para "*vedar o funcionamento de contas inautênticas*".

A redação pouco precisa dos dispositivos dá margem ao surgimento de diversas dúvidas quanto ao contorno legal das obrigações apresentadas, revelando que, ao tentar conceituar diretrizes para o que é (e o que não é) legítimo na internet, o legislador se coloca em terreno pantanoso, tentando instituir definições que não se sustentam.

Na prática, estará legalmente transferida ao provedor de aplicação a obrigação de interpretar se uma conta foi criada para simular a identidade de terceiros, ou se um determinado usuário está buscando "enganar o público". A partir da leitura do artigo, também é possível discernir que, a partir da vigência do dispositivo, a plataforma precisará criar um método para identificar para qual propósito uma conta foi criada, dúvida que também é transferida ao usuário, que terá que se perguntar o que a plataforma espera que seja a sua intenção com a criação daquela conta.

O texto ainda dita que estarão resguardadas da possibilidade de remoção as contas com "*explícito ânimo humorístico ou de paródia*". Isso significa que os usuários que, na mesma situação, optarem por utilizar o humor de forma implícita poderão não ter a mesma sorte?

Dada a natureza subjetiva que é intrínseca às avaliações que passam a ser outorgadas aos provedores, as quais englobam até a necessidade de interpretar o real intuito de um indivíduo ao criar uma conta em uma plataforma de rede social, é evidente que este tipo de decisão não deveria estar a cargo dos provedores e sim do poder judiciário.

Ainda no seu ânimo de identificação de práticas "não legítimas", o PL estabelece no art. 7º que os provedores terão a liberalidade de pedir aos usuários que "*confirmem sua identificação, inclusive por meio da apresentação de documento de identidade válido*", nas hipóteses "*de indícios de contas automatizadas não identificadas como tal", "indícios de contas inautênticas*", "*casos de ordem judicial*", ou quando a plataforma receber denúncia em que seja relatado que o usuário estaria violando a referida Lei.

O dispositivo cria uma clara hipótese de violação da privacidade dos usuários, relegando às plataformas a arbitrariedade de requisitar documento de identidade do indivíduo, bastando que a empresa justifique o pedido em critérios facilmente manipuláveis, tal como a alegação de que uma conta estaria apresentando indícios de comportamento inautêntico.

Não bastasse, o texto do art. 7º do PL 2360/2020 ainda contraria os princípios da minimização e necessidade a serem observados na atividade de tratamento de dados pessoais.

Conferir o documento de identidade do indivíduo não se mostra necessário para o êxito da finalidade de identificação de usuário de aplicação da internet.

Com o advento do Marco Civil da Internet, já está consolidada a obrigação legal dos provedores de aplicação de armazenar os registros de acesso a aplicações de internet (conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP), sob sigilo, pelo prazo de 6 (seis) meses (art. 15). Com isso, a parte interessada está apta a, por meio de ordem judicial, requerer que a plataforma responsável forneça tais registros. Em seguida, em posse de tais informações e munido de determinação judicial[7] para a quebra de sigilo, a parte se volta aos provedores de conexão que, também pelo Marco Civil, estão obrigado a fornecer os dados pessoais disponíveis acerca do(s) usuário(s) responsável(is) pela criação da conta questionada (art. 22).

Isso significa que, existindo fundados indícios da ocorrência de ato ilícito por qualquer usuário na internet, a parte interessada já possui meios legais para identificação do indivíduo responsável, de modo que a criação de dispositivo legal que oportuniza plataformas a requisitar apresentação de documento de identidade para justificar a necessidade de identificação precisa de um usuário, representa medida desnecessária e um tanto quanto antiquada.

Nesse sentido, os artigos 6º e 7º do PL 2360/2020 colidem com o entendimento consolidado das Cortes Superiores brasileiras quanto a identificação de usuários na internet, quando provocadas a decidirem sobre o anonimato nesse ambiente.

No Brasil, a "vedação ao anonimato" foi concebida no sistema de direito constitucional positivo com a finalidade de propiciar a identificação dos autores de eventuais manifestações ilícitas para fins de responsabilização. Não significa, no entanto, a necessidade de identificação completa e imediata da autoria no exato momento de sua manifestação, mas sim a possibilidade de que, caso seja identificada eventual pratica de ato ilícito, o(a) autor(a) possa posteriormente ser responsabilizado.

Este é o entendimento referendado pelo Supremo Tribunal Federal, conforme ilustra decisão do então Ministro CELSO DE MELLO:

> "(...) O veto constitucional ao anonimato, como se sabe, busca impedir a consumação de abusos no exercício da liberdade de manifestação do pensamento, pois, ao exigir-se a identificação de quem se vale dessa extraordinária prerrogativa político-jurídica, essencial à própria configuração do Estado democrático de direito,

[7] O Marco Civil da Internet autoriza a requisição de dados cadastrais, sem ordem judicial, por autoridades administrativas com competência legal para tanto (art. 10, §3º). As autoridades podem ter acesso a dados cadastrais "*que informem qualificação pessoal, filiação e endereço*".

> visa-se, em última análise, a possibilitar que eventuais excessos, derivados da prática do direito à livre expressão, sejam tornados passíveis de responsabilização, ***'a posteriori'*, tanto na esfera civil, quanto no âmbito penal**.
>
> Essa cláusula de vedação - que jamais deverá ser interpretada como forma de nulificação das liberdades do pensamento - surgiu, no sistema de direito constitucional positivo brasileiro, com a primeira Constituição republicana, promulgada em 1891 (art. 72, § 12), que objetivava, ao não permitir o anonimato, inibir os abusos cometidos no exercício concreto da liberdade de manifestação do pensamento, viabilizando, desse modo, a adoção de medidas de responsabilização daqueles que, no contexto da publicação de livros, jornais ou panfletos, viessem a ofender o patrimônio moral das pessoas agravadas pelos excessos praticados, consoante assinalado por eminentes intérpretes daquele Estatuto Fundamental (JOÃO BARBALHO, "Constituição Federal Brasileira - Comentários", p. 423, 2ª ed., 1924, F. Briguiet; CARLOS MAXIMILIANO, "Comentários à Constituição Brasileira", p. 713, item n. 440, 1918, Jacinto Ribeiro dos Santos Editor).
>
> Vê-se, portanto, tal como observa DARCY ARRUDA MIRANDA ("Comentários à Lei de Imprensa", p. 128, item n. 79, 3ª ed., 1995, RT), que a proibição do anonimato tem um só propósito, qual seja, o de permitir que o autor do escrito ou da publicação possa expor-se às conseqüências jurídicas derivadas de seu comportamento abusivo (...)" (BRASIL, STF, DJ 16/10/2002, MS 24369 MC/DF – Rel. Min. Celso de Mello)

O Superior Tribunal de Justiça, por sua vez, em diversas oportunidades apreciou a questão da vedação ao anonimato na internet, firmando o entendimento de que os provedores de serviços de Internet que possibilitam aos usuários que expressem livremente sua opinião devem propiciar os meios para que estes sejam identificados em caso de violação de direitos de terceiros, em especial através do registro dos respectivos endereços IP (Internet Protocol). A Corte tem se manifestado no sentido de que a preservação de dados e registros de acesso pelos respectivos provedores são medidas satisfatórias à identificação do usuário e, portanto, para o atendimento da "vedação ao anonimato" prevista no artigo 5º, inciso IV, da Constituição Federal[8]:

> CIVIL E PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. ORKUT. REMOÇÃO DE CONTEÚDO REPUTADO OFENSIVO. POSSIBILIDADE. MONITORAMENTO PRÉVIO DE PUBLICAÇÕES NA REDE SOCIAL. FORNECIMENTO DE DADOS PESSOAIS. IMPOSSIBILIDADE. JULGAMENTO EXTRA PETITA. PRESENÇA. ASTREINTES. OBRIGAÇÃO IMPOSSÍVEL. AFASTAMENTO. - (...) - Esta Corte fixou entendimento de que "(i) não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários; (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos; (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso". Precedentes. - **Ainda que**

[8] No mesmo sentido, v.: BRASIL, STJ, DJe 23/05/2014, AgRg no REsp 1396963/RS, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 28/05/2014, AgRg no REsp 1285756/MG, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 26/05/2014, AgRg no REsp 1395803/RJ, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 22/05/2014, AgRg no REsp 1395768/RJ, Rel. Min. Raul Araújo.

> **não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de internet.** - (...). - Há violação ao art. 461 do CPC/73 a imposição de multa cominatória para obrigação de fazer que se afigura impossível de ser cumprida, o que enseja o afastamento das astreintes. - Recurso especial conhecido e provido. (BRASIL, STJ, DJe 14/02/2017, REsp 1.342.640/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA – sem ênfase no original)
>
> .....
>
> A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato. **O fornecimento do registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na internet constitui meio satisfatório de identificação de usuários**. (BRASIL, STJ, DJe 18/06/2014, AgRg no REsp 1402104/RJ, Rel. Min. Raul Araújo – sem ênfase no original)

Tudo isso mostra que o texto do PL 2360/2020 aprovado no Senado Federal, além de impor às plataformas a obrigação de análise subjetiva de comportamento de usuário, ainda regride em questões já superadas pela legislação e jurisprudência, representando um desserviço para a privacidade dos usuários e para o avanço tecnológico.

RASTREABILIDADE DE MENSAGENS

Talvez a inovação mais polêmica trazida pelo PL 2360/2020, o art. 10º do projeto estabelece que os serviços de mensageria privada[9] (como os aplicativos WhatsApp e Telegram) deverão promover o armazenamento dos "*registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses*". Ainda que próprio texto esclareça adiante que este armazenamento não engloba o conteúdo das mensagens, isso não significa que tal medida não represente afronta a privacidade, já que possibilita o rastreamento da comunicação privada dos usuários.

Ao definir os critérios para a guarda dos registros, o projeto define como encaminhamento em massa "*o envio de uma mesma mensagem por mais de 5 (cinco)*

[9] PL 2360/2020: Art. 5º. (...)
IX — serviço de mensageria privada: aplicação de internet que viabiliza o envio de mensagens para destinatários certos e determinados, inclusive protegidas por criptografia de ponta a ponta, a fim de que somente remetente e destinatário da mensagem tenham acesso ao seu conteúdo, excluídas aquelas prioritariamente destinadas a uso corporativo e os serviços de correio eletrônico.

usuários, em intervalo de até 15 (quinze) dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários". Adiante, no § 4º do mesmo dispositivo, é esclarecido que a retenção dos registros se aplica somente às mensagens que alcançarem no mínimo 1.000 (mil) usuários.

Ocorre que, embora o legislador busque fazer uma ressalva quanto às mensagens que atinjam menos que 1.000 (mil) usuários, na prática, os metadados de todas as mensagens enviadas a "*grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários"*, por quaisquer usuários, deverão ser armazenadas pelos provedores ao menos por 15 (quinze) dias.

Nesse sentido, suponha o exemplo em que uma mensagem é enviada hoje somente para um grupo e, apenas daqui 15 (quinze) dias ela se torne viral, extrapolando o número de usuários estabelecido no PL. Se o provedor não tiver armazenado os registros da mensagem enviada há quinze dias, estará descumprindo a Lei e deverá ser submetido às suas sanções (considerando a hipótese em que o texto do PL 2360/2020 teria sido sancionado na forma como está).

Ainda nesse ponto, as plataformas consequentemente também terão que adotar medidas para, constante e ininterruptamente, analisar e comparar o conteúdo de todas as mensagens enviadas a grupos de usuários por meio de sua aplicação, de modo a certificar se aquela mensagem é a mesmo enviada anteriormente enviada por outro usuário, configurando assim possível encaminhamento em massa, analisando em seguida se foi atingido o quantitativo de 1.000 (mil) encaminhamentos por 5 (cinco) usuários.

Vale destacar que não há nenhum estudo que atualmente demonstre que tal medida é tecnicamente viável de ser implementado pelas plataformas, inclusive porque não há notícia de exigência similar em qualquer lugar do mundo. Há uma profunda incerteza inerente à identificação inequívoca de conteúdo em tais plataformas, na medida em que qualquer mínima alteração em um conteúdo eletrônico (mesmo que se consubstancie em salvar o conteúdo e realizar o upload em seguida) é suficiente para criar dois arquivos tecnicamente distintos, sendo controversa a existência de qualquer registro que possa ser considerado como a "impressão digital" de um conteúdo. Tal fato, inclusive, foi reconhecido pelo Superior Tribunal de Justiça, ao analisar caso em que se discutia a adulteração de arquivos digitais:

> "Conforme as descrições metodológicas dos laudos de exame de dispositivo computacional juntados aos autos, por ocasião de cada perícia nas mídias, é calculado, em relação à própria mídia e a cada arquivo extraído do material examinado e reproduzido na mídia que acompanha o laudo, o algoritmo SHA-512.

> Tal algoritmo, denominado hash (ou resumo), tem a propriedade de ser alterado em caso de qualquer alteração do arquivo ao qual é correspondente. Com isso, é possível verificar se a mídia ou o arquivo reproduzido foi alterado. A mesma mídia ou arquivo deve produzir sempre o mesmo algoritmo.
>
> A Informação Técnica 230/2010 (fls. 5136-7) esclarece que, por ocasião da elaboração da primeira perícia (Laudo 823/07), foi extraído o código hash da própria mídia. Tal código constou do DVD que acompanhou o laudo pericial. Posteriormente, foram elaboradas novas análises periciais da mesma mídia (Laudos 1728/09, 3028/10 e 54/10). Entretanto, o código hash calculado mudou.
>
> Ou seja, houve alteração de arquivos na mídia apreendida. Essa alteração ocorreu após a apreensão, quando a mídia estava na guarda policial, pericial ou judicial, aparentemente sem qualquer concurso das defesas. Não há dúvida de que a alteração é indesejável. A questão que se põe é se a conseqüência a ser extraída é a invalidade da prova". (BRASIL, STJ, DJe 13/09/2013, HC 213.448/RS, Rel. Ministro SEBASTIÃO REIS JÚNIOR, Rel. p/ Acórdão Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA)

Independentemente do que se possa concluir sobre a possibilidade da comparação entre arquivos eletrônicos, a discussão por si só já demonstra que as disposições do PL 2360/2020 potencialmente inviabilizam o funcionamento no país dos serviços de mensageria privada que adotem a criptografia ponta-a-ponta, na qual os provedores ou quaisquer terceiros não estão aptos a ter acesso às mensagens e arquivos trocados entre os usuários.

É válido que se estabeleça o entendimento de que, se o provedor precisa certificar se uma mensagem específica ultrapassou um certo limite pré-estabelecido de envios por usuários, a ponto de ser classificada como objeto de um "encaminhamento em massa", é razoável inferir que a plataforma precisa ter acesso ao conteúdo da mensagem para tanto.

Sendo assim, na hipótese em que tal necessidade seja confirmada, ainda que o art. 10º disponha que a obrigação imposta não abarca a guarda do conteúdo das mensagens, a consequência lógica seria que, ao menos em princípio, o conteúdo terá sim que ser analisado.

Mesmo que assim não fosse, é preciso afastar a percepção de que o referido dispositivo não promove a violação da privacidade dos usuários, apenas porque não determina o armazenamento dos conteúdos enviados por meio dos serviços de mensageria privada. Mesmo que não obrigue a guarda das mensagens em si, o projeto determina o armazenamento e possível disponibilização dos metadados destas, o que significa o acesso a informações tão relevantes quanto a data e horário de quando uma mensagem foi enviada, para quais grupos foram encaminhadas e quantas pessoas estão nestes grupos (art. 10º, § 2º). Isso sem contar a infinidade de inferições que serão possíveis às próprias empresas com base em tais informações, coletadas e geridas por instituições privadas que, por óbvio, atendem aos seus próprios interesses econômicos, mas que estarão preservadas pela justificativa de cumprimento de obrigação legal imposta pelo Estado.

É evidente, portanto, que o art. 10º do PL 2360/2020 significa verdadeiramente o monitoramento preventivo da conduta de usuários de serviços de mensageria privada, a partir da rastreabilidade e retenção dos registros de suas atividades. Na forma como aprovado no Senado Federal, o texto fere os princípios da adequação, da necessidade e da minimização no tratamento de dados pessoais, além de violar a presunção de inocência e o princípio da reserva legal.

CONCLUSÃO

Embora este artigo tenha se limitado a análise das proposições relacionadas a identificação de usuários, contas inautênticas e rastreabilidade de mensagens, o PL 2360/2020, mesmo que possua apenas 36 (trinta e seis) artigos, também apresenta outras inovações bastante prejudiciais em diversos aspectos, mas principalmente para a privacidade e à liberdade de expressão e que poderiam render inúmeros trabalhos acadêmicos.

Dentre os inúmeros problemas identificados no texto, podem ser listados a redação, que por diversas vezes se mostra imprecisa quanto ao limite das obrigações e pouco claras quanto a própria estruturação do texto; a consequência prática das disposições que basicamente impõe às plataformas a obrigação de moderação de conteúdo; a alteração do modelo de responsabilidade dos provedores na forma como hoje é previsto no Marco Civil da Internet; a regulação de conteúdo patrocinados, que responsabiliza diretamente o meio de distribuição pela veiculação de publicidade abusiva e/ou ilegal, e não ao anunciante[10]; a criação do Conselho de Transparência e Responsabilidade na Internet, com atribuições semelhantes da Autoridade Nacional de Proteção de Dados, e já atualmente previstas no artigo 55-A e seguintes da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados); as excessivas, desproporcionais e por vezes desnecessárias diretrizes impostas aos provedores de aplicação, oferecendo riscos de inviabilizar a operação destas empresas no Brasil ou de alguns de seus serviços, dentre outros.

Considerando que a questão é muito mais extensa do que poderia ser abarcada por este trabalho, o artigo buscou ao menos tecer alguns comentários que contextualizam o cenário e a forma como o projeto de lei foi conduzido, o que explica bastante de suas deficiências. Além

[10] INTERVOZES. **Contribuições ao debate sobre regulação de publicidade e remuneração por direitos autorais no âmbito das discussões do PL 2630/2020**. 2020. Disponível em: https://intervozes.org.br/wp-content/uploads/2020/09/Contribuicoes-do-Intervozes-ao-debate-acerca-da-publicidade-e-direitos-autorais-no-PL-2630_2020_vfinal.docx.pdf. Acesso em: 12 dez. 2020.

disso, o trabalho também apresentou as razões pelas quais o texto aprovado no Senado Federal, se sancionado, não seria apenas inócuo para enfrentar a questão da desinformação, como também um risco para a privacidade dos usuários e para o caráter democrático que se espera da internet.

Ao analisar o projeto, espera-se que a Câmara dos Deputados promova uma discussão mais ampla na qual todos os indivíduos, órgãos e entidades da sociedade civil sejam convidados a colaborar. Dessa forma, caso haja o entendimento conjunto sobre uma proposta normativa realmente útil para o enfrentamento da questão, poderemos então construir uma legislação muito mais adequada e eficiente, sem que para isso tenhamos que abrir mão do avanço tecnológico e do respeito aos direitos e garantias já adquiridos e consolidados.

REFERÊNCIAS

ANISTIA INTERNACIONAL. **Projeto de lei sobre desinformação ameaça a liberdade de expressão e a privacidade online**. Disponível em: https://anistia.org.br/informe/projeto-de-lei-sobre-desinformacao-ameaca-a-liberdade-de-expressao-e-a-privacidade-online/. Acesso em: 13 dez. 2020.

ARTIGO 19. **Nota Técnica - Projeto de Lei nº 2.630/2020:** "PL das Fake News": contribuições ao debate legislativo sob os parâmetros da liberdade de expressão. Artigo 19, São Paulo, 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Diário Oficial da União, 24 abr. 2014. Seção 1, p. 1.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). 157. ed. Brasília, DF: Diário Oficial da União, 18 ago. 2018. Seção 1, p. 59.

BRASIL, STF, DJ 16/10/2002, MS 24369 MC/DF – Rel. Min. Celso de Mello

BRASIL, STJ, DJe 13/09/2013, HC 213.448/RS, Rel. Ministro SEBASTIÃO REIS JÚNIOR, Rel. p/ Acórdão Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA

BRASIL, STJ, DJe 14/02/2017, REsp 1.342.640/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA

BRASIL, STJ, DJe 18/06/2014, AgRg no REsp 1402104/RJ, Rel. Min. Raul Araújo

BRITO CRUZ, Francisco; FRAGOSO, Nathalie; MASSARO, Heloisa; **Estratégias de proteção do debate democrático na internet**. InternetLab, São Paulo, 2020.

Câmara dos Deputados. **Projeto de Lei 1429/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242713. Acesso em: 12 dez. 2020.

CANABARRO, Diego R.; RENÁ, Paulo. Veja dez razões para rejeitar artigo 10 do projeto sobre fake news, que rastreia mensagens: dispositivo é ineficaz ao que se propõe e soluciona problemas que não existem ao preço de criar vários novos obstáculos. **Folha de S. Paulo.** São Paulo, 5 ago. 2020. Poder, p. 8-8.

CHADE, Jamil. **Em carta, relator da ONU diz que PL das Fake News ameaça privacidade**. 2020. Disponível em: https://noticias.uol.com.br/colunas/jamil-chade/2020/07/14/em-carta-relator-da-onu-diz-que-pl-das-fake-news-ameaca-privacidade.htm. Acesso em: 13 dez. 2020.

COALIZÃO DIREITOS NA REDE. **Combater desinformação assegurando liberdade de expressão e privacidade**. 2020. Disponível em: https://intervozes.org.br/wp-content/uploads/2020/06/CDR-Posicionamento-PL2630-29MAIO2020.pdf. Acesso em: 12 dez. 2020..

Comissão de Juristas da Câmara dos Deputados responsável pela elaboração de Anteprojeto de Lei sobre proteção de dados pessoais em segurança pública e investigações criminais. **Ofício à Secretaria-Geral da Mesa da Câmara dos Deputados**: Ref. Art. 10 do PL 2.630/2020. Brasília, 9 set. 2020.

CUNHA E MELO, Mariana. **Anonimato, Proteção de Dados e Devido Processo Legal:** Por que e como Conter uma das Maiores Ameaças ao Direito à Privacidade no Brasil. In:

BRANCO, Sérgio. DE TEFFÉ, Chiara (Org.). **Privacidade em perspectivas.** Rio de Janeiro : Lumen Juris, 2018.

DA SILVA, Nayane Maria Rodrigues. **Fake News:** a revitalização do jornal e os efeitos Fact-Checking e CrossCheck no noticiário digital. Temática, v. 13, n. 8, ago/2017.

DE SOUZA, Carlos Affonso Pereira; PADRÃO, Vinicius. **Quem lê tanta notícia falsa?** Entendendo o combate contra as "fake news. ITS Rio, 2020.

DELMAZO, Caroline e VALENTE, Jonas C.L. **Fake news nas redes sociais online:** propagação e reações à desinformação em busca de cliques. Media & Jornalismo [online]. 2018, vol.18, n.32 [citado 2019-07-22], pp.155-169.

GALLO, Fernando. **O PL das Fake News e a Internet que Queremos**: projeto, da forma que está, contribui para a desinformação. 2020. Revista Piauí. Disponível em: https://piaui.folha.uol.com.br/o-pl-das-fake-news-e-a-internet-que-queremos/. Acesso em: 12 dez. 2020.

HUMAN RIGHTS WATCH. **Brasil: Rejeite o projeto de lei sobre "fake news"**: projeto viola a liberdade de expressão e de associação e o direito à privacidade. Projeto viola a liberdade de expressão e de associação e o direito à privacidade. 2020. Disponível em: https://www.hrw.org/pt/news/2020/06/24/375579. Acesso em: 13 dez. 2020.

INTERNETLAB. **Rastrear o viral? Riscos à privacidade no projeto de lei "de combate às fake news"**. InternetLab, São Paulo, 2020.

INTERVOZES. **Contribuições ao debate sobre regulação de publicidade e remuneração por direitos autorais no âmbito das discussões do PL 2630/2020**. 2020. Disponível em: https://intervozes.org.br/wp-content/uploads/2020/09/Contribuicoes-do-Intervozes-ao-debate-acerca-da-publicidade-e-direitos-autorais-no-PL-2630_2020_vfinal.docx.pdf. Acesso em: 12 dez. 2020.

ITS. **Nota Técnica sobre os Projetos de Lei n° 2927/2020 (Câmara) e nº 2630/2020 (Senado)**. ITS, Rio de Janeiro, 2020.

LARA, Matheus. **Os argumentos pró e contra os pontos mais polêmicos do PL das fake news**. 2020. O Estado de S.Paulo.. Disponível em: https://politica.estadao.com.br/noticias/geral,os-argumentos-pro-e-contra-os-pontos-mais-polemicos-do-pl-das-fake-news,70003351137. Acesso em: 12 dez. 2020.

Ministério Público Federal. Procuradoria Geral da República. 2ª Câmara de Coordenação e Revisão (Criminal). **Nota Técnica 2CCR nº 04/2020 - Sugestões ao Projeto de Lei 2630/2020** - fake news. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas/notas-tecnicas-1/2020/nt_4.pdf. Acesso em: 12 dez. 2020.

OLHAR DIGITAL. **PL das fake news: artigo 10 viola direitos humanos**. 2020. Disponível em: https://olhardigital.com.br/2020/08/08/noticias/pl-das-fake-news-artigo-10-viola-direitos-humanos/. Acesso em: 13 dez. 2020.

Senado Federal. **Marco Civil da Internet foi reação brasileira a denúncias de Snowden**. Disponível em: https://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/propostas-senadores-querem-inteligencia-forte/marco-civil-da-internet-foi-reacao-brasileira-a-denuncias-de-snowden. Acesso em: 12 dez. 2020.

Senado Federal. **Projeto de Lei 1358/2020.** Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141372. Acesso em: 12 dez. 2020..

Senado Federal. **Projeto de Lei 2630/2020**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 12 dez. 2020..

Supremo Tribunal Federal. **Nota do Gabinete do Ministro Alexandre de Moraes.** 2020. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444198&ori=1. Acesso em: 12 dez. 2020.

TILT - UOL (São Paulo). **PL das fake news: aprovado no Senado, entenda o que pode mudar**. 2020. Por Bruna Souza Cruz. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/30/com-44-votos-senado-aprova-pl-das-fake-news.htm. Acesso em: 12 dez. 2020.

TILT - UOL (São Paulo). **PL das fake news: senadores festejam; ativistas e empresas criticam.** 2020. Por Bruna Souza Cruz. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/07/01/pl-das-fake-news-veja-a-repercussao-da-votacao-do-senado.htm. Acesso em: 12 dez. 2020.