

19/08/2020


ENC: camara-e.net | PL 2630/2020 (PL d... - Jacqueline de Souza Alves da Silva

ENC: camara-e.net | PL 2630/2020 (PL das Fake News) - Nota Técnica com Sugestões de Alteração

Presidência

ter 18/08/2020 20:10

Para: Jacqueline de Souza Alves da Silva <JACQUES@senado.leg.br>;

 1 anexo

PL Fake News - camara-e.net_Manifestação - PL 2630-2020_VF.pdf;

De: Agenda do Presidente do Senado Federal

Enviada em: terça-feira, 18 de agosto de 2020 20:01

Para: Presidência <presidente@senado.leg.br>

Assunto: ENC: camara-e.net | PL 2630/2020 (PL das Fake News) - Nota Técnica com Sugestões de Alteração

De: Arthur Teodoro [<mailto:arthur.teodoro@camara-e.net>]

Enviada em: terça-feira, 18 de agosto de 2020 17:17

Para: Leonardo Palhares | camara-e.net <presidencia@camara-e.net>

Cc: Felipe Brandão <felipe.brandao@camara-e.net>

Assunto: camara-e.net | PL 2630/2020 (PL das Fake News) - Nota Técnica com Sugestões de Alteração

Excentíssimo Sr. Deputado, boa tarde!

Em nome da **Câmara Brasileira de Comércio Eletrônico (camara-e.net)**, encaminho para análise uma **nota técnica preparada pela associação para o PL 2630/2020 (PL das Fake News)**. A camara-e.net é a associação com maior representatividade na Economia Digital brasileira, portanto, nosso posicionamento engloba os mais diversos setores econômicos, e reflete os anseios de grande parte da iniciativa privada que será frontalmente impactada pelo PL.

Compreende-se a ansiedade em torno de tema tão complexo e premente, bem como a intenção louvável de buscar dar-lhe uma resposta legislativa. Entretanto, verificamos que, os potenciais efeitos do substitutivo apresentado não demonstram eficácia no combate à desinformação, podendo ainda colocar o Brasil no mapa da insegurança jurídica e dos prejuízos à liberdade de expressão e à economia e à livre iniciativa.

Neste sentido, recomenda-se que o PL 2630/2020 seja repensado, a partir dos debates com os mais diversos setores. Para isso, encaminhamos em anexo uma nota técnica muito bem detalhada, sugerindo alterações ao texto do PL, bem como detalhando as razões das sugestões.

Permanecemos à disposição para conversar sobre o tema, bem como renovamos os votos de elevada estima e consideração.

Att.,

Arthur Teodoro

Jurídico

arthur.teodoro@camara-e.net

Avenida Angélica, 2503 - 5º andar –



19/08/2020

ENC: camara-e.net | PL 2630/2020 (PL d... - Jacqueline de Souza Alves da Silva

Conj. 56

+55 (11) 3237 1102

São Paulo, 12 de agosto de 2020.

À
CÂMARA DOS DEPUTADOS
Praça dos Três Poderes – Palácio do Congresso
CEP 70.160-900
Brasília | DF

**REF.: MANIFESTAÇÃO DA CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO (CAMARA-E.NET)
SOBRE O PL 2360/2020.**

Excelentíssimos Senhores,

A **CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO** (“camara-e.net”), associação sem fins lucrativos, com sede na Cidade de São Paulo, Estado de São Paulo, à Avenida Angélica, 2503 – Consolação – CEP 01227-200, inscrita no CNPJ/MF sob o nº 04.481.317/00001-48 vem, por meio deste documento, expor o posicionamento da entidade e de seus associados sobre o Projeto de Lei nº 2360/2020.

I – APRESENTAÇÃO DA CAMARA-E.NET

Fundada em 2001, a camara-e.net fez de sua missão e objetivo promover o desenvolvimento da Economia Digital de maneira sustentável. É, atualmente, a principal entidade multisetorial da América Latina e entidade brasileira de maior representatividade da Economia Digital.

O seu papel tem sido fundamental a formulação de políticas públicas alinhadas aos anseios da sociedade moderna e, especialmente, para o aprimoramento de marcos regulatórios setoriais que dão suporte legal às medidas de incentivo necessárias ao desenvolvimento de nosso país.

Além disso, compõem seu quadro de associados os mais relevantes nomes de diversos setores da Economia Digital, incluindo provedores de conteúdo e de serviços na internet, empresas de meios de pagamento e certificação digital, mídias sociais, bancos, lojas, entre outros.

II – DO PROJETO DE LEI Nº 2630/2020 (“PL DAS FAKE NEWS”)

Apresentado pelo Exmo. Senador Alessandro Vieira (Cidadania/SE) em 15 de maio de 2020, o Projeto de Lei nº 2630/2020 (“PL 2630/20”) foi aprovado com texto substitutivo no Senado em 30 de junho de 2020, e pretende instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, impondo regras e obrigações sobre moderação de conteúdo, combate à desinformação e publicidade online a provedores de aplicação, além de sanções pelo seu descumprimento.

Trata-se evidentemente de um projeto bem intencionado que, no contexto volátil e sensível da pandemia global do novo coronavírus, busca endereçar preocupações legítimas da sociedade, como o combate às “fake news”, por exemplo. A camara-e.net compreende a relevância do tema e a necessidade de se tomar medidas para combater a disseminação de notícias falsas, especialmente na era digital, no entanto, a construção de soluções deve necessariamente passar por um processo maduro de discussão.

Além de desconsiderar os efeitos negativos à população, à economia brasileira e aos provedores de aplicação, o PL 2630/20 (i) contraria princípios constitucionais, representando uma ameaça à liberdade de expressão e à privacidade; (ii) subverte o regime de responsabilidade firmado pelo Marco Civil da Internet (“MCI”); (iii) impacta negativamente o acesso à informação, a privacidade, a proteção de dados pessoais e a segurança da população; e (iv) cria barreiras à liberdade econômica e à inovação.

Esses riscos e vícios legais se agravaram notadamente pela tramitação acelerada e a consequente ausência de um debate amplo e democrático à época de aprovação do texto no Senado. Dessa forma, com o objetivo de auxiliar na exposição objetiva das preocupações do setor, detalhamos na tabela anexa a seguir os trechos mais sensíveis ao setor da economia digital, sugerindo alterações imprescindíveis para a construção de um regramento robusto e adequado, tanto para o setor privado quanto para a sociedade.

Por fim, compreende-se a ansiedade em torno de tema tão complexo e premente, bem como a intenção louvável de buscar dar-lhe uma resposta legislativa. Ocorre que, os potenciais efeitos do substitutivo apresentado não demonstram eficácia no combate à desinformação, podendo ainda colocar o Brasil no mapa da insegurança jurídica e dos prejuízos à liberdade de expressão e à economia e à livre iniciativa.

Neste sentido, recomenda-se que o PL 2630/2020 seja repensado, a partir dos debates com os mais diversos setores. Nesta perspectiva, encaminhamos no Anexo a seguir as sugestões da camara-e.net a respeito do presente Projeto de Lei.

Sendo o que nos cumpria para o momento, renovamos nossos votos de elevada estima e consideração.

Cordialmente,

CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO

Leonardo A. F. Palhares

Presidente

ANEXO I – ANÁLISE DOS TRECHOS MAIS CRÍTICOS DA REDAÇÃO FINAL DO PROJETO DE LEI Nº 2630/2020 APROVADO NO SENADO FEDERAL

	REDAÇÃO ATUAL	SUGESTÃO DE ALTERAÇÃO NA REDAÇÃO	JUSTIFICATIVA DA ALTERAÇÃO
ESCOPO DE APLICAÇÃO	Art. 1º Esta Lei, denominada Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, estabelece normas, diretrizes e mecanismos de transparência para provedores de redes sociais e de serviços de mensageria privada a fim de garantir segurança e ampla liberdade de expressão, comunicação e manifestação do pensamento.	Art. 1º Esta Lei, denominada Lei Brasileira de Liberdade, Responsabilidade e Transparência da Internet no Brasil , estabelece normas, diretrizes e mecanismos de transparência para provedores de redes sociais e de serviços de mensageria privada a fim de garantir segurança e ampla liberdade de expressão, comunicação e manifestação do pensamento.	Entendemos que a inserção do trecho “no Brasil” delimita de maneira objetiva o escopo de aplicação da Lei.
	§ 1º Esta Lei não se aplica aos provedores de redes sociais e de serviços de mensageria privada que ofertem serviços ao público brasileiro com menos de 2.000.000 (dois milhões) de usuários registrados, para os quais as disposições desta Lei servirão de parâmetro para aplicação de programa de boas práticas, com vistas à adoção de medidas adequadas e proporcionais no combate ao comportamento inautêntico e na transparência sobre conteúdos pagos.	Exclusão	Entendemos que a lei prevista deve ser aplicável a todos os provedores de serviços de rede social e serviços de mensageria. O estabelecimento de um piso mínimo a ser atingido antes de que se tenha a aplicação da lei na prática cria um desincentivo para o crescimento das empresas e uma barreira para a inovação, pois convida a empresas a limitar seu plano de negócios e seu crescimento para deixar de atrair o ônus regulatório da lei.
	Art. 5º Para os efeitos desta Lei, considera-se: (...) VIII – rede social: aplicação de internet que se destina a realizar a conexão de usuários entre si, permitindo e tendo como centro da atividade a comunicação, o compartilhamento e a disseminação de conteúdo em um mesmo sistema de informação, através de contas conectadas ou acessíveis entre si de forma articulada; e	Art. 5º Para os efeitos desta Lei, considera-se: (...) VIII – rede social: aplicação de internet que se destina a realizar a conexão de usuários entre si, permitindo e tendo como centro da atividade a comunicação, o compartilhamento e a disseminação de conteúdo em um mesmo sistema de informação, através de contas conectadas ou acessíveis entre si de forma articulada, excluindo-se dessa definição as aplicações cujo foco principal das atividades seja o comércio eletrônico; e	O conceito de “redes sociais” definido pelo inciso VIII deste artigo é amplo, e há o risco de enquadramento dos Marketplaces e outros e-commerces, cujo foco é a comercialização de produtos, fugindo totalmente do escopo deste PL. Portanto, incluímos esses provedores como exceção ao PL.

LIBERDADE DE EXPRESSÃO E PROTEÇÃO DE DADOS	<p>Art. 7º Os provedores de redes sociais e de serviços de mensageria privada poderão requerer dos usuários e responsáveis pelas contas, em caso de denúncias por desrespeito a esta Lei, no caso de indícios de contas automatizadas não identificadas como tal, de indícios de contas inautênticas ou ainda nos casos de ordem judicial, que confirmem sua identificação, inclusive por meio da apresentação de documento de identidade válido.</p>	<p>Art. 7º Os provedores de redes sociais e de serviços de mensageria privada poderão requerer dos usuários e responsáveis pelas contas “, em caso de denúncias por desrespeito a esta Lei, no caso de indícios de contas automatizadas não identificadas como tal, ou de indícios de contas inautênticas ou ainda nos casos de ordem judicial , que confirmem sua identificação, inclusive por meio da apresentação de documento de identidade válido , que será usado exclusivamente para a finalidade prevista de confirmação e segundo o disposto na Lei nº 13.709/2018 .</p>	<p>Apesar de evoluir em relação às versões anteriores do texto, o artigo ainda prevê situações genéricas, que poderiam causar coleta muito ampla de dados, em contrariedade ao princípio de coleta do mínimo necessário à provisão de serviços. Quanto à ordem judicial, sugere-se a exclusão do trecho por não estar alinhado ao cenário atual. Hoje já é possível que juízes determinem o fornecimento de registros e dados de identificação de usuários, nos termos do Marco Civil da Internet. Sugeriu-se ainda a inclusão de um trecho final, para deixar clara a conformidade do disposto aos parâmetros e regras da Lei Geral de Proteção de Dados.</p>
	<p>Parágrafo único. Os provedores de redes sociais e de serviços de mensageria privada deverão desenvolver medidas técnicas para detectar fraude no cadastro e o uso de contas em desacordo com a legislação, devendo informá-las em seus termos de uso ou em outros documentos disponíveis aos usuários.</p>	<p>Parágrafo único. Os provedores de redes sociais e de serviços de mensageria privada poderão desenvolver medidas técnicas para detectar fraude no cadastro e o uso de contas em desacordo com a legislação, devendo informá-las em seus termos de uso ou em outros documentos disponíveis aos usuários.</p>	<p>Não só para manter a coerência com o caput (que comanda a interpretação de todo o dispositivo), mas porque na forma anterior, o parágrafo único dava poder excessivo às plataformas, e poderia resultar em monitoramento ou amplo controle de contas. Isso porque exigia a adoção de medidas para detecção de contas "em desacordo com a legislação" - expressão excessivamente vaga.</p>

EXCLUSÃO DIGITAL	Art. 8º Os serviços de mensageria privada que ofertem serviços vinculados exclusivamente a números de celulares ficam obrigados a suspender as contas de usuários que tiveram os contratos rescindidos pelas operadoras de telefonia ou pelos usuários do serviço.	Exclusão	<p>Ao exigir a suspensão de usuários cujos contratos foram rescindidos pelas operadoras de telefonia, o artigo amplia a exclusão social no Brasil, e impacta direta e negativamente os milhões de brasileiros usuários de celulares pré-pagos.</p> <p>Em maio deste ano, foi realizada uma pesquisa¹ que estimou que cerca de 25 milhões das pessoas mais pobres usam somente a internet do celular, e muitas sequer conseguem manter o celular com crédito. Logo, o artigo significaria uma obrigação forçada de recarga de celulares pré-pagos, algo hoje difícil ou mesmo impossível para muitas famílias, especialmente diante do cenário atual de crise econômica.</p> <p>Por sua vez, o parágrafo 1º impõe o compartilhamento de dados amplo e desproporcional entre serviços de mensageria privada e operados de telefonia, o que levanta uma série de preocupações sob a ótica de privacidade e proteção de dados.</p>
	§ 1º Para o cumprimento do caput, os serviços de mensageria privada deverão solicitar os números objeto de contratos rescindidos às operadoras de telefonia, que os disponibilizarão, sem acréscimo de quaisquer outros dados cadastrais, conforme regulamentação.	Exclusão	
	§ 2º O disposto no caput não se aplica aos casos em que os usuários tenham solicitado a vinculação da conta para novo número de telefone.	Exclusão	

¹ <https://www1.folha.uol.com.br/mercado/2020/05/cerca-de-70-milhoes-no-brasil-tem-acesso-precario-a-internet-na-pandemia.shtml>

EXCLUSÃO DIGITAL	Art. 9º Os provedores de serviços de mensageria privada devem estabelecer políticas de uso destinadas a:	Art. 9º Os provedores de serviços de mensageria privada devem estabelecer políticas de uso destinadas a:	
	II – limitar o número de encaminhamentos de uma mesma mensagem a usuários ou grupos, bem como o número máximo de membros por grupo.	Exclusão	Grupos de família, amigos e de negócios médios ou pequenos, ONG, etc., se organizam em grupos de mensageria. Limitar o número de membros de grupos fere o direito constitucional de livre associação de pessoas (art. 5º, XVII da Constituição Federal). O artigo em comento afeta os benefícios sociais dessa tecnologia para as pessoas que usam os serviços para fins lícitos. Ainda, a legislação não deveria intervir no nível operacional das empresas, e sim, deixar que mecanismos inovadores que cumpram o propósito da lei sejam criados.
	III – instituir mecanismos para aferir consentimento prévio do usuário para inclusão em grupos de mensagens, listas de transmissão ou mecanismos equivalentes de encaminhamento de mensagens para múltiplos destinatários; e	III – instituir mecanismo para aferir consentimento prévio de dar controle ao usuário para inclusão ou exclusão em grupo de mensagens, listas de transmissões ou mecanismos equivalentes de encaminhamento de mensagem para múltiplos destinatários; e	As sugestões de alteração aos incisos III e IV endereçam parte da problemática do consentimento prévio e garante o direito de livre associação das pessoas.
	IV – desabilitar, por padrão, a autorização para inclusão em grupos e em listas de transmissão ou mecanismos equivalentes de encaminhamento de mensagens para múltiplos destinatários.	IV – desabilitar, por padrão, a autorização para instituir mecanismo para bloquear chamadores desconhecidos, impossibilitando a inclusão em grupos e em listas de transmissões ou mecanismos equivalentes de encaminhamento de mensagem para múltiplos destinatários realizados por desconhecidos .	

RASTREABILIDADE	Art. 10. Os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens.	Art. 10. Para fins de constituição de prova em investigação criminal e em instrução processual penal, a autoridade judicial pode determinar aos provedores de serviço de mensageria privada a preservação e disponibilização das interações de usuários determinados por um prazo de 15 (quinze) dias, considerados os requisitos estabelecidos no artigo 2º da Lei 9.296/1996, vedados os pedidos genéricos ou fora do âmbito e dos limites técnicos do seu serviço.	<p>O rastreamento de mensagens por encaminhamento em massa significa uma coleta massiva e desproporcional de dados. A proposta traz elevada onerosidade, não apenas em termos de custos para as plataformas, mas principalmente em relação à forma como afetará a privacidade do cidadão comum.</p> <p>O mero encaminhamento em massa não deve ser considerado algo negativo ou suspeito, por si só, invertendo a lógica da presunção de inocência. Além disso, as redes de distribuição de informações falsas muitas vezes utilizam identidade falsa, contas fora do país, e outros artifícios para iniciar o processo de viralização, tornando impossível a efetiva identificação da origem.</p> <p>Dessa forma, não se deve enfraquecer a privacidade e a segurança de todos os usuários, com o objetivo de atingir a minoria de casos de uso abusivo ou de má-fé.</p>
	§ 1º Considera-se encaminhamento em massa o envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários.	§ 1º As interações de usuário determinado de que trata o caput correspondem aos dados de envio e recebimento de mensagens por sua conta e devem incluir data e hora de sua ocorrência.	
	§ 2º Os registros de que trata o caput devem conter a indicação dos usuários que realizaram encaminhamentos em massa da mensagem, com data e horário do encaminhamento e o quantitativo total de usuários que receberam a mensagem	§ 2º O prazo de 15 (quinze) dias de disponibilização das interações de usuários determinados poderá ser renovado por até 3 (três) oportunidades mediante autorizações judiciais específicas.	
	§ 3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento em massa de conteúdo ilícito, para constituição de prova em investigação criminal e em instrução processual penal, mediante ordem judicial, nos termos da Seção IV do Capítulo III da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).	§ 3º A autoridade policial ou o Ministério Público poderão requerer cautelarmente a prorrogação justificada da preservação dos dados de que trata o caput por igual período, devendo ingressar com o pedido de autorização judicial de acesso aos respectivos registros em um prazo não superior a 30 (trinta) dias.	
	§ 4º A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 (mil) usuários, devendo seus registros ser destruídos nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).	§ 4º Exauridos os prazos ou diante de decisão judicial que denegue o pedido cautelar de prorrogação da preservação e disponibilização dos dados de que trata o caput e o § 2º, o provedor de serviço de mensageria privada deverá proceder sua eliminação em até 10 (dez) dias da respectiva notificação pela autoridade competente.	

MODERAÇÃO DE CONTEÚDO	Art. 12. Os provedores de aplicação de internet submetidos a esta Lei devem garantir o direito de acesso à informação e à liberdade de expressão de seus usuários nos processos de elaboração e aplicação de seus termos de uso, disponibilizando mecanismos de recurso e devido processo.	Art. 12. Os provedores de aplicação de internet submetidos a esta Lei devem garantir o direito de acesso à informação e à liberdade de expressão de seus usuários na aplicação de seus termos de uso e de suas políticas , disponibilizando mecanismos para eventuais pedidos de revisão por parte do usuário responsável pelo conteúdo afetado .	O ajuste na redação tem o cunho de evitar confusão sobre uma possível burocratização ou procedimentalização excessiva e prévia da aplicação dos termos de uso dos provedores de aplicação. Esta sugestão inclui a supressão da referência à elaboração de termos e políticas, uma vez que submeter alterações nos termos e/ou políticas à participação dos usuários seria uma intervenção desproporcional na liberdade de iniciativa e de organização empresarial. Por fim, a sugestão contempla a supressão da ideia de recurso como remédio disponível aos usuários, uma vez que isso somente faria sentido numa disputa concreta e não no caso de discussões abstratas sobre o conteúdo de termos e/ou políticas.
	§1º Em caso de denúncia ou de medida aplicada em função dos termos de uso das aplicações ou da presente Lei que recaia sobre conteúdos e contas em operação, o usuário deve ser notificado sobre a fundamentação, o processo de análise e a aplicação da medida, assim como sobre os prazos e procedimentos para sua contestação.	§ 1º Em caso de medida aplicada em função dos termos de uso das aplicações ou da presente Lei que recaia sobre conteúdos e contas em operação, o usuário deve ser notificado sobre a fundamentação e a aplicação da medida, assim como sobre os prazos e procedimentos para recorrer .	Mesma questão abordada acima sobre a procedimentalização excessiva e prévia à moderação de conteúdo, engessando a aplicação dos termos de uso e políticas dos provedores de aplicações, e podendo abrir margem para abusos.
	§ 2º Os provedores dispensarão a notificação aos usuários se verificarem risco: I – de dano imediato de difícil reparação; II – para a segurança da informação ou do usuário; III – de violação a direitos de crianças e adolescentes; IV – de crimes tipificados na Lei nº 7.716, de 5 de janeiro de 1989; V – de grave comprometimento da usabilidade, integridade ou estabilidade da aplicação.	Exclusão	A aplicação imediata dos termos de uso deve ser possível, sem exceções formais que acabariam por descaracterizar completamente os serviços prestados pelas plataformas e impedir que estas atendam às expectativas de seus usuários, além de facilitar a disseminação rápida de conteúdo irregular e de induzir dúvidas, com grande risco de incentivo à judicialização.

MODERAÇÃO DE CONTEÚDO	<p>§ 5º O prazo de defesa será diferido nos casos de conteúdo que use imagem ou voz manipuladas para imitar a realidade, com o objetivo de induzir a erro acerca da identidade de candidato a cargo público, ressalvados o ânimo humorístico ou de paródia.</p>	Exclusão	<p>O parágrafo poderá fazer com que casos abusivos de mídia manipulada enganosa (as chamadas "deep fakes") sobre políticos e candidatos fiquem ainda mais tempo online. Além disso, com as mudanças do artigo 12 em relação aos textos anteriores, não há mais sentido se falar em "defesa". O artigo cria a norma geral de notificação e possibilidade de recurso do usuário afetado pela decisão de moderação, independentemente do caso. O parágrafo apenas prolonga situações de abuso envolvendo candidatos, o que pode ser particularmente grave em contexto eleitoral.</p>
	<p>§ 6º A decisão do procedimento de moderação deverá assegurar ao ofendido o direito de resposta na mesma medida e alcance do conteúdo considerado inadequado.</p>	Exclusão	<p>Em linha com o parágrafo anterior. Além disso, o dispositivo confere um poder excessivo às plataformas, que determinarão os casos e critérios para resposta. Também não há qualquer clareza sobre quem seria a figura do ofendido. E, no contexto de eleições e candidatos à cargos públicos, a legislação eleitoral prevê em detalhe o exercício do direito de resposta, inclusive na internet e especialmente quando há impulsionamento de propaganda eleitoral, conforme disposto pelo artigo 58 da Lei Eleitoral. O parágrafo 6º pode gerar insegurança e desequilíbrio na disputa eleitoral.</p>

TRANSPARÊNCIA DOS RELATÓRIOS	Art. 13. Os provedores de redes sociais devem produzir relatórios trimestrais de transparência, disponibilizados em seus sítios eletrônicos, em português, para informar os procedimentos e as decisões de tratamento de conteúdos gerados por terceiros no Brasil, bem como as medidas empregadas para o cumprimento desta Lei	Art. 13. Os provedores de redes sociais devem, no âmbito e nos limites técnicos de seus serviços , produzir relatórios semestrais de transparência, disponibilizados em seus sítios eletrônicos, em português, para informar os procedimentos e as decisões de tratamento de conteúdos gerados por terceiros, bem como as medidas empregadas para o cumprimento desta Lei	A periodicidade semestral é adotada em todo o mundo, inclusive na Europa e países como a Alemanha, sendo, portanto, factível, especialmente se levarmos em consideração o nível de granularidade exigido do artigo 13. Além disso, sugere-se a pequena ressalva de que sejam respeitados os limites técnicos das plataformas para que possam contemplar um período em que será necessário desenvolver alguns pontos, como histórico e comparações (métricas ainda não disponíveis) a fim de observar o princípio da qualidade dos dados, conforme disposto pelo artigo 6º, inciso V da LGPD. Por fim, sugere-se a supressão da referência ao Brasil uma vez que implicaria a coleta e tratamento generalizado de dados de localização dos usuários, levantando a uma série de preocupações sob a ótica de proteção de dados, além de desconsiderar completamente o caráter global da internet.
	§ 1º Os relatórios devem conter, no mínimo:		
	I – número total de usuários que acessaram os provedores de redes sociais a partir de conexões localizadas no Brasil e número de usuários brasileiros ativos no período analisado;	Exclusão	Ao exigir e tratar dados de localização, haverá uma coleta ampla e desproporcional de dados pessoais mais do que o necessário para a provisão dos serviços, violando o princípio da necessidade, disciplinado no artigo 6º, inciso III da LGPD.
	II – número total de medidas de moderação de contas e conteúdos adotadas em razão do cumprimento dos termos de uso privado dos provedores de redes sociais, especificando as motivações, a metodologia utilizada na detecção da irregularidade e o tipo de medida adotada;	Exclusão	O dever de revelar a metodologia utilizada na detecção resulta na revelação da tática do provedor, e facilita ações de terceiros mal-intencionados para tentar escapar da detecção ou mesmo da aplicação dos termos de uso e/ou políticas no futuro.

TRANSPARÊNCIA DOS RELATÓRIOS	III – número total de medidas de moderação de contas adotadas em razão do cumprimento desta Lei, especificando as motivações, a metodologia utilizada na detecção da irregularidade e o tipo de medida adotada;	Exclusão	Mesmo comentário realizado acima. O dever de revelar a metodologia utilizada na detecção resulta na revelação da tática do provedor, e facilita ações de terceiros mal-intencionados para tentar escapar da detecção ou mesmo da aplicação dos termos de uso e/ou políticas no futuro.
	IV – número total de medidas de moderação de contas e conteúdos adotadas em razão de cumprimento de ordem judicial, especificando as motivações;	Exclusão	A remoção de contas e conteúdo em razão de ordem judicial não deve ser tratada como moderação de conteúdo. Isto é, não cabe aos provedores discutir as bases legais de decisões judiciais que determinem a remoção de conteúdo e/ou contas.
	V – número total de contas automatizadas e de redes de distribuição artificial detectadas pelo provedor e de conteúdos impulsionados e publicitários não identificados, especificando as correspondentes medidas adotadas e suas motivações e a metodologia utilizada na detecção da irregularidade;	Exclusão	Os dispositivos estabelecem exigências excessivas, granulares a tal ponto que desconsideram e ameaçam a diversidade de aplicações e a necessária neutralidade tecnológica. Esta desproporcionalidade é realçada especialmente quando se considera a complexidade envolvida na elaboração de relatórios de transparência, bem como a necessidade de se observar o princípio da qualidade de dados, podendo criar barreiras práticas possivelmente insuperáveis.
	VI – número total de medidas de identificação de conteúdo e os tipos de identificação, remoções ou suspensões que foram revertidas pela plataforma;	Exclusão	
	VII – características gerais do setor responsável por políticas aplicáveis a conteúdos gerados por terceiros, incluindo informações sobre a qualificação, a independência e a integridade das equipes de revisão de conteúdo, por pessoa natural;	Exclusão	Ao fazer referência às características gerais, o inciso se torna desproporcional, não resolvendo o problema público e levantando preocupações sob a ótica de privacidade.

TRANSPARÊNCIA DOS RELATÓRIOS	VIII – médias de tempo entre a detecção de irregularidades e a adoção de medidas em relação às contas e aos conteúdos referidos nos incisos II, III e IV;	Exclusão	A inclusão de métricas sobre tempo de detecção e resposta é excessivamente onerosa, haja vista que a cada semestre ocorrem milhões de remoções pelas plataformas. Como exemplo, nos relatórios de transparência divulgados por alguns provedores ² , podemos perceber a remoção de milhões de postagens contendo discurso de ódio no primeiro trimestre de 2020.
	IX – dados relacionados a engajamentos ou interações com conteúdos que foram identificados como irregulares, incluindo número de visualizações e de compartilhamentos e alcance; e	Exclusão	Assim como nos incisos V e VI, esse item também estabelece exigências excessivas, granulares a tal ponto que desconsideram e ameaçam a diversidade de aplicações e a necessária neutralidade tecnológica. Esta desproporcionalidade é realçada especialmente quando se considera a complexidade envolvida na elaboração de relatórios de transparência, bem como a necessidade de se observar o princípio da qualidade de dados, podendo criar barreiras práticas possivelmente insuperáveis.
	X – atualizações das políticas e termos de uso feitas no trimestre, a data da modificação e a justificativa para a sua adoção.	X – atualizações das políticas e termos de uso feitas no semestre , a data da modificação e a justificativa para a sua adoção.	Traz uma melhor delimitação, dando consistência ao PL, contemplando a mudança sugerida no <i>caput</i> .
	§ 2º Os dados e os relatórios publicados devem ser disponibilizados com padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.	§ 2º Os dados e os relatórios publicados devem ser disponibilizados com padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados no âmbito e nos limites técnicos do seu serviço .	A sugestão considera que os padrões de interoperabilidade devem estar disponíveis, e atender a preocupações técnicas e de segurança. Por exemplo, não à toa a LGPD confere à futura Autoridade Nacional de Proteção de Dados o papel de dispor sobre padrões de interoperabilidade para fins de portabilidade.

² [Apple](#), [Google](#), [Facebook](#)

TRANSPARÊNCIA DOS RELATÓRIOS	§ 3º Os relatórios de transparência devem ser disponibilizados ao público em até 30 (trinta) dias após o término do trimestre.	Exclusão	A exclusão visa apenas manter a periodicidade semestral dos relatórios – conforme sugestão de alteração do caput – uma vez que a confecção dos relatórios de transparência exigirá mais tempo e esforço das plataformas para sua elaboração.
	§ 4º Os relatórios e dados disponibilizados devem apontar a relação entre contas automatizadas não identificadas como tal, contas e disseminação de conteúdos, de modo que seja possível a identificação de redes artificiais de disseminação de conteúdo.	Exclusão	A exigência é excessiva, e acaba implicando análise de conteúdos ao tratar de "disseminação de conteúdos". Caso essa exigência seja adotada, ao invés de ser um documento de transparência em nível agregado, o relatório se torna um verdadeiro documento personalizado, indicando especificamente contas e conteúdos, e atropelando princípios de proteção de dados.
	§ 6º Resguardado o respeito à proteção de dados pessoais, os provedores de redes sociais devem facilitar o compartilhamento de dados com instituições de pesquisa acadêmica, incluindo os dados desagregados	Exclusão	A redação levanta preocupações e riscos. Importante considerar que "respeito à proteção de dados" não é específica o suficiente para permitir "compartilhamento de dados" de maneira geral. Há questões sérias de privacidade, propriedade intelectual (e segredo de negócio), bem como segurança e existência de padrões técnicos que permitam isso. Além disso, o termo genérico de "instituição de pesquisa acadêmica" poderia ser interpretado como um direito de acesso a dados amplo e irrestrito, pondo em risco os dados de milhões de usuários sem salvaguardas previstas além de um amplo "respeito à proteção de dados".

IMPULSIONAMENTO E PUBLICIDADE	Art. 14. Os provedores de redes sociais devem identificar todos os conteúdos impulsionados e publicitários, de modo que:	Art. 14. Os provedores de redes sociais devem identificar como tal todo conteúdo impulsionado e publicitários.	<p>O objeto do PL é garantir que todos os conteúdos impulsionados e publicitários sejam identificados como tal, em linha com o princípio de transparência da publicidade. No entanto, as exigências que vão muito além dessa garantia básica – como a de identificação de todas as contas responsáveis – devem ser restritas aos anúncios políticos eleitorais. Exigir identificação de todas as contas responsáveis por qualquer tipo de anúncio ou publicidade esbarra em obstáculos práticos e econômicos.</p> <p>Neste caso sugere-se a que os incisos I e II sejam contemplados apenas no dispositivo seguinte, que cuida de impulsionamento de propaganda eleitoral ou conteúdo político. Estes, pelo seu interesse público, são tipos de anúncio que merecem o maior grau de transparência possível. Exigir indicação de contas e informações de contato de todo e qualquer anunciante é desproporcional, desnecessário e pode expor a privacidade e a segurança, sobretudo dos pequenos empreendedores que fazem impulsionamento ou publicidade de seus negócios, produtos ou serviços.</p>
	I – identifique a conta responsável pelo impulsionamento ou anunciante; e	Exclusão – Já é contemplado pelo inciso II do artigo 15	
	II – permita ao usuário acessar informações de contato da conta responsável pelo impulsionamento ou o anunciante.	Exclusão	

IMPULSIONAMENTO E PUBLICIDADE	Art. 15. Os provedores de redes sociais que fornecerem impulsionamento de propaganda eleitoral ou de conteúdos que mencionem candidato, coligação ou partido devem disponibilizar ao público todo o conjunto de anúncios para efeito de checagem pela Justiça Eleitoral e outros fins, incluindo:		
	V – características gerais da audiência contratada.	V – características gerais da audiência atingida.	Exigir a exposição da audiência contratada poderá expor as estratégias de campanha de cada candidato e partido, o que inevitavelmente gerará ruído ou confusão, pois muitas vezes a audiência efetivamente atingida difere e pode ser bem menor que a audiência contratada. Além disso, a legislação eleitoral já cuida razoavelmente do tema, e agora a LGPD traz parâmetros sobre a coleta e o tratamento de dados (inclusive por candidatos e partidos) que deverão ser observados a ajudarão a evitar abusos.
	Art. 16. Os provedores de redes sociais devem disponibilizar mecanismos para fornecer aos usuários as informações do histórico dos conteúdos impulsionados e publicitários com os quais a conta teve contato nos últimos 6 (seis) meses.	Exclusão	A redação levanta questões de privacidade e proteção de dados (especialmente na expressão vaga e ampla de "com os quais a conta teve contato"). Além disso, o propósito de transparência é mais amplo, e os anúncios devem estar disponíveis à visibilidade social, independentemente de se ter tido "contato" com aquele conteúdo. Ao mesmo tempo, exigir um histórico de todo e qualquer conteúdo impulsionado ou publicitário seria excessivo e apenas geraria ruído. Como se observou antes, o histórico de anúncios, inclusive inativos, deve ser medida para aqueles tipos de anúncio que exigem maior nível de transparência, isto é, os anúncios políticos e eleitorais.

IMPULSIONAMENTO E PUBLICIDADE	Art. 17. Os provedores de redes sociais devem requerer dos anunciantes e responsáveis pelas contas que impulsionam conteúdos que confirmem sua identificação, inclusive por meio da apresentação de documento de identidade válido.	Art. 17. Os provedores de redes sociais podem requerer dos anunciantes e responsáveis pelas contas que impulsionam conteúdos políticos e propaganda eleitoral que confirmem sua identificação, inclusive por meio da apresentação de documento de identidade válido.	A exigência generalizada de confirmação de identidade de todo e qualquer anunciante impacta diretamente os pequenos e médios negócios e empreendedores individuais que anunciam em plataformas. Essa aproximação será dificultada e desacelerada com a imposição generalizada de um burocrático processo de verificação a ser enfrentado. É um processo de difícil e custosa execução prática por parte das plataformas também é desnecessário e desproporcional em relação aos anunciantes, gerando um impacto econômico negativo robusto. Por isso, sugere-se focar essa exigência de confirmação de identificação nos anúncios de impacto público e que merecem maior nível de transparência, isto é, os anúncios políticos e eleitorais.
	Parágrafo único. O nome e a identidade do contratante de impulsionamento ou publicidade devem ser mantidos em sigilo pelos provedores de aplicação, podendo ser exigíveis por ordem judicial nos termos do art. 22 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).	Exclusão	A coleta de dados pessoais nesse caso tem por finalidade confirmar a identidade do responsável por impulsionar a propaganda eleitoral ou conteúdo político. Assim, em respeito aos princípios e parâmetros de proteção de dados, especialmente o princípio da necessidade positivado no artigo 6, inciso III da LGPD, esses dados não precisam e não devem continuar armazenados.

FISCALIZAÇÃO E SANÇÕES	Art. 31. Sem prejuízo das demais sanções civis, criminais ou administrativas, os provedores de redes sociais e de serviços de mensageria privada ficam sujeitos a:	Art. 31. Sem prejuízo das demais sanções civis, criminais ou administrativas, os provedores de redes sociais e de serviços de mensageria privada que violarem dispositivos desta lei ficam sujeitos a às seguintes penalidades a serem aplicadas pelo Poder Judiciário, assegurados o devido processo legal, a ampla defesa e o contraditório:	
	II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício.	II – multa de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração.	Embora a redação preveja que as multas serão aplicadas com proporcionalidade, verifica-se que a quantia estipulada de 10% (dez por cento) é extremamente danosa aos provedores. Portanto, a sugestão é de que tanto a multa, quanto o procedimento de análise para sua estipulação, sigam o que já está disposto no artigo 52 da LGPD, que dispõe sobre uma série de considerações a serem realizadas quando da aplicação da multa, e fixa a porcentagem máxima em até 2% (dois por cento) do faturamento do grupo econômico no Brasil em seu último exercício. Ademais, a alteração realizada no caput pretende tornar a medida sancionatória mais clara e objetiva, para que não gere dúvidas e maiores judicializações.
	§ 1º Na aplicação da sanção, a autoridade judicial observará a proporcionalidade, considerando a condição econômica do infrator, as consequências da infração na esfera coletiva e a reincidência.	§ 1º Na aplicação da sanção, a autoridade judicial observará: I – a gravidade e a natureza das infrações; II – a boa-fé do infrator; III – a condição econômica do infrator; IV – a reincidência; V – o grau do dano; VI – a cooperação do infrator; VII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; VIII – a adoção de política de boas práticas e governança; IX – a pronta adoção de medidas corretivas; e X – a proporcionalidade entre a gravidade da falta e a intensidade da sanção.	
		Sugestão de Inclusão: § 2º O procedimento para apuração das sanções mencionadas nesse capítulo deverá observar o disposto na Lei 7.347, de 24 de julho de 1985, inclusive no que se refere aos legitimados para propositura de ação.	
			Com esta mudança, eventuais sanções deverão ser processadas em termos já definidos no ordenamento jurídico brasileiro. Isso traz mais segurança jurídica, haja vista que, na falta de um órgão administrativo de fiscalização, isso impede a advocação desta competência por qualquer Órgão.

ACESSO REMOTO AO BANCO DE DADOS	<p>Art. 32. Os provedores de redes sociais e de serviços de mensageria privada deverão ter sede e nomear representantes legais no Brasil, informações que serão disponibilizadas em seus sítios na internet, bem como manter acesso remoto, a partir do Brasil, aos seus bancos de dados, os quais conterão informações referentes aos usuários brasileiros e servirão para a guarda de conteúdos nas situações previstas em lei, especialmente para atendimento de ordens de autoridade judicial brasileira</p>	<p>Exclusão</p>	<p>O artigo 32 determina, sem qualquer tipo de salvaguarda, o acesso remoto "referente a usuários brasileiros", sem definir quais tipos de dados estariam abrangidos na lei. Na prática, isto leva a uma série de preocupações que vão de encontro ao previsto pelo Marco Civil da Internet e em acordos de cooperação internacional, fundamentados na Constituição Federal. Da forma que está escrito, o texto do artigo 32 coloca em risco a privacidade dos usuários e segurança desses dados, que estariam sujeitos a abusos e acessos indevidos.</p> <p>Além disso, exigir sede e representação legal implica exigir excessivo aumento de custos. Por envolver alto investimento tecnológico em manutenção e implementação, pode ser impeditiva não apenas a diversas startups sediadas em outros locais do mundo, mas até mesmo redes sociais e serviços de mensageria estrangeiros já consolidados. A exigência de sede e representação também é contrária ao caráter aberto e global da internet (artigo 2º, inciso I do Marco Civil da Internet), incentivando movimento de cunho protecionista e nacionalista que é insustentável para a internet como a conhecemos caso seguida por outros países do mundo.</p> <p>A obrigação é contrária à lógica da transferência internacional de dados viabilizada pela LGPD e sem equivalente em qualquer lei paradigmática de proteção de dados pessoais no mundo. Também importa em redução da segurança, ao prever, de maneira ampla e sem garantias, uma hipótese de "acesso remoto" a dados.</p>
---------------------------------	--	-----------------	--

PORTA LÓGICA	<p>Art. 35. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:</p> <p>“Art. 5º..... VIII – registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP e a porta lógica, quando o IP for roteado; IX – roteamento de IP: o compartilhamento de um IP para mais de uma conexão ou usuário único, individualizadas através de diferentes portas lógicas; e X – portas lógicas: os dispositivos que operam e trabalham com um ou mais sinais lógicos de entrada para produzir uma e somente uma saída.” (NR)</p> <p>“Art. 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, inclusive os registros que individualizem o usuário de um IP de maneira inequívoca, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.” (NR)</p>	<p style="text-align: center;">Exclusão</p>	<p>A proposta do artigo 35 vai além do escopo de aplicação para alterar o próprio Marco Civil da Internet, cristalizado após anos de discussão, o que afetaria toda e qualquer aplicação de Internet, inclusive do poder público. Esse artigo busca adicionar o conceito de porta lógica como registro de acesso a aplicações de internet. A porta lógica é um expediente técnico utilizado por provedores de conexão como medida de transição entre o sistema IPv4, pelo qual muitos usuários precisam compartilhar o mesmo IP, para o protocolo IPv6. No entanto a lei cria um incentivo inverso ao investimento em infraestrutura por parte das empresas de telecomunicações. A porta lógica é apenas mecanismo paliativo de transição enquanto a infraestrutura brasileira não é integralmente substituída pelo sistema IPv6. Ao transformar em um mecanismo legal, a lei privilegiaria a manutenção do antigo sistema IPv4, adiando e desincentivando os investimentos para a transição ao sistema IPv6, mais seguro e eficiente. O esgotamento dos IPs disponíveis passa a ser contornado em definitivo por um paliativo. Atribuir agora esse dever de coleta e armazenamento de dados, que não existia anteriormente, envolve soluções complexas de engenharia e altíssimos custos. E tudo isso para uma obrigação que em breve deve se tornar obsoleta. Não é razoável exigir uma adaptação imediata dos sistemas da empresa em razão transitória. Por essa mesma razão, cria-se um relevante barreira de entrada para provedores de aplicações de pequeno e médio porte, que não teriam condições de arcar com os custos de adaptação de seus sistemas, o que traria prejuízo da pluralidade de conteúdos e de atividade econômica na internet brasileira. Por fim, a ausência de dados de porta lógica por parte dos provedores de aplicação não dificulta ou impede a identificação dos usuários na internet. Na</p>
--------------	--	--	---

			<p>prática, pela experiência dos provedores de aplicações de maior expressão, o compartilhamento de IPs não tem sido um obstáculo para o avanço de investigações criminais. Os dados já disponibilizados pelas aplicações de internet às autoridades de investigação (registros de acesso previstos no Marco Civil da Internet combinados com dados cadastrais, como endereços de e-mail, números de telefone e números de cartão de crédito, quando existentes), aliados aos dados fornecidos pelas empresas de telecomunicações, já são suficientes para identificação de indivíduos por trás de condutas ilegais nas plataformas.</p> <p>Ainda, vale reiterar que a definição de “porta lógica” bem como as alterações propostas no art. 15 do PL estão inadequadas e representam grave insegurança jurídica, sendo imperiosa a exclusão deste artigo.</p>
VIGÊNCIA	<p>Art. 36 . Esta Lei entra em vigor em:</p> <p>I – na data de sua publicação, quanto aos arts. 25, 26, 27, 28 e 29; e</p> <p>II – após decorridos 90 (noventa) dias de sua publicação oficial, demais artigos, observado o dispositivo no art. 16 da Constituição Federal.</p>	<p>Art. 36 . Esta Lei entra em vigor em:</p> <p>I – na data de sua publicação, quanto aos arts. 25, 26, 27, 28 e 29; e</p> <p>II – após 12 (doze) meses de sua publicação, quanto aos demais artigos, observado o dispositivo no art. 16 da Constituição Federal.</p>	<p>Para estar em conformidade com a Lei, empresas deverão trabalhar em planos de conformidade e reestruturação de produtos e/ou serviços. Assim, a <i>vacatio legis</i> deve considerar as complexidades técnicas para garantir a efetividade da Lei.</p>



SENADO FEDERAL
Secretaria-Geral da Mesa

DESPACHO Nº 2/2021

Junte-se à página oficial da tramitação das proposições legislativas as cópias eletrônicas de manifestações externas, conforme listagem a seguir exposta:

1. PLS nº 158 de 2018. Documento SIGAD nº 00100.092667/2020-54
2. PL nº 575 de 2020. Documento SIGAD nº 00100.10884/2020-21
3. PEC nº 187 de 2019. Documento SIGAD nº 00100.114120/2020-17
4. PEC nº 65 de 2019. Documento SIGAD nº 00100.040432/2020-87
5. PL nº 2630 de 2020. Documento SIGAD nº 00100.075445/2020-77
6. PL nº 5961 de 2019. Documento SIGAD nº 00100.092670/2020-78
7. PL nº 735 de 2020. Documento SIGAD nº 00100.092684/2020-91
8. PL nº 2139 de 2020. Documento SIGAD nº 00100.092409/2020-78
9. PL nº 2564 de 2020. Documento SIGAD nº 00100.092403/2020-09
10. PL nº 439 de 2015. Documento SIGAD nº 00100.092392/2020-59
11. PL nº 1095 de 2019. Documento SIGAD nº 00100.092398/2020-26
12. PL nº 3267 de 2019. Documento SIGAD nº 00100.077595/2020-15
13. PL nº 1615 de 2019. Documento SIGAD nº 00100.100994/2020-97
14. PLC nº 134 de 2018. Documento SIGAD nº 00100.077607/2020-10
15. PL nº 3204 de 2019. Documento SIGAD nº 00100.077632/2020-95
16. MPV nº 983 de 2020. Documento SIGAD nº 00100.077660/2020-11
17. PL nº 2564 de 2020. Documento SIGAD nº 00100.072552/2020-43
18. MPV nº 927 de 2020. Documento SIGAD nº 00100.072366/2020-12
19. MPV nº 975 de 2020. Documento SIGAD nº 00100.087563/2020-28
20. PEC nº 18 de 2020. Documento SIGAD nº 00100.073354/2020-05
21. PL nº 2048 de 2020. Documento SIGAD nº 00100.073322/2020-00
22. PLS nº 166 de 2018. Documento SIGAD nº 00100.072565/2020-12
23. PLS nº 166 de 2018. Documento SIGAD nº 00100.073287/2020-11



24. PEC nº 110 de 2019. Documento SIGAD nº 00100.088138/2020-56
25. PEC nº 110 de 2019. Documento SIGAD nº 00100.077096/2020-28
26. PL nº 5106 de 2019. Documento SIGAD nº 00100.113120/2020-08
27. MPV nº 910 de 2019. Documento SIGAD nº 00100.049575/2020-54
28. PL nº 3267 de 2019. Documento SIGAD nº 00100.050001/2020-29
29. VET nº 39 de 2020. Documento SIGAD nº 00100.080420/2020-95
30. VET nº 39 de 2020. Documento SIGAD nº 00100.079993/2020-76
31. PEC nº 21 de 2020. Documento SIGAD nº 00100.076390/2020-12
32. PLS nº 486 de 2017. Documento SIGAD nº 00100.076416/2020-22
33. VET nº 30 de 2020. Documento SIGAD nº 00100.085426/2020-59
34. PL nº 3932 de 2020. Documento SIGAD nº 00100.083745/2020-20
35. PL nº 4458 de 2020. Documento SIGAD nº 00100.085080/2020-99
36. PL nº 3267 de 2019. Documento SIGAD nº 00100.074819/2020-37
37. MPV nº 961 de 2020. Documento SIGAD nº 00100.079662/2020-36
38. PLS nº 5 de 2015. Documento SIGAD nº 00100.106067/2020-81
39. MPV nº 951 de 2020. Documento SIGAD nº 00100.069133/2020-24
40. MPV nº 951 de 2020. Documento SIGAD nº 00100.070465/2020-51
41. PL nº 3364 de 2020. Documento SIGAD nº 00100.102688/2020-95
42. PL nº 3267 de 2019. Documento SIGAD nº 00100.079555/2020-16
43. PL nº 3267 de 2019. Documento SIGAD nº 00100.079858/2020-21
44. PL nº 4414 de 2020. Documento SIGAD nº 00100.080005/2020-31
45. PL nº 4021 de 2020. Documento SIGAD nº 00100.081717/2020-78
46. PLP nº 197 de 2020. Documento SIGAD nº 00100.081717/2020-78
47. PL nº 172 de 2020. Documento SIGAD nº 00100.082379/2020-70
48. PL nº 6549 de 2019. Documento SIGAD nº 00100.082379/2020-70
49. PLS nº 349 de 2018. Documento SIGAD nº 00100.082379/2020-70
50. PEC nº 187 de 2019. Documento SIGAD nº 00100.082379/2020-70

Secretaria-Geral da Mesa, 21 de janeiro de 2021.

(assinado digitalmente)
JOSÉ ROBERTO LEITE DE MATOS
Secretário-Geral da Mesa Adjunto

