Rastreabilidade de mensagens instantâneas

Comunicações privadas, investigações e **direitos**

iris
INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

Rastreabilidade de mensagens instantâneas

AUTORIA

Gustavo Ramos Rodrigues

Paulo Rená da Silva Santarém

Victor Barbieri Rodrigues Vieira

REVISÃO

Lahis Pasquali Kurtz

Luíza Couto Chaves Brandão

REVISÃO EXTERNA

Nathalia Sautchuk Patrício

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO

Felipe Duarte

PRODUÇÃO EDITORIAL

Instituto de Referência em Internet e Sociedade

COMO CITAR EM ABNT

RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos**: rastreabilidade de mensagens instantâneas. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em: <https://bit.ly/3yLlb0P>. Acesso em: dd mmm aaaa.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

DIREÇÃO

Luíza Couto Chaves Brandão

VICE-DIREÇÃO

Paloma Rocillo

MEMBROS

Ana Bárbara Gomes | Pesquisadora

Felipe Duarte | Coordenador de Comunicação

Fernanda Rodrigues | Pesquisadora

Gustavo Rodrigues | Coordenador de Políticas Públicas e Pesquisador

Juliana Roman | Pesquisadora

Júlia Caldeira | Pesquisadora

Lahis Kurtz | Coordenadora de Pesquisa e Pesquisadora

Paloma Rocillo Rolim do Carmo | Vice-diretora e Pesquisadora

Paulo Renâ da Silva Santarém | Pesquisador

Rafaela Ferreira | Estagiária de pesquisa

Thais Moreira | Estagiária de comunicação

Victor Barbieri Rodrigues Vieira | Pesquisador

SUMÁRIO

Resumo executivo

O projeto **Comunicações privadas, investigações e direitos**, do Instituto de Referência em Internet e Sociedade – IRIS, busca oferecer subsídios confiáveis para o debate político e jurídico de investigações em comunicações privadas no Brasil combinar segurança de tecnologias da informação e comunicação com proteção de direitos humanos e de garantias democráticas. Pretende-se analisar impactos e riscos; sistematizar conhecimento científico; e, ao final, produzir recomendações para setores público e privado. O objeto de análise serão três mecanismos para investigações sobre comunicações privadas: rastreabilidade de mensagens instantâneas, *hacking* governamental, e varredura pelo lado do cliente.

Neste primeiro relatório, avaliou-se o panorama sobre a **rastreabilidade de mensagens instantâneas**. O termo se refere a um conjunto impreciso de métodos para guarda de metadados dessas comunicações, a fim de identificar o percurso ou a origem específica de um dado conteúdo. Por meio de uma revisão sistemática, investigou-se um total de 32 publicações selecionadas.

A seleção seguiu três etapas de buscas: palavras-chave, contribuições técnicas ao processo legislativo, e avaliação de relevância. Os achados foram organizados em quatro eixos: conceito; cenário brasileiro;cenário indiano; e modos, riscos e desafios da implementação da rastreabilidade.

Primeiro, a análise conceitual apontou múltiplos significados do termo rastreabilidade. E como o debate sobre sua inserção em sistemas online com criptografia carece de descrições sobre como implementá-lo, a indefinição tecnológica permite que várias propostas legislativas distintas usem o mesmo termo. Ademais, a falta de precisão conceitual enseja proposições sem base em conhecimentos técnicos e alheias à produção acadêmica pertinente.

Segundo, na disputa legislativa e jurídica no Brasil sobre a rastreabilidade de comunicações instantâneas, destacou-se a tramitação do Projeto de Lei nº 2630/2020. A proposta oficial de "instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet" ficou conhecida como "PL das Fake News". Na redação aprovada pelo Senado em junho de 2020, e até abril de 2022 formalmente válida, identificam-se, em síntese, a partir da literatura, cinco potenciais tipos de impactos negativos da rastreabilidade de mensagens instantâneas: i) a natureza interpessoal ou viral das mensagens definir o grau de proteção jurídica; ii) a identificação da cadeia de encaminhamento em massa afetar a livre expressão; iii) o enfrentamento à desinformação deslegitimar todo anonimato; iv) a guarda de dados desnecessários ao serviço afrontar o princípio legal de minimização do tratamento de dados pessoais; v) a guarda generalizada de dados violar direitos constitucionais ao devido processo legal, à proteção de dados pessoais, à presunção de inocência e ao sigilo das comunicações.

Terceiro, no âmbito político e legal da Índia, a partir das particularidades em torno das "Regras de TI", vigentes desde 2021, observaram-se os efeitos fáticos da positivação de regras de rastreabilidade sem a devida abertura do processo legislativo. A imprecisão do texto legal se reflete, por exemplo, na indefinição da extensão e dos limites de aplicação. Ainda, a unilateralidade do procedimento legislativo das Regras de TI gera, até hoje, críticas à própria legalidade e legitimidade da norma e amplifica incertezas jurídicas.

Quarto, aspectos tecnológicos dos modos de implementação, riscos e desafios da rastreabilidade de mensagens instantâneas em ambos países foram examinados. O mecanismo se contrapõe aos algoritmos criptográficos, usados em meios eletrônicos para segurança das comunicações. A análise dos métodos de implementação propostos (assinaturas digitais; verificação por *hashing*; análise de metadados; e franqueamento de mensagens), em todas abordagens disponíveis, revela ineficiência e deficiência, em falhas exploráveis para fins danosos. Atores mal-intencionados poderiam, por exemplo, tanto contornar os mecanismos de rastreabilidade, quanto imputar condutas ilícitas a inocentes.

Finalmente, os resultados confirmam a percepção de que a rastreabilidade de mensagens instantâneas requerida publicamente enseja propostas com razões políticas, mas sem evidências de viabilidade tecnológica.

Apresentação

Os primeiros debates sobre a criptografia forte envolviam a inserção de mecanismos para acesso excepcional das agências estatais de investigação e persecução penal aos algoritmos criptográficos. Mas a sociedade civil e a comunidade técnico-científica foram bem sucedidas na defesa de que políticas de segurança pública considerem riscos tecnológicos, jurídicos e econômicos.

Esses setores demonstraram que as ferramentas de quebra da criptografia para investigações por agentes públicos seriam inevitavelmente acessíveis também por terceiros mal intencionados, que poderiam migrar para plataformas sem acesso excepcional. O resultado seria a população em geral com menos segurança e os suspeitos intocáveis.[1] Tais argumentos diminuíram as demandas por soluções como portas clandestinas. Alternativas legislativas à quebra da criptografia surgiram, porém, para dar às autoridades acesso a dados e informações supostamente necessárias para identificar e punir criminosos.

O projeto **Comunicações privadas, investigações e direitos** busca sistematizar a literatura sobre métodos alegadamente alternativos à quebra da criptografia, para nutrir o debate científico, político e jurídico sobre o tema no Brasil. Pretende-se oferecer subsídios confiáveis para decisões políticas, regulatórias e judiciais combinarem a segurança das tecnologias de informação e comunicação com a proteção de direitos humanos e garantias democráticas. Em específico, objetiva-se: 1) analisar impactos e riscos à segurança de dados e informações digitais, e direitos envolvidos; 2) sistematizar conhecimento sobre técnicas de investigação; 3) produzir recomendações para o Estado e empresas.

Relatórios científicos analisarão três métodos alternativos: rastreabilidade de mensagens instantâneas, na qual se guardam metadados da comunicação para futura identificação do caminho ou da origem de um eventual conteúdo ilícito; *hacking* governamental, pelo qual se exploram vulnerabilidades ocultas e não-intencionais de um sistema; e varredura pelo lado do cliente, pelo qual se analisa e compara um dado conteúdo em um dispositivo com bases de dados prévias, em busca de um padrão específico.

A partir dos resultados, o Instituto de Referência em Internet e Sociedade – IRIS pretende dialogar com diversos setores e construir posicionamentos sobre esses métodos, com base em evidências científicas e no respeito aos direitos humanos. O material será disponibilizado online, para consulta e uso geral.

1. Introdução

A discussão de mecanismos de rastreabilidade de mensagens instantâneas destacou-se a partir de 2020, quando se criaram previsões legais na Índia para identificar autores originais de mensagens instantâneas criptografadas. Em poucos meses, o termo foi apropriado, com alterações no significado prático, em projetos de lei no Brasil, notadamente no denominado PL das Fake News. Desde então, o mecanismo figura como novo tema de intensas discussões no país.

Diferentes propostas têm em comum a retenção obrigatória de metadados para permitir eventual identificação ou do percurso de envios de um conteúdo por meio de sistemas eletrônicos de mensagens instantâneas com criptografia de ponta a ponta, ou das pessoas específicas que o criaram e difundiram. Essa guarda de dados conflita com a confidencialidade das comunicações, protegida pela criptografia: as propostas, alegadamente, não quebrariam os padrões de segurança criptográfica forte, mas seriam legais, eficientes e consistentes os meios propostos na adoção da rastreabilidade de mensagens instantâneas?

Coloca-se como pergunta central se a literatura pertinente permite afirmar a rastreabilidade como um meio adequado para, sem mecanismos de acesso excepcional, permitir investigações em sistemas com criptografia forte. Ao investigar riscos e desafios políticos, jurídicos e tecnológicos, este estudo busca organizar os principais pontos de defesa e crítica às propostas e avaliar sua viabilidade técnica e jurídica, mediante revisão bibliográfica sistemática de 32 textos selecionados. Definiu-se o *corpus* final à luz do cenário político, jurídico, legislativo e social brasileiro e indiano, e da técnica computacional.

Refletindo prós e contras, conforme o peso político e os parâmetros legais do debate, os resultados compõem quatro seções: o conceito de rastreabilidade; o contexto brasileiro do PL das Fake News; o contexto indiano das Regras de TI; e os pontos tecnológicos compartilhados entre eles. Ainda, os textos analisados estão listados no Apêndice 1, e o formulário de análise no Apêndice 2.

Antes da metodologia, narra-se a emergência, no debate das investigações de comunicações privadas, da rastreabilidade de mensagens instantâneas.

2. Contexto

Na segunda metade do século XX, o debate sobre a disponibilidade pública de criptografia forte para a proteção de comunicações privadas tem como centro a inserção de mecanismos para seu acesso por agências estatais de investigação e persecução penal. Esses esforços, todavia, renderam grandes controvérsias públicas quanto a seus

efeitos jurídico, político e econômico. Tais conflitos na governança da criptografia forte ficaram conhecidos como guerras criptográficas (*crypto wars*) e foram marcados pela resistência da comunidade técnico-científica, do setor privado e de ativistas de direitos humanos na área digital aos arranjos de acesso excepcional.[2]

Conquanto persista a pressão pública de autoridades, de diversos países, por tais mecanismos,[3] a década de 2010 viu novos tipos de propostas, sem acesso excepcional ao teor das comunicações cifradas. Com a promessa de combinar a segurança dos sistemas e meios para investigações de dados e informações exigidos para identificar e punir criminosos, elas abarcam técnicas de *hacking* governamental, varredura pelo lado do cliente e rastreabilidade de mensagens instantâneas com criptografia, que é o objeto deste estudo.

3. Metodologia

Há notável acúmulo histórico de estudos detalhando[4] riscos e impactos do acesso excepcional à criptografias. Mas as alegadas alternativas carecem do mesmo escrutínio. Em específico, a rastreabilidade de mensagens instantâneas tem proeminente discussão pública internacional a partir da instituição das Regras de TI na Índia e do PL 2630/2020 no Brasil, sem maturidade equivalente.

Se a ideia é responsabilizar por conteúdos danosos, como desinformação e discurso de ódio, a discussão política e jurídica - sobre se as investigações de comunicações privadas poderiam combinar segurança de TICs e proteção de direitos humanos - depende da consistência das bases técnicas e acadêmicas das propostas legislativas.

Para esse exame, realizou-se revisão sistemática de literatura, abordagem que investiga o estado da arte sobre determinado tema, com recorte empírico em um grupo de obras selecionadas e avaliadas por critérios e procedimentos explícitos e sistemáticos. Ela pode ajudar a identificar lacunas em estudos acadêmicos de certo campo ou temática,[5] questões e subtemas para novas investigações e projetos. Pesquisas assim

> *[...] são particularmente úteis para integrar as informações de um conjunto de estudos realizados separadamente sobre determinada terapêutica/intervenção, que podem apresentar resultados conflitantes e/ou coincidentes, bem como identificar temas que necessitam de evidência, auxiliando na orientação para investigações futuras.*[6]

Aqui, o *corpus* documental analisado tem três fontes: palavras-chave; contribuições ao processo legislativo; e obras relevantes selecionadas.

Primeiro, realizaram-se buscas em duas bases de dados, com 9 grupos de termos.

Na plataforma Scopus,[7] as palavras-chave foram: 1) "*traceability*" + ("*disinformation*" OR "*misinformation*"); 2) "*traceability of messages*"; 3) "*traceability* + *IT Rules*". E, na plataforma Google Acadêmico,[8] foram: 4) "*traceability*" + "*disinformation*"; 5) "*traceability of messages*"; 6) "rastreabilidade de mensagens"; 7) "rastreabilidade" + "desinformação"; 8) "rastreabilidade" + "PL 2630"; 9) "*traceability*" + "*IT Rules*".

Podem-se traduzir os termos em inglês por rastreabilidade (*traceability)*, rastreabilidade de mensagens (*traceability of messages*), e Regras de TI (*IT Rules*). A desinformação pode ser traduzida tanto como *disinformation* quanto como *misinformation,* dado o contexto[9]. A busca por termos em inglês, além dos em português, decorreu da escassez de bibliografia relativa ao contexto indiano das Regras de TI em língua brasileira, bem como para ampliação do estudo.

Excluídas as entradas repetidas, as 52 referências restantes foram sujeitas a avaliação preliminar de pertinência temática. Título, resumo (se presente) e seção inicial de cada obra foram lidos por dois pesquisadores, que votavam pela inclusão ou exclusão. Havendo dissenso, a decisão era do terceiro pesquisador. Essa fase filtrou textos com temas alheios ao estudo, como rastreabilidade em cadeias produtivas de gado, medicamentos, alimentos industrializados, matérias primas, etc. Restaram 30 textos, dos quais foram excluídos 2, cujo conteúdo se encontra sob restrição comercial, impedindo o acesso da equipe.

As 28 obras restantes foram então integralmente lidas, analisadas e inseridas em um formulário, com categorização (artigo, dissertação, capítulo de livro, etc); resumo; observações do pesquisador responsável; e citações em destaque. Gerou-se, então, uma síntese descritiva, orientada a identificar, em cada obra: proposta, metodologia (ou sua ausência), eventuais referências relevantes (citadas como base para o conceito ou posicionamento do trabalho); e qual a abordagem sobre a rastreabilidade de mensagens instantâneas.

Pelas categorias, deliberou-se excluir textos sem natureza acadêmica: 3 matérias de jornal, 1 publicação em *blog*, e 1 artigo de opinião. Assim, as buscas de palavras-chave gerou um subconjunto de **23 obras no *corpus* documental**.

O segundo subconjunto veio de contribuições técnicas de organizações sociais no debate legislativo do PL 2630/2020. A intenção foi inserir a discussão da rastreabilidade de mensagens instantâneas que poderia não constar entre os resultados da primeira fase. Os documentos foram buscados nos respectivos sites das entidades listadas na página institucional do "Grupo de Trabalho para Aperfeiçoamento da Legislação Brasileira - Internet" da Câmara dos Deputados, como participantes das audiências públicas realizadas por esse GT-Net.

De 87 entidades listadas: 11 foram descartadas, cujos websites não se conseguir identificar ou acessar; 14 cujos sites não possuíam buscadores; e 4 cujos buscadores

falharam. Nos demais 58, buscou-se por "rastreabilidade": 22 não apresentaram resultados pertinentes; 6 apresentaram apenas resultados sobre a cobertura da imprensa ao projeto de lei; 19 não retornaram resultados; e 11 deram resultado positivo. Desses, foram excluídos 8 por impertinência formal: eram notas de posicionamento político sobre o PL, e não contribuições técnicas ou acadêmicas. Ao final, **restaram 3 documentos, adicionados ao corpus examinado**.

Terceiro, de modo discricionário foram agregadas 6 referências bibliográficas já conhecidas pela equipe, mas que não figuraram nos resultados das fases anteriores. Esses textos foram selecionados pela relevância temática direta, com mais elementos para a análise aprofundada sobre o tema. Sabe-se que esse procedimento reduz a sistematicidade do estudo, com perda em termos de representatividade dos resultados, porquanto dependentes de uma análise subjetiva da equipe de pesquisa. Entendeu-se que essa desvantagem se compensa pelo ganho de subsídios para reflexão sobre a matéria, e se ameniza com um procedimento coletivo, não individual, para a delimitação de quais trabalhos foram ou não considerados.

Ainda, o impacto sobre o resultado final é limitado, pois a ampla maioria dos textos analisados (81,25%) seguiu métodos não-discricionários, como descrito no Apêndice 1. Essa indicação específica – de quais textos foram selecionados conforme um dado método, e quais foram inseridos por via discricionária – mitiga o dano à sistematicidade e preserva a replicabilidade: o estudo pode ser reproduzido sem essas obras, ou na íntegra.

Assim, o *corpus* documental final abrange 32 publicações, listadas no Apêndice 1: 4 obras publicadas em anais de eventos, 17 artigos científicos, 1 monografia de conclusão de curso, 1 dissertação de mestrado, 3 notas técnicas e 6 relatórios. Após seleção, os subconjuntos 2 e 3 foram também analisados pelo formulário aplicado ao subconjunto 1.

4. Resultados

Os resultados da revisão sistemática da literatura selecionada foram organizados em quatro tópicos: o panorama do conceito de rastreabilidade, que reflete diferentes significados nas publicações; os contextos específicos, respectivamente, do Projeto de Lei nº 2630 de 2020 no Brasil, e das Regras de TI de 2021 na Índia; e aspectos tecnológicos, riscos e desafios da implementação da proposta de rastreabilidade de mensagens instantâneas.

4.1. A polissemia do conceito de rastreabilidade

A polissemia conceitual é um dos desafios mais elementares para o estudo da rastreabilidade. A norma ISO 9000 da Organização Internacional de Padrões, por exemplo, a define como "a habilidade de rastrear o histórico, aplicação ou localização de um objeto"[10]. Para produtos ou serviços o conceito pode se referir à origem de materiais e partes, a histórico do processamento e/ou a distribuição e localização após a entrega. Observa-se uma ausência de relação imediata do termo com o meio digital.

Rastreabilidade, portanto, não tem significado unívoco, consensual ou evidente de imediato no contexto das comunicações interpessoais digitais. Por isso, a literatura examinada mobiliza múltiplos significados, às vezes explicitamente enunciados, outras vezes deixados implícitos.

Uma das menções mais antigas ao termo na regulação de comunicações digitais está no documento de 2018 "Combater a desinformação em linha: uma estratégia europeia"[11], publicado pela Comissão Europeia. Mesmo sem traçar um conceito, descreve como pilar da disseminação de desinformação a "falta de transparência e rastreabilidade do ecossistema de plataformas existente". Ao viabilizar a "identificação da fonte da informação" ao longo do processo de divulgação, a rastreabilidade seria necessária para responsabilizar e promover a confiança na internet, contra a desinformação.[12] Ainda, a Comissão destaca que novas tecnologias garantidoras da integridade da informação, como *blockchain*, permitiriam implementar essa ferramenta.

O potencial das tecnologias de contabilidade distribuída foi similarmente enfatizado por uma parcela do *corpus* analisado. De teor mais exploratório, cogitam a aplicação da *blockchain* para o combate à desinformação e a promoção da responsabilização e prestação de contas no ambiente online. Nesses textos, a palavra rastreabilidade tem sentido expandido[13], incluindo ferramentas para identificar remetentes originais de mensagens, promover confiabilidade de bases de dados,[14] e rastrear conteúdos publicitários e noticiosos.[15] [16].

Nesse último caso, a rastreabilidade não figura como um mecanismo para facilitar a responsabilização dos envolvidos na disseminação de conteúdo desinformativo e/ou nocivo, mas como meio de maximizar a confiança de conteúdo considerado informativo. Esse ponto é ilustrado pela seguinte citação de Pinho Filho (ênfase nossa), que entende caber às plataformas digitais uma postura ativa no enfrentamento da desinformação:[17]

> *A nosso ver, é papel das plataformas, nesse sentido, atuar para reduzir drasticamente a visibilidade e o alcance de conteúdos enganosos ou fraudulentos enquanto incrementa a*

> **rastreabilidade de conteúdo confiável**, *incentivando os usuários a sempre buscarem informações adicionais que tragam contexto e enriquecimento de detalhes.*

Outras publicações tratam, ainda, a rastreabilidade de modo mais abstrato e geral, sem menção ao contexto específico da mensageria instantânea. Patrick Taillon defende, por exemplo, que, diante da excessiva dificuldade em se aferir a veracidade, a rastreabilidade da informação – teorizada em sentido amplo – seria "o principal mecanismo para assegurar a lisura do processo e oferecer transparência ao debate público" e no combate à desinformação.[18] A publicação, porém, direcionada especificamente para o contexto da legislação canadense vigente, não se aprofunda nos efeitos da implementação desse mecanismo, seja em termos jurídicos ou mesmo de segurança da informação.

Entre os textos analisados, o trabalho de Dos Santos e outros[19] foi pioneiro, no contexto brasileiro, em definir a rastreabilidade de mensagens instantâneas como a identificação do remetente original de certo conteúdo, e em considerá-la fundamental no combate à desinformação. Sua análise, porém, não tratou do mecanismo como um dever legal para plataformas de mensageria instantânea, mas como recurso para autoridades e pesquisadores. Na proposta, identificar os usuários originadores de conteúdos específicos viria da combinação entre métodos de análise computacional de redes e o acesso a metadados sobre os envios de arquivos associados a conteúdos desinformativos virais, durante investigações específicas, baseado nas normas legais já existentes.

O estudo pressupunha que o art. 15 do Marco Civil da Internet previa o dever de guarda desses metadados, sujeitos ao acesso pelas autoridades. Mas tal dispositivo só exige dos provedores de aplicações de internet a guarda de registros de acesso a aplicações, sem o dever de guardar dados propriamente sobre o uso dos serviços online, logo, sem metadados sobre o envio de arquivos.

À exceção dessa obra, os trabalhos dedicados à análise específica da rastreabilidade em mensageria instantânea baseiam-se nas Regras de TI de 2021 da Índia, no PL nº 2630/2020 do Brasil, ou em ambos. Por isso, os conceitos adotados refletiam a redação dessas propostas normativas.

Nesses trabalhos, portanto, **a rastreabilidade é compreendida como a capacidade de identificação do usuário originador de um conteúdo (no caso indiano) ou dos usuários que o tenham encaminhado e que se incluem em certos critérios normativamente determinados (no caso brasileiro)**. As próximas subseções apresentam as discussões sobre cada um desses contextos.

4.2. Brasil e o PL nº 2630, de 2020

A imprecisão do termo rastreabilidade não impediu o reconhecimento de algumas tendências para o âmbito das mensagens instantâneas. E à falta de uma previsão vigente, no Brasil a proposta inscrita no PL das Fake News foi o eixo em torno do qual se polarizaram as defesas e críticas.

A revisão sistemática da literatura selecionada permitiu identificar o contexto jurídico e político dos debates, e pontos comuns de controvérsia.

4.2.1. PL das Fake News e rastreabilidade de mensagens instantâneas

Em 30 de junho de 2020, o Senado Federal brasileiro aprovou o Projeto de Lei nº 2630, de 2020.[20] A proposta para "instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet" ficou conhecida como "PL das Fake News".[21] Entre as várias regras para alguns provedores de aplicações de Internet com mais de 2 milhões de usuários no Brasil, o PL previa o dever de as plataformas de mensagens instantâneas manterem registros dos envios de mensagens encaminhadas em massa.

Na Câmara dos Deputados, o texto foi analisado pelo Grupo de Trabalho para o aperfeiçoamento da legislação Brasileira referente à Liberdade, Responsabilidade e Transparência na Internet – GT NET[22]. Em 07 de dezembro de 2021, apresentou parecer pela aprovação de uma redação bem diferente daquela do Senado, sem propor a rastreabilidade de mensagens instantâneas.[23]

Não obstante, caso venha a ser aprovado pela Câmara, a proposta ainda precisará voltar ao Senado, a quem caberá confirmar as mudanças ou manter o texto de 2020. A rastreabilidade continua, assim, a merecer atenção.

Um ponto nebuloso é a origem, ou a entrada da proposta no projeto de lei. Em 2019, Dos Santos e outros viram como vantagens do WhatsApp para "estratégias criminosas": a) anonimizar a fonte de mensagens encaminhadas, b) oferecer criptografia; e c) dificultar o rastreamento da origem de conteúdos virais.[24] Como já dito, o estudo via a rastreabilidade de mensagens instantâneas como meio para se identificar o remetente original de um certo conteúdo, a fim de combater a desinformação, pela combinação da análise computacional de redes e do acesso a metadados sobre os envios de arquivos, à luz do Marco Civil.

Um ano depois, no Senado, durante a tramitação do PL 2630/2020, o autor do texto original, sen. Alessandro Vieira, "introduziu o polêmico artigo para rastrear a cadeia de encaminhamento de mensagens em serviços de mensageria privada",[25] como parte de uma proposta global de alteração do PL. A justificativa do Senador não mencionou esse artigo. Assim, sem uma motivação explícita, em 02 de junho de 2020, foi proposto o seguinte:

> *Art. 17. O provedor de aplicação que apresente funcionalidade reencaminhamento ou similar de conteúdos deve guardar os registros da cadeia de reencaminhamentos até sua origem, pelo prazo mínimo de 1 (um) ano, resguardada a privacidade do conteúdo das mensagens, podendo esses registros ser solicitados mediante ordem judicial nos termos da Seção IV da Lei 12.965 de 2014.*[26]

O texto do Relator Ângelo Coronel, aprovado no Senado, trocou "cadeia de reencaminhamentos até sua origem" por "encaminhamentos em massa":

> *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.*
>
> *§ 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.*
>
> *§ 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.*
>
> *§ 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).*
>
> *§ 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).*[27]

A previsão obrigaria esses provedores a manter por 3 meses os registros de mensagens que, no prazo de 15 dias, fossem enviadas por mais de 5 e recebidas por mais de mil usuários. Tais registros deveriam indicar remetente, data e horário de encaminhamento, e

o número total de destinatários da mensagem em questão. O acesso de terceiros exigiria autorização judicial, tanto para fins de investigação criminal, quanto para instrução de processo penal.

4.2.2. Controvérsias jurídicas

As controvérsias da proposta desse mecanismo vão de questões jurídicas mais amplas até aspectos pontuais da proteção de dados pessoais. Um eixo divisor de posicionamentos contra ou a favor da rastreabilidade de mensagens instantâneas no Brasil é a natureza pública ou privada desse serviço, e quais os direitos dos usuários dela decorrentes.

Essa perspectiva, aparentemente influenciada pela regulamentação dos meios de comunicação social tradicionais, é encontrada em Ribeiro, que aponta a finalidade – interpessoal ou viral – como fator distintivo para a proteção do sigilo do teor das comunicações: "quem envia um arquivo pode fazê-lo para fins de uma conversa interpessoal e, portanto, deve ter seus dados protegidos. Quem encaminha o arquivo tira-o do contexto privado e assim assume o risco de viralizá-lo".[28] Sem fontes, esse estudo narra que "Originalmente o WhatsApp foi concebido como uma ferramenta de comunicação interpessoal (um para um)",[29] mas sua natureza foi afetada por funcionalidades como "grupos, envio de mensagens para múltiplos usuários e encaminhamentos de mensagens". Também sem amparo em fontes, sustenta que essas funções preocupariam os proponentes do PL de Fake News, "porque elas permitem que um pequeno grupo opere uma cadeia de grupos e espalhe conteúdo criminoso para milhões de usuários". E reitera: "a decisão de implementar o encaminhamento de mensagens preservando a identidade dos intermediários não passou pelo mesmo processo de debate público".[30]

Os efeitos da rastreabilidade sobre a liberdade de expressão se evidenciam pela identificação das pessoas envolvidas na troca de mensagens. O Relator Especial da ONU para Liberdade de Expressão, ao tratar de criptografia e do anonimato em um contexto geral, defendeu que empresas forneçam, por padrão, as mais altas configurações de privacidade do usuário; e que Estados apenas editem leis que justifiquem restrições a ferramentas de criptografia e anonimato sob requisitos de excepcionalidade, necessidade, proporcionalidade e legitimidade do objetivo.[31] Mas no Brasil, conforme Pinho Filho, desde a Constituição Federal de 1891, a garantia de liberdade de expressão sempre veio acompanhada da vedação ao anonimato.[32]

Especificamente quanto à rastreabilidade de mensagens, Ribeiro sustenta que, do ponto de vista privado, o Whatsapp não oferece anonimato, de forma que a proteção de metadados "nunca foi uma preocupação";[33] e, tendo em vista o interesse público, "não debatemos o suficiente se o encaminhamento anônimo é desejável", por empoderar grupos subalternos, ou indesejável, por permitir "que um pequeno grupo de atores possa espalhar conteúdo criminoso para milhões de pessoas sem ser responsabilizado".[34] Nisso, alinha-se à visão (canadense) de Taillon,[35] de que o anonimato seria um dos aspectos da internet que ampliam a disseminação da desinformação.

A garantia jurídica mais desenvolvida na literatura é a proteção de dados pessoais. A propósito, a exigência do art 46 da Lei Geral de Proteção de Dados (de proteção contra qualquer forma de tratamento inadequado) foi elevada, desde a Emenda Constitucional 115, de 10 de fevereiro de 2022, ao patamar de direito constitucional, no inciso LXXIX do art. 5º da CF 1988.

Para Ribeiro e Lana e outros, exigir a guarda de dados não essenciais ao serviço infringe o princípio da minimização de dados previsto na LGPD e no Marco Civil[36], "abandonando o paradigma do *privacy-by-design* e inaugurando uma era de *surveillance-by-design*"[37]. Lana e outros criticam a criação de "uma gigantesca base de dados com metadados das interações interpessoais de todos aqueles que utilizam um determinado serviço de mensageria privada na Internet",[38] especialmente porque os requisitos "não limitam efetivamente a quantidade de dados a serem guardados pelos serviços de mensageria".[39] E, para Trindade, "Tal escrutínio iria afetar as redes sociais, fazendo com que armazenem ainda mais dados pessoais, o que vai justamente contra todo o trabalho exercido pela LGPD discutido anteriormente".[40]

Segundo Aguiar e outros, metadados entram na definição legal de dados pessoais e têm proteção jurídica, "na medida em que tornam uma pessoa identificada ou identificável",[41] sendo "tão ou talvez mais críticos que outros tipos de dados pessoais, como o conteúdo em si de mensagens".[42] Conforme Curzi e outros, na análise algorítmica e no cruzamento de dados simples, podem-se inferir muito, inclusive dados sensíveis: logo, não há dado insignificante.[43]

Para a Internet Society,[44] afora varredura pelo lado do cliente, usuário fantasma ou custódia de chaves, mesmo técnicas capazes de implementar a rastreabilidade sem afetar diretamente a criptografia poderiam trazer graves riscos específicos: assinaturas digitais dariam margem a ameaças à liberdade de expressão e exposição à falsidade ideológica, assédios e perseguição; e a análise de metadados poderia mapear grupos para extorsão, engenharia social e chantagem. Ao risco de se "transferir a culpa para inocentes"[45] (por não permitir encontrar a origem das mensagens, não ser imune a pistas falsas, nem distinguir usos comuns de ações nocivas, como campanhas de desinformação), Lana e outros adicionam que a obrigação de vigilância em massa maximiza o tratamento de dados pessoais e contraria a lógica do Marco Civil e da LGPD:[46]

> *(...) ao criar um sistema para supostamente combater a desinformação na era digital, o legislador brasileiro está criando um sistema de vigilância massiva que coloca direitos fundamentais, a ordem democrática e a própria economia digital em risco.*

Também Trindade cogita que essa ferramenta seria ilegal por ensejar requerimentos abusivos de informações pessoais e obrigar a manutenção de dados também daqueles que, "por razões legítimas ou involuntárias, participem de cadeias de compartilhamento de conteúdos".[47]

Aguiar e outros alegam que monitorar e guardar dados pessoais de todo mundo, mesmo sem acusação de algum ato ilícito, com "retenção preventiva indiscriminada e generalizante de metadados",[48] afeta desproporcionalmente direitos, liberdades e garantias constitucionais: presunção de inocência até o trânsito em julgado de sentença penal condenatória, sigilo das comunicações, e proteção de dados pessoais, objeto de decisões recentes do STF, "desde os casos de bloqueio do Whatsapp, até o caso IBGE".[49] Curzi e outros incluem o devido processo legal, diante de um "estado perene de vigilância preventiva que abarca muito mais pessoas do que efetivamente se pretende atingir".[50]

Por falta de definições precisas, há divergências técnicas entre a proposta legislativa e as suposições favoráveis na literatura. Afirmando que "seria possível rastrear uma mensagem sem violar os princípios de segurança"[51] e "sem comprometer a criptografia" de ponta a ponta,[52] Ribeiro pontua que a redação do art. 10 "aprovada pelo senado impõe ao WhatsApp a retenção de metadados de cada usuário que requisitou acesso a algum arquivo armazenado nos seus servidores".[53] Sem amparo em fontes, noticia que para os proponentes do PL das Fake News a "preocupação com a disseminação de conteúdos nocivos gira principalmente em torno do encaminhamento de arquivos de mídia (imagem, áudio, vídeo etc.)". Nessa chave, descreve e analisa apenas uma plataforma, em apenas uma funcionalidade, e parte da premissa de que a redação aprovada no Senado se limitaria ao monitoramento de quem acessou arquivos antes enviados:[54]

> *Como os metadados armazenados são dos que requisitaram acesso ao arquivo, o usuário que enviou-o ao servidor não terá seus dados expostos. Isso é desejável porque quem envia um arquivo pode fazê-lo para fins de uma conversa interpessoal e, portanto, deve ter seus dados protegidos. Quem encaminha o arquivo tira-o do contexto privado e assim assume o risco de viralizá-lo. Dessa forma, é ao mesmo tempo possível responsabilizar quem opera esquemas de disseminação de conteúdo criminoso e proteger a comunicação interpessoal.*

O texto do art. 10 não diferencia texto, som, imagem, vídeo ou qualquer mídia: nem mesmo cita arquivos, compartilhados ou armazenados. Trata do "envio de uma mesma mensagem" e prevê incidência ampla, sem distinções. Para os pesquisadores do Instituto de Tecnologia e Sociedade do Rio de Janeiro, "a rastreabilidade acaba exigindo um aumento considerável do fluxo de dados, sobrecarregando servidores e tornando o serviço mais lento e oneroso".[55]

4.3. Índia e as Regras de TI de 2021

Na análise do *corpus*, referências sobre a Índia foram recorrentes, quanto às chamadas Regras de TI,[56] [57] em vigor desde 2021. O contexto político, legal e judicial indiano se reflete na proposta de rastreabilidade dessa norma jurídica.

4.3.1. Criptografia na Índia: histórico legislativo e político

As Regras de TI chamam a atenção de ativistas e legisladores de diversos países. O quadro normativo hoje vigente na Índia muitas vezes serve em outros países de fomento argumentativo da rastreabilidade de comunicações cifradas. É o que ocorreu no Brasil, nas discussões do PL 2630/2020.

Mas as iniciativas regulatórias indianas contra a criptografia forte datam de vários anos. As tentativas iniciais de regular a criptografia no país também previam técnicas de rastreabilidade em serviços de mensageria instantânea criptografada. Em 2015, o governo da Índia tentou inserir esse mecanismo na legislação, com o Projeto de Política Nacional sobre Criptografia,[58] do Ministério da Eletrônica e Tecnologia da Informação.[59] O texto preliminar exigia a guarda, por 90 dias, de conteúdos cifrados enviados por usuários, e obrigava ao compartilhamento com órgãos investigativos, mediante requerimento.[60] Sob muitas críticas, o projeto foi cancelado dois dias depois de apresentado.[61]

Em 2018, o então Ministro da Eletrônica e Tecnologia da Informação, Ravi Shankar Prasad, chamou a atenção do Parlamento para o mau uso de redes sociais, o risco proveniente do compartilhamento de desinformações nesses meios, e a subsequente necessidade de regulação dessas plataformas.[62] No mesmo ano, o texto inicial do Projeto das Diretrizes para Intermediários,[63] proposto para substituir as diretrizes vigentes no país desde 2011,[64] foi submetido a consulta pública.[65]

A proposição foi a primeira a prever a rastreabilidade de usuários em plataformas digitais. A Seção 3(5), mais especificamente, determinava casos em que intermediários de internet deviam rastrear a autoria de conteúdos tidos por ilegais, com devida diligência:

> *3. Devida diligência a ser observada pelo intermediário – O intermediário deve observar a devida diligência no exercício de suas funções, nomeadamente:*
>
> *[...]*
>
> *(5) Quando exigido por ordem legal, o intermediário deverá, dentro de 72 horas da comunicação, fornecer as informações*

> *ou assistência conforme solicitado por qualquer agência governamental ou assistência relativa à segurança do Estado ou segurança cibernética; ou investigação ou detecção ou processo ou prevenção de ilícito(s); proteção ou segurança cibernética e assuntos relacionados ou a eles incidentais. Qualquer solicitação desse tipo pode ser feita por escrito ou por meio eletrônico, informando claramente o objetivo de buscar essas informações ou assistência. O intermediário deve permitir o rastreamento de tal originador de informações em sua plataforma, conforme exigido por agências governamentais que sejam legalmente autorizadas.*
>
> *[...]*
>
> *(9) O Intermediário deverá implementar ferramentas automatizadas baseadas em tecnologia ou mecanismos apropriados, com controles apropriados, para identificar e remover ou desabilitar proativamente o acesso público a informações ou conteúdos ilegais.*[66]

O Projeto foi submetido a rodadas de comentários[67] [68] e réplicas.[69] [70] Durante essas etapas, organizações e entidades da sociedade civil repetidamente apontaram abusividade e ilegalidade quanto à responsabilidade de intermediários de internet; e alegaram que as medidas causariam efeito inibidor nas liberdades individuais – em especial, a liberdade de expressão –, em razão do controle estatal desproporcional sobre os intermediários e, por consequência, sobre as comunicações interpessoais.[71]

Apesar disso, o projeto de 2018 foi incorporado à legislação indiana, na forma de uma norma subordinada[72] à Lei de Tecnologia da Informação,[73] de 2000.[74] O texto final denomina-se "Regras de Tecnologia da Informação (Diretrizes para Intermediários e Código de Ética para Mídias Digitais)",[75] de 2021 – comumente referenciado apenas como "Regras de TI".[76]

As Regras de TI mantiveram a rastreabilidade de comunicações apresentada no projeto de lei das Diretrizes de 2018. A lista de situações passíveis de requisições, contudo, foi ampliada:

> *4. Devida diligência adicional a ser observada por intermediários de mídia social significativos.*
>
> *(2) Um intermediário de mídia social significativo que preste serviços primariamente com a natureza de mensagens deve permitir a identificação do primeiro remetente das informações em seu recurso de computador, conforme exigido por uma ordem judicial*

> *emitida por um tribunal de jurisdição competente ou uma ordem emitida pela Autoridade Competente nos termos da seção 69 de acordo com as Regras de Tecnologia da Informação (Procedimento e Salvaguardas para interceptação, monitoramento e decifragem de informações), de 2009, que deve ser acompanhada de uma cópia dessas informações em formato eletrônico:*
>
> *Contanto que uma ordem seja emitida apenas para fins de prevenção, detecção, investigação, acusação ou punição de uma ofensa relacionada à soberania e integridade da Índia, à segurança do Estado, relações amistosas com Estados estrangeiros ou ordem pública, ou de incitação a um delito relacionado com os motivos anteriores ou em relação com estupro, material sexualmente explícito ou material de abuso sexual infantil, punível com prisão por um período não inferior a cinco anos:*
>
> *Contanto ainda que nenhuma ordem seja emitida nos casos em que outros meios menos intrusivos sejam eficazes na identificação do originador da informação:*
>
> *Contanto também que, no cumprimento de uma ordem de identificação do primeiro remetente, nenhum intermediário de mídia social significativo será obrigado a divulgar o conteúdo de qualquer mensagem eletrônica, qualquer outra informação relacionada ao primeiro remetente ou qualquer informação relacionada a seus outros usuários:*
>
> *Contanto também que, quando o primeiro originador de qualquer informação sobre o recurso informático de um intermediário estiver localizado fora do território da Índia, o primeiro originador dessa informação dentro do território da Índia será considerado o primeiro originador da informação para efeitos desta cláusula.*[77]

Para além dos esforços legislativos do país, em 2020, a Índia se uniu aos países da aliança *Five Eyes* para defender o fim das tecnologias protegidas por criptografia de ponta a ponta.[78] Impugnaram os desafios significativos para a segurança pública e demandaram mecanismos de acesso excepcional a comunicações e informações cifradas com esses algoritmos, como necessários à defesa de interesses estatais.

4.3.2. Regras de TI: aspectos jurídicos relevantes e críticas à normativa

Desde a abertura do Projeto das Diretrizes para Intermediários, em 2018, sociedade civil, ativistas por direitos digitais e as plataformas que operam na Índia criticam a abordagem do governo indiano sobre criptografia, em especial, nas comunicações instantâneas cifradas. A vigência das Regras de TI de 2021 manteve-se como objeto de ampla cobertura jornalística e acadêmica contrária.

Um dos principais aspectos apontados como problemáticos nas Regras de TI é sua contraposição ao precedente da Suprema Corte da Índia no caso K.S. Puttaswamy vs. União da Índia,[79] em 2017. De modo unânime, 9 juízes afirmaram a privacidade como direito fundamental protegido pelas garantias constitucionais indianas. A decisão ficou popularmente conhecida como "o veredito do direito à privacidade". No julgamento, estipulou-se um teste para avaliar se alguma medida poderia se sobressair ao direito à privacidade: a quebra dessa proteção constitucional poderia se justificar mediante a análise da legalidade, da necessidade e da proporcionalidade. Críticas às Regras de TI, nessa linha, apontam que a previsão legal de rastreabilidade das comunicações não passa no teste triplo, logo, viola o "veredito do direito à privacidade".[80]

Primeiramente, quanto à legalidade dos novos dispositivos, argumenta-se que a legislação indiana não apresenta mecanismos vigentes válidos para justificar a rastreabilidade. Nesse aspecto, também se critica a insubordinação indevida das Regras de TI à Lei de Tecnologia da Informação de 2000, conforme será melhor elaborado abaixo.

Ainda, aponta-se a afronta à expectativa de proporcionalidade inerente ao teste triplo do caso Puttaswamy. Pela Seção 4(2) das Regras de TI, as ordens de rastreabilidade não podem ser determinadas se houver meios menos intrusivos para se obterem as informações pretendidas por órgãos investigativos. Mas a omissão do dispositivo em exemplificar meios menos intrusivos, que poderiam anteceder às ordens de rastreabilidade, enseja imediata aplicabilidade de meios mais intrusivos e danosos.[81]

Além do respeito ao precedente da Suprema Corte, a legalidade mesma das Regras de TI tem sido questionada.[82] Por ser norma subordinada, com fulcro nas Seções 69(A), 79 e 87(2)(zg) da Lei de Tecnologia da Informação de 2000, ela deveria observar os limites impostos por esses dispositivos legais e só regular meios para sua prática. O processo legislativo essencial, que pode criar novos parâmetros legais mediante leis ordinárias, compete ao Poder Legislativo.[83]

Mas a Lei de Tecnologia da Informação não prevê possíveis obrigações de rastreabilidade. A Seção 69(A) dispõe sobre a possibilidade de bloqueio de plataformas online no país, mas não abre espaço para impor sanções diversas das previstas; já a Seção 79 prevê casos em que intermediários podem se eximir de responsabilidade se cumprirem certos pressupostos legais de auditoria de suas atividades; a Seção 87(2)(zg), por fim, aborda

a possibilidade de criação de normas subordinadas para regular alguns dos requisitos para intermediários da Seção 79 – mas sem autorizar a criação de medidas adicionais às da Lei.

Quanto à ilegalidade das Regras de TI, fala-se[84] do precedente do caso Indian Express Newspapers vs. União da Índia[85]. Nele, a Suprema Corte da Índia decidiu que representa uma arbitrariedade do Executivo exercer atribuições do Poder Legislativo e criar normas subordinadas com conteúdo normativo que deveria ser aprovado na forma de lei ordinária.

Também na seara jurídica, critica-se a permissão legal para que ordens de compartilhamento dos dados de usuários possam ser emitidas por "qualquer autoridade competente", permitindo arbitrariedades do Poder Executivo. Mais especificamente, há críticas quanto à falta de salvaguardas procedimentais; de supervisão judicial para a emissão dessas ordens; e de transparência, pois as ordens de compartilhamento não são divulgadas para escrutínio público.[86]

Além das críticas formais e jurídicas às Regras de TI, também se levantam questões sobre a efetividade de suas previsões. As diversas propostas Foram submetidas, de implementação prática dos mecanismos de rastreabilidade, são consideradas ainda problemáticas para a proteção da privacidade dos usuários indianos,[87] [88] conforme detalhado no tópico 5.4.

Sidharth Narayan e Amol Kulkarni[89] apontam repercussões consumeristas relevantes da inserção de ferramentas de rastreabilidade em plataformas de mensageria instantânea. Segundo eles, a privacidade das comunicações interpessoais é um dos principais aspectos de atração para o uso de serviços de mensageria com criptografia de ponta a ponta. Portanto, o enfraquecimento da privacidade nesses sistemas – ou mesmo a percepção de a segurança estar em risco – pode levar a uma redução do uso desses aplicativos pela população, por receio de que suas conversas estejam comprometidas.

4.4. Modos de implementação, riscos e desafios

A rastreabilidade de mensagens instantâneas consiste num dever regulatório que se pretende impor às plataformas, e não numa funcionalidade já existente nos sistemas de comunicação instantânea. Os efeitos tecnológicos da adequação a esse requisito se tornaram uma parte sensível da controvérsia. Debate-se intensamente quais os métodos disponíveis para sua concretização, sua eficácia para a finalidade pretendida, os riscos de segurança decorrentes e a compatibilidade da medida com os atributos da criptografia de ponta a ponta.

A subseção 6.4.1. lista os métodos citados no *corpus* para a implementação da rastreabilidade. A subseção 6.4.2. discute os riscos associados às propostas.

4.4.1. Métodos para implementação da rastreabilidade

- **Atribuição por assinatura digital.** Teve notoriedade na Índia após ser apresentada ao Tribunal Superior de Madras pelo professor de ciência da computação no Instituto Indiano de Tecnologia, V. Kamakoti.[90] O método vincula um dado identificador dos usuários às mensagens por eles enviadas. A identificação, similar a uma assinatura digital, poderia ser visível a todos destinatários participantes da cadeia de compartilhamento ou, em alternativa, ser informada apenas a autoridades competentes, sob requisição. Neste caso, a mensagem carregaria a assinatura cifrada do originador, e essa apenas poderia ser decifrada pelo intermediário, que manteria um banco de chaves privadas. Como essa base de dados seria sensível, o Grupo de Políticas Públicas para o Acesso a Informação sugere em nota técnica a possibilidade de armazenamento distribuído das chaves, porém não detalha como isso seria operacionalizado.[91]

- **Verificação por *hashing*.** Defendida pelo coordenador do grupo de direito cibernético e segurança eletrônica do Ministério da Eletrônica e Tecnologia da Informação indiano, Rakesh Maheshwari,[92] a proposta sugere atribuir a cada mensagem ou arquivo enviado um identificador alfanumérico (*hash*). Caberia ao intermediário manter um banco de dados que permitisse, via identificador do conteúdo, atender a uma requisição da identificação do usuário originador.

- **Inferência a partir da análise de metadados.** Em seminário fechado realizado pela Internet Society e a Medianama[93] com um grupo internacional de especialistas em tecnologia e cibersegurança, examinou-se a possibilidade de uso de metadados sobre mensagens virais para a identificação retroativa da cadeia de mensagens e, nessa trilha, a determinação de seu originador. Em vez de se atribuir um dado novo – *hash* ou assinatura – ao conteúdo disseminado, o intermediário poderia inferir a trajetória via análise de metadados particulares relativos à própria mensagem viral, em especial o tamanho. Implementar essa estratégia seria mais fácil para arquivos de mídia. E a análise de metadados poderia favorecer a criação de grafos sociais de comunicação no contexto de redes específicas, o que poderia amparar as autoridades em investigações.

- **Franqueamento de mensagens.** Um tipo de esquemas de denúncia por usuários, adequados para serviços com criptografia de ponta a ponta, conforme descrito pelo *Center For Democracy & Technology*.[94] A própria denúncia, por alguém que participa da conversa e escolhe revelar a mensagem ao provedor, é criptografada, e se mantém confidencial, íntegra, autêntica e não-repudiável. Assim, sem interferir nas chaves originais ou criar portas clandestinas, pode-se vincular o remetente ao conteúdo enviado e responsabilizar por mensagens de ódio e assédio, desinformação, material de abuso sexual de crianças, propaganda terrorista, spam, etc. Esse uso da criptografia também permite ao denunciante se demonstrar destinatário, e não remetente, de algum conteúdo.

4.4.2. Os riscos das propostas

Nos textos examinados, as implicações das propostas de assinatura digital, *hashing* e análise de metadados em geral foram reputadas nocivas quanto à eficiência e à segurança da informação. Por outro lado, o franqueamento de mensagens, ao exigir por lei "visibilidade a uma informação que antes era invisível"[95] e, assim, permitir o rastreamento, é criticado por Lana e outros como solução não testada, que desconsidera opções menos gravosas, e "tecnicamente falha e ineficiente, sendo relativamente fácil de burlar ou, até mesmo, transferir a culpa para inocentes".[96]

Assim, um dos aspectos mais incisivamente criticados nos textos examinados foi a eficácia das propostas. Ao considerar os métodos de atribuição por assinatura e a inferência a partir da análise de metadados, os especialistas consultados pela Internet Society e Medianama consideraram que ambos os métodos não poderiam garantir a identificação de responsáveis pelo conteúdo viral. No primeiro, agentes maliciosos poderiam usar versões alteradas do app para modificar a assinatura e incriminar inocentes. Além disso, ambos os métodos desconsiderariam o caráter multi-plataforma da desinformação: um conteúdo viral pode ter sido recebido na plataforma A pelo primeiro usuário a compartilhá-lo na plataforma B, dificultando atribuir ao usuário na plataforma B a autoria ou responsabilidade pelo conteúdo.

Similarmente, pesquisadores do *Center for Democracy and Technology (CDT)* viram nos métodos de verificação por *hashing* e atribuição por assinatura uma falha desde a base conceitual, pela indeterminação intrínseca do conceito de "originador". [97] Mas para integrantes do Instituto de Tecnologia e Sociedade do Rio de Janeiro, a rastreabilidade de mensagens instantâneas não separaria usos comuns de campanhas de desinformação, nem seria à prova de pistas falsas.

Em nota técnica sobre o PL 2630/2020, os pesquisadores da Associação Data Privacy Brasil de Pesquisa também apontam a possibilidade de serem desenvolvidas soluções pouco custosas, por agente maliciosos, para burlar os requisitos legais da retenção de dados. Bastaria replicar o conteúdo de outra forma, que não pelo encaminhamento, e os dados não seriam retidos: "supondo que fosse tecnicamente e juridicamente possível o rastreamento, **não existe comprovação, estudo, ou caso em nenhuma parte do mundo em que o método se demonstrou eficaz no combate à desinformação**"[98]. Esse limite foi notado já por V. Kamakoti, no documento de apresentação de seus métodos: um ator interessado em disseminar um conteúdo sem rastros poderia capturar sua tela, ou só copiar e colar a mensagem antes de enviá-la.[99]

Muito problematizados pela literatura, os riscos para a segurança seriam altos, afetando a proteção de dados pessoais. Na atribuição por assinatura e na verificação por *hashing*, o intermediário detentor do banco de chaves ou *hashes* se tornaria alvo de ataques cibernéticos e seu comprometimento poderia deixar os usuários vulneráveis a "falsidade

ideológica, assédio e perseguição".[100] Para os pesquisadores do CDT, esse problema é fundamental:

> *"a rastreabilidade como um conceito não é consistente com as garantias de privacidade para sistemas com criptografia de ponta a ponta; e que corrigir problemas de design nesses exemplos falhos não resolverá essa tensão inerente".*[101]

Ao fornecer a terceiros o acesso a informações sobre toda a cadeia de encaminhamento, a rastreabilidade compromete a confidencialidade das interações, um atributo cerne da criptografia. Essa perspectiva se alinha à de Pereira e outros, em cujo estudo, sobre as percepções de profissionais envolvidos no debate público, "mecanismos de rastreabilidade de mensagens privadas encaminhadas - a exemplo do PL 2630" foram apontados como ameaça à criptografia forte.[102] Mesmo sem gestão de chaves ou acesso ao algoritmo, quaisquer afetações aos atributos próprios da criptografia, inclusive indiretas, equivalem, em princípio, a quebrá-la.

Por fim, em vários textos[103,104,105,106,107] se aponta que a rastreabilidade promove vigilantismo, em prejuízo à liberdade de expressão de usuários; e contraria o princípio da minimização da coleta de dados pessoais ao necessário para se cumrprir a finalidade, inerente ao princípio da necessidade, e afirmado nos padrões internacionais de proteção e na própria LGPD.

4.4.3. Rastreabilidade: entre o ideal proposto e a inviabilidade prática

Os resultados deste estudo sugerem que a associação da rastreabilidade às mensagens instantâneas não foi impulsionada por um amplo debate técnico e científica sobre mecanismos de combate à desinformação e sua eficiência. Pelo contrário: excetuada uma das obras analisadas,[108] a literatura se mostrou amplamente reativa a propostas e atos normativos de formuladores de políticas públicas, a exemplo da Comissão Europeia, do Poder Legislativo brasileiro e do Ministério da Eletrônica e Tecnologia da Informação da Índia. Nesse sentido, as conclusões desta revisão sistemática subsidiam o observado pela equipe do Center for Democracy and Technology: "A demanda por rastreabilidade entre os governos é frequentemente baseada em propostas politicamente motivadas com pouca ou nenhuma orientação técnica em termos de viabilidade".[109]

Não surpreende, portanto, que parte significativa da argumentação encontrada nos textos analisados tenha se dedicado a examinar os contextos brasileiro e indiano e a indicar os riscos e problemáticas suscitados pelas propostas de rastreabilidade encontradas em ambos os contextos.

No Brasil, até o final de abril de 2022, as previsões de rastreabilidade previstas no texto do PL 2630/2020 aprovado pelo Senado foram removidas da redação substitutiva

agora em análise na Câmara dos Deputados. Esse cenário decorreu de longos debates e intensas críticas, provenientes da sociedade civil e da comunidade técnico-científica, em meio a um processo de tramitação obtuso e demasiadamente célere, tendo em vista a complexidade técnica e as possíveis repercussões sociais. Todavia, nada foi definido. Tanto na Câmara dos Deputados quanto no Senado Federal a proposta ainda pode vir a ser reapresentada, nos mesmo termos de junho de 2020, ou alterada, o que justifica a pertinência da análise de impactos e riscos.

No texto do Senado, as obrigações de rastreabilidade incluíam a identificação de toda a cadeia de compartilhamento de uma mensagem instantânea encaminhada em massa. Esses termos abrangentes impõem riscos significativos e reduzem a segurança de serviços protegidos por criptografia – o que em si representa uma quebra com os princípios e garantias de privacidade, segurança e proteção de dados protegidos por criptografia.

Já na Índia, o fato de as previsões de rastreabilidade das Regras de TI estarem em vigor representa não apenas um risco para a população do país, mas também um ambiente factual de redução da segurança garantida por técnicas criptográficas. Além da falta de definição precisa das soluções tecnológicas esperadas dos provedores de aplicações afetados pelas medidas de rastreabilidade, os argumentos sobre a legitimidade da legislação subordinada através da qual as Regras de TI foram implementadas representa um alerta para possíveis abusos de poder pelo Executivo indiano. Não à toa, a literatura voltada a analisar a normativa indiana de 2020 superou as fronteiras do país e alcançou uma escala global, demarcando o início aos atuais debates sobre a viabilidade e a eficácia do uso da rastreabilidade de conteúdo cifrado como uma alternativa à inserção de mecanismos de acesso excepcional em algoritmos criptográficos.

Ainda, constatou-se que as poucas análises dos métodos disponíveis para implementação das proposições regulatórias a consideravam ineficiente para os propósitos almejados e problemática quanto aos riscos de segurança gerados. As diferentes metodologias analisadas (verificação por *hashing*, inferência por metadados e assinaturas digitais) foram consideradas facilmente burláveis, ilustrando um problema conceitual mais amplo das propostas: a desconsideração do caráter multiplataforma da desinformação e a consequente ambiguidade do conceito de “originador”.

Ademais, as propostas foram consideradas redutoras da segurança de todos os usuários do sistema, uma vez que compeliriam as plataformas à retenção de grandes bases de dados altamente atraentes para atacantes maliciosos. Em sentido similar, a rastreabilidade foi tomada como antitética às garantias de privacidade e proteção de dados pessoais características dos principais padrões nacionais e internacionais relativos à matéria. Tais soluções estariam identificadas com uma lógica de monitoramento massivo que contrário ao princípio da necessidade, afirmado na Lei Geral de Proteção de Dados, que limita o tratamento dos dados ao mínimo necessário para o cumprimento de sua finalidade. Além disso, tal vigilantismo interferiria na liberdade de expressão

dos usuários do sistema, que poderiam se refrear de compartilhar conteúdos por temer o monitoramento e, portanto, teriam seu livre desenvolvimento da personalidade impactado.

5. Conclusão

O presente trabalho evidenciou como a literatura tem discutido a rastreabilidade de mensagens instantâneas. A fim de contribuir com subsídios para a formação de um entendimento fático da matéria e para uma avaliação mais qualificada das propostas legislativas a ela relacionadas, foram analisadas 32 publicações, a partir de quatro eixos: o conceito de rastreabilidade, o PL nº 2630/2020 no Brasil, as Regras de TI na Índia e o os modos de implementação da rastreabilidade e suas consequências.

O primeiro aspecto notório é a própria conceituação de rastreabilidade de mensagens instantâneas. Mesmo no processo de seleção, quando parcela significativa das referências resultantes das buscas em bases de dados acadêmicas oferecia resultados tematicamente impertinentes aos objetivos deste projeto, ficou evidenciada a ausência de uma conotação única, consensual ou inconteste na bibliografia analisada. Isoladamente, a "rastreabilidade" é um termo mais associado à produção e a sistemas de gestão de qualidade, com o sentido mais amplo definido na norma ISO 9000: "a habilidade de rastrear o histórico, aplicação ou localização de um objeto", tais como gado, medicamentos, alimentos industrializados, matérias primas, etc.

No Brasil, a previsão de rastreabilidade aprovada no Senado Federal incluía permitir identificar toda a cadeia de compartilhamento de uma mensagem instantânea encaminhada em massa. A redação imprecisa do mecanismo afronta a criptografia forte de serviços de comunicação online, por reduzir a privacidade, segurança e proteção de dados que se busca proteger através do uso da tecnologia. Embora pareça ter sido descartada pela Câmara dos Deputados, ao final de abril de 2022, a proposta ainda pode retornar ao debate, nos mesmo termos de junho de 2020, ou alterada.

Também na Índia, a rastreabilidade nas Regras de TI vigentes coloca em risco o povo e reduz a segurança da criptografia. A falta de precisão na definição da tecnologia e a possibilidade de abuso de poder por parte do Executivo levou o debate nacional a uma escala global.

Em ambos os contextos, as poucas análises dos métodos disponíveis indicam ineficiência para os propósitos almejados, dada a facilidade de burlar, além de riscos de segurança com a retenção excessiva de dados, redução de direitos como liberdade de expressão, vigilância em massa, e ambiguidade do conceito de originador.

A conclusão desta análise aponta que, de acordo com a literatura analisada, as obrigações de rastreabilidade – embora não necessariamente envolvam uma quebra literal de

algoritmos criptográficos, como é o caso dos mecanismos de acesso excepcional – violam prerrogativas fundamentais para o devido funcionamento de sistemas de segurança baseados em criptografia. Evidencia, ainda, que os esforços legislativos para criação dessas regras não encontram a devida fundamentação e análises de eficácia e viabilidade técnica na literatura, que possibilitem sua implementação. Por fim, ilustra a necessidade de que avanços normativos sobre matérias tão delicadas sejam construídos com base no devido diálogo entre os diversos setores da sociedade e na condução de minuciosas análises de risco.

Ao longo do presente estudo, foi realizada uma revisão bibliográfica extensiva sobre os debates que permeiam as previsões legais de rastreabilidade de comunicações cifradas, bem como suas repercussões sociais, jurídicas e políticas. Espera-se que a análise realizada possa ser utilizada como base para o aprofundamento das discussões em trabalhos futuros.

Notas

1 Uma discussão em detalhes sobre os diversos aspectos pertinentes e as percepções quanto às propostas de inserção de mecanismos de acesso excepcional em ambientes com criptografia foi objeto de um estudo prévio conduzido pelo IRIS (PEREIRA, 2021). PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 19 de abril de 2022.

2 SCHULZE, M. Clipper meets Apple vs. FBI – a comparison of the cryptography discourses from 1993 and 2016. Media and Communication, v. 5, n. 1, p. 54-62, 22 mar. 2017.

3 REUTERS. 'Five Eyes' security alliance calls for access to encrypted material. Reuters, 30 jul. 2019. Disponível em: https://www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199. Acesso em: 28 abr. 2022.

4 Ver DONEDA, Danilo; MACHADO, Diego (orgs.). A criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2020.

5 GALVÃO, Maria C.; RICARTE, Ivan L. M. Revisão sistemática da literatura: conceituação, produção e publicação. Logeion: Filosofia da Informação, [S.l.] , v. 6, n. 1, p. 57 - 73, set. 2019. P. 58. 7 - 73. Disponível em: http://revista.ibict.br/fiinf/article/view/4835. Acesso em: 10 jun. 2021.

6 SAMPAIO, R. F.; MANCINI, M. C. Estudos de Revisão Sistemática: um guia para síntese criteriosa da evidência científica. Revista Brasileira de Fisioterapia, São Carlos, v. 11, n. 1., p. 83-89, 2007. p. 84.

7 Scopus. https://www.scopus.com/search/form.uri?display=basic#.

8 Google Acadêmico. http://scholar.google.com.br/.

9 Para uma discussão sobre os diferentes sentidos possíveis dos termos disinformation e disinformation, ver WARDLE, C. and DERAKHSHAN, H. Information Disorder: Toward an interdisciplinary framework for research and policymaking. Strasbourg Cedex: Council of Europe, 2017. Disponível em: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html. Acesso em 26 abr. 2022.

10 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO 9000: Sistemas de gestão da qualidade - Fundamentos e vocabulário. Rio de Janeiro:

ABNT, 2015. p. 23

11 COMISSÃO EUROPEIA. Comunicação da comissão ao parlamento europeu, ao conselho, ao comitê econômico e social europeu e ao comitê das regiões: combater a desinformação em linha: uma estratégia europeia. Bruxelas, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0236. Acesso em: 17 abr; 2022.

12 PIELEMEIER, Jason. Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?. Utah L. Rev., 2020, 917.

13 PAPI, Fernando G.; HÜBNER, Jomi Fred; DE BRITO, Maiquel. Instrumenting Accountability in MAS with Blockchain. In: CARe-MAS@ PRIMA. 2017. p. 20-34.

14 DO VAL, Ronaldo Borges; VIANA, Thamirys Dias; GOUVEIA, Luis Borges. O uso de Blockchain na identificação de Fake News: ferramentas de apoio tecnológico para o combate à desinformação. Brazilian Journal of Business, 2021, 3.3: 2726-2742.

15 MARBOUH, D. et al., Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. Arabian Journal for Science and Engineering, v. 45, n. 12, 2020. pp. 9895-9911.

16 FRAGA-LAMAS, P., FERNANDEZ-CARAMES, T.M. Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. IT Professional. 22(2),9049288, 2020. pp. 53-59.

17 PINHO FILHO, José Célio Belém de. Desinformação e regulação de redes sociais digitais. 2021. 170 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021. P. 67. Disponível em https://repositorio.idp.edu.br//handle/123456789/3391.

18 TAILLON, Patrick. From veracity to traceability: A new Canadian legal framework for deliberative referenda. IN: BAUME, Sandrine; BOILLET, Véronique; MARTENET, Vincent (eds.) Misinformation in Referenda. Routledge, 2020. p. 257-280.

19 DOS SANTOS, João Guilherme Bastos, et al. WhatsApp, política mobile e desinformação: a hidra nas eleições presidenciais de 2018. Comunicação & Sociedade, 2019, 41.2: 307-334.

20 BRASIL. Congresso Nacional. Projeto de Lei nº 2630, de 2020 (Senador Alessandro Vieira - CIDADANIA/SE). Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Congresso Nacional [Congresso Nacional / Matérias Legislativas / Matérias Bicamerais], 13 Mai. 2020. Disponível em: https://www.

congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-2630-2020. Acesso em: 31 Mar. 2022.

21 AGÊNCIA SENADO. Senado aprova projeto de combate a notícias falsas; texto vai à Câmara. Senado Federal [Senado Notícias / Matérias / Plenário], 30/06/2020 21h27; atu. 23h10. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/06/30/aprovado-projeto-de-combate-a-noticias-falsas. Acesso em: 30 Mar. 2022.

22 BRASIL. Câmara dos Deputados. Aperfeiçoamento da Legislação Brasileira - Internet. Câmara dos Deputados [Início / Atividade Legislativa / Comissões / Grupos de trabalho / 56ª Legislatura (2019-2023) / Esta página], 23 Jun. 2020. Última Atualização: 23/02/2022 20:59:33. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/aperfeicoamento-da-legislacao-brasileira-internet. Acesso em: 30 mar. 2022.

23 AGÊNCIA CÂMARA DE NOTÍCIAS; MUGNATTO, Sílvia. Grupo da Câmara conclui votação de relatório sobre combate às fake news. Portal da Câmara dos Deputados [Início / Comunicação / Notícias / Ciência, Tecnologia e Comunicações], 08 Dez. 2021, 12:18. Disponível em: https://www.camara.leg.br/noticias/836267-GRUPO-DA-CAMARA-CONCLUI-VOTACAO-DE-RELATORIO-SOBRE-COMBATE-AS-FAKE-NEWS. Acesso em: 30 Mar. 2022.

24 DOS SANTOS, João Guilherme Bastos e outros. WhatsApp, política mobile e desinformação: a hidra nas eleições presidenciais de 2018. Comunicação & Sociedade, 2019, 41.2: 307-334. P. 321.

25 RODRIGUES, T. M.; BONONE, L.; MIELLI, R. DESINFORMAÇÃO E CRISE DA DEMOCRACIA NO BRASIL: é possível regular fake news?. Confluências | Revista Interdisciplinar de Sociologia e Direito, v. 22, n. 3, p. 30-52, 2 dez. 2020. P. 45.

26 BRASIL. Senado Federal. Emenda Substitutiva Global nº 55/PLEN (ao PL nº 2.630, de 2020). Senador Alessandro Vieira (CIDADANIA/SE). Brasília, Senado Federal, 02 Jun. 2020. (P. 7) Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8117352&disposition=inline. Acesso em: 31 Mar. 2022.

27 BRASIL. Câmara dos Deputados. Inteiro Teor. Projeto de Lei nº 2.630, de 2020 (Senado Federal - Alessandro Vieira - CIDADANIA/SE). Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Apresentação: 03/07/2020. Câmara dos Deputados [Página Inicial / Atividade Legislativa / Projetos de Lei e Outras Proposições / PL 2630/2020]. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01a0of2nobwcps1ftk5qmn0dt3263717022.node0?codteor=1909983&filename=PL+2630/2020. Acesso em: 31 Mar. 2022.

28 RIBEIRO, Márcio Moretto. Nota Técnica 10 – Rastreamento de mensagens virais

no WhatsApp. Monitor do Debate Político no Meio Digital. Grupo de Políticas Públicas para o Acesso à Informação. São Paulo: Universidade de São Paulo, 2020. P. 5. Disponível em https://www.monitordigital.org/2020/08/17/nota-tecnica-10/.

29 Idem, P. 3.

30 Idem, P. 5.

31 UN. Human Rights Council. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; Secretariat. Encryption and anonymity follow-up report: note / by the Secretariat (A/HRC/38/35/Add.5). Genebra: UN, 13 July 2018. 18 p. Disponível em https://digitallibrary.un.org/record/1638475.

32 Apenas em 1937 não houve proibição expressa ao anonimato, mas o art. 122 era literal quanto à possibilidade de censura prévia em favor da segurança nacional, da moral e dos bons costumes. Ver PINHO FILHO, José Célio Belém de. Desinformação e regulação de redes sociais digitais. 2021. 170 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021. https://repositorio.idp.edu.br//handle/123456789/3391. P. 28-34.

33 RIBEIRO, Márcio Moretto. Nota Técnica 10 – Rastreamento de mensagens virais no WhatsApp. Monitor do Debate Político no Meio Digital. Grupo de Políticas Públicas para o Acesso à Informação. São Paulo: Universidade de São Paulo, 2020. P. 6. Disponível em https://www.monitordigital.org/2020/08/17/nota-tecnica-10/.

34 Idem, Ibidem.

35 TAILLON, Patrick. From veracity to traceability: A new Canadian legal framework for deliberative referenda. IN: BAUME, Sandrine; BOILLET, Véronique; MARTENET, Vincent (eds.) Misinformation in Referenda. Routledge, 2020. p. 257-280.

36 LANA, Alice de Perdigão; PERRONE, Christian; ARCHEGAS, João Victor. Rastreabilidade de mensagens instantâneas e vigilância em massa. Instituto de Tecnologia e Sociedade – ITS, 16 jul. 2021. 28 p. Disponível em https://itsrio.org/pt/publicacoes/rastreabilidade-de-mensagens-instantaneas-e-vigilancia-em-massa-pl-2630-2020/. P. 24.

37 Idem, p. 28.

38 Idem, p. 18.

39 Idem, p. 19.

40 TRINDADE, Henrique de Oliveira. Elementos para uma discussão acerca do papel do direito no avanço digital e em suas implicações na crise da democracia. Monografia de Conclusão de Curso (Bacharelado em Direito). Universidade Federal de Juiz de Fora, 2021. P. 38. Disponível em https://repositorio.ufjf.br/jspui/handle/ufjf/12831.

41 AGUIAR, Thaís; BIONI, Bruno; FAVARO, Iasmine; KITAYAMA, Marina; RIELLI, Mariana; VERGILI, Gabriela; ZANATTA, Rafael. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís; BIONI, Bruno; MESQUITA, Hana; PIGATTO, Jaqueline; VERGILI, Gabriela. p. 34.

42 Idem, p. 15.

43 CURZI, Yasmin. ZINGALES, Nicolo. GASPAR, Walter. LEITÃO, Clara. COUTO, Natália. REBELO, Leandro. OLIVEIRA, Maria Eduarda. Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2630/2020. Rio de Janeiro: FGV Direito Rio, 2021. pp. 13-16. P. 15.

44 INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. Internet Society, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india. Acesso em: 31 mar. 2022.

45 LANA, Alice de Perdigão; PERRONE, Christian; ARCHEGAS, João Victor. Rastreabilidade de mensagens instantâneas e vigilância em massa. Instituto de Tecnologia e Sociedade – ITS, 16 jul. 2021. 28 p. Disponível em https://itsrio.org/pt/publicacoes/rastreabilidade-de-mensagens-instantaneas-e-vigilancia-em-massa-pl-2630-2020/. p. 28.

46 Idem, p. 23.

47 TRINDADE, Henrique de Oliveira. Elementos para uma discussão acerca do papel do direito no avanço digital e em suas implicações na crise da democracia. Monografia de Conclusão de Curso (Bacharelado em Direito). Universidade Federal de Juiz de Fora, 2021.

48 AGUIAR, Thaís; BIONI, Bruno; FAVARO, Iasmine; KITAYAMA, Marina; RIELLI, Mariana; VERGILI, Gabriela; ZANATTA, Rafael. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís; BIONI, Bruno; MESQUITA, Hana; PIGATTO, Jaqueline; VERGILI, Gabriela. Pp. 8-9.

49 Idem, p. 9.

50 CURZI, Yasmin. ZINGALES, Nicolo. GASPAR, Walter. LEITÃO, Clara. COUTO, Natália. REBELO, Leandro. OLIVEIRA, Maria Eduarda. Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2630/2020. Rio de Janeiro: FGV Direito Rio, 2021. pp. 13-16. P. 14.

51 RIBEIRO, Márcio Moretto. Nota Técnica 10 – Rastreamento de mensagens virais no WhatsApp. Monitor do Debate Político no Meio Digital. Grupo de Políticas Públicas para o Acesso à Informação. São Paulo: Universidade de São Paulo, 2020. P. 6. Disponível em https://www.monitordigital.org/2020/08/17/nota-tecnica-10/.

52 Idem, Ibidem.

53 Idem, Ibidem.

54 Idem, p. 5.

55 LANA, Alice de Perdigão; PERRONE, Christian; ARCHEGAS, João Victor. Rastreabilidade de mensagens instantâneas e vigilância em massa. Instituto de Tecnologia e Sociedade – ITS, 16 de julho de 2021. 28 p. Disponível em https://itsrio.org/pt/publicacoes/rastreabilidade-de-mensagens-instantaneas-e-vigilancia-em-massa-pl-2630-2020/. P. 25.

56 Tradução livre de “IT Rules”.

57 INDIA. Ministry of Electronics and Information Technology. The Information Technology (Intermediary Guideline and Digital Media Ethics Code) Rules, 2021. Disponível em https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

58 Tradução livre de “Draft National Encryption Policy”.

59 INDIA. Ministry of Electronics and Information Technology. Draft National Encryption Policy. Disponível em https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf.

60 Idem. Seção IV, 4.

61 INDIA. Ministry of Electronics and Information Technology. Note on withdrawal of the Draft National Encryption Policy. Disponível em: https://www.meity.gov.in/writereaddata/files/national-encryption-policy-govt_0.pdf.

62 SANSAD TV. Minister Ravi Shankar Prasad’s remarks | Calling Attention on misuse of social media. YouTube, 26 jul. 2018. Disponível em https://www.youtube.com/watch?v=aU1m2O7We6E.

63 Tradução livre de “Draft on Intermediary Guidelines”.

64 INDIA. Ministry of Electronics and Information Technology. Information Technology (Intermediaries Guidelines) Rules, 2011. Disponível em: https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf.

65 INDIA. Ministry of Electronics and Information Technology. The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018. Disponível em https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

66 Tradução livre de: “3. Due diligence to be observed by intermediary — The intermediary shall observe following due diligence while discharging his duties, namely: [...]

(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorized. [...]

(9) The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.” (INDIA. Ministry of Electronics and Information Technology. The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018. Disponível em https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf)

67 INDIA. Ministry of Electronics and Information Technology. Comments Invited on Intermediary Guidelines. Disponível em: https://www.meity.gov.in/comments-invited-draft-intermediary-rules.

68 INDIA. Ministry of Electronics and Information Technology. Public Comments on the Draft Intermediary Guidelines Rules, 2018. Disponível em: https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf.

69 INDIA. Ministry of Electronics and Information Technology. Counter Comments Invited on Comments Received by Public Stakeholders on the Draft Intermediary Guidelines. Disponível em: https://www.meity.gov.in/content/counter-comments-invited-comments-received-publicstakeholders-draft-“-information-technology.

70 INDIA. Ministry of Electronics and Information Technology. Counter Comments on Public Comments on the Draft Intermediary Guidelines. Disponível em: https://www.meity.gov.in/writereaddata/files/Counter_Comments_on_public_comments_on_draft_intermediary_guidelines.pdf.

71 CHATTERJEE, Siddhant, Disinformation and Beyond: Co-Regulatory Approaches for India, from the West. 26 de fevereiro de 2021. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3853451. P. 2.

72 No sistema jurídico indiano, normas subordinadas podem ser promulgadas na forma de Rules (traduzidas livremente neste texto como "Regras") ou Regulations ("Regulações"). Trata-se de instrumentos com força de lei, mas que são criados para especificar a forma de aplicação, ou definir diretrizes adicionais, de leis ordinárias. Por esse motivo, as normas subordinadas têm seu escopo restrito ao objeto da legislação principal que complementam, e devem ater-se a essas limitações. O caminho para publicação de normas subordinadas é diferente do processo legislativo comum: elas são aprovadas pelo Executivo sem votação pelo Parlamento, e em algumas situações é possível até mesmo contornar a necessidade de consultas públicas para aprovação. Para mais informações, consultar: UNNIKRISHNAN, A. Scope and Limitations of Subordinate Legislation Under IBC. Disponível em: https://ibbi.gov.in/uploads/resources/6ebf0b574193197ec88c562234877962.pdf.

73 Tradução livre de "Information Technology Act".

74 INDIA. Ministry of Electronics and Information Technology. The Information Technology Act, 2000. Disponível em https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

75 Tradução livre de "Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules".

76 INDIA. Ministry of Electronics and Information Technology. The Information Technology (Intermediary Guideline and Digital Media Ethics Code) Rules, 2021. Disponível em https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

77 Tradução livre de: 4. Additional due diligence to be observed by significant social media intermediary.

(2) A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the

Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form:

Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:

Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:

Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users:

Provided also that where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for the purpose of this clause. (INDIA. Ministry of Electronics and Information Technology. The Information Technology (Intermediary Guideline and Digital Media Ethics Code) Rules, 2021. Disponível em: https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf. Acesso em: 10 mai. 2022).

78 FIVE EYES. International Statement: End-to-End Encryption and Public Safety. 11 out. 2020. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925601/2020.10.11_International_statement_end-to-end_encryption_and_public_safety_for_publication_final.pdf.

79 ÍNDIA. Supreme Court of India. Justice K.S.Puttaswamy(Retd) ... vs Union Of India And Ors. 24 ago. 2017. Disponível em: https://indiankanoon.org/doc/91938676/.

80 SUGATHAN, Prasanth; SINGH, Apurva. Tracing encrypted messages: an analysis of the law. CSI Transactions on ICT, 2021. Disponível em https://link.springer.com/content/pdf/10.1007/s40012-021-00338-3.pdf. p. 4.

81 Idem, p. 5.

82 Idem, pp. 3-5.

83 Idem, p. 4.

84 Idem, ibidem.

85 INDIA. Supreme Court of India. Indian Express Newspapers ... vs Union Of India & Ors. Etc. Etc. 06 dez. 1984. Disponível em: https://indiankanoon.org/doc/223504/.

86 NARAYAN, Sidharth; KULKARNI, Amol. Understanding intermediary guidelines wrt encryption from the lens of consumer welfare. CSI Transactions on ICT, 2021. Disponível em: https://link.springer.com/content/pdf/10.1007/s40012-021-00339-2. pdf. p. 5-6.

87 INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. Internet Society, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india.

88 CENTER FOR DEMOCRACY & TECHNOLOGY. Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta. Tradução: SANTARÉM, Paulo Renná da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 de fevereiro de 2022. p. 20-21. Disponível em https://bit.ly/3GKVY7e.

89 NARAYAN, Sidharth; KULKARNI, Amol. Understanding intermediary guidelines wrt encryption from the lens of consumer welfare. CSI Transactions on ICT, 2021. Disponível em https://link.springer.com/content/pdf/10.1007/s40012-021-00339-2. pdf. P. 4-5.

90 KAMAKOTI, V. Report on Originator Traceability in WhatsApp Messages. 31 jul. 2019. Disponível em https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf.

91 RIBEIRO, Márcio Moretto. Nota Técnica 10 – Rastreamento de mensagens virais no WhatsApp. Monitor do Debate Político no Meio Digital. Grupo de Políticas Públicas para o Acesso à Informação. São Paulo: Universidade de São Paulo, 2020.

92 MAHESHWARI, R. CCAOIIndia. New IT Rules: Empowering Control or Controlled Empowerment? Deciphering the Intermedia. Youtube, 2021. Disponível em: https://www.youtube.com/watch?v=E8wkfidXaWs. Acesso em: 31 mar. 2022.

93 INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. Internet Society, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india. Acesso em: 31 mar. 2022.

94 CENTER FOR DEMOCRACY & TECHNOLOGY. Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta. Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 de fevereiro de 2022. Disponível em https://irisbh.com.br/publicacoes/abordagens-para-a-moderacao-de-conteudo-em-sistemas-com-criptografia-de-ponta-a-ponta/. Pp. 17-19.

95 LANA, Alice de Perdigão; PERRONE, Christian; ARCHEGAS, João Victor. Rastreabilidade de mensagens instantâneas e vigilância em massa. Instituto de Tecnologia e Sociedade – ITS, 16 jul. 2021. 28 p. Disponível em https://itsrio.org/pt/publicacoes/rastreabilidade-de-mensagens-instantaneas-e-vigilancia-em-massa-pl-2630-2020/. P. 24.

96 Idem, p. 28.

97 CENTER FOR DEMOCRACY & TECHNOLOGY. Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta. Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 de fevereiro de 2022. Disponível em https://bit.ly/3GKVY7e. Pp. 20-21.

98 AGUIAR, Thaís e outros. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís e outros. p. 10

99 KAMAKOTI, V. Report on Originator Traceability in WhatsApp Messages. 31 jul. 2019. Disponível em https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf.

100 INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. Internet Society, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india. Acesso em: 31 mar. 2022.

101 CENTER FOR DEMOCRACY & TECHNOLOGY. Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta. Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 de fevereiro de 2022. Pp. 20-21.

102 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 10 jan 2022.

103 NARAYAN, Sidharth; KULKARNI, Amol. Understanding intermediary guidelines wrt encryption from the lens of consumer welfare. CSI Transactions on ICT, p. 1-6, 2021.

104 CURZI, Yasmin e outros. Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2630/2020. Rio de Janeiro: FGV Direito Rio, 2021. Pp. 13-16.

105 TRINDADE, Henrique de Oliveira. Elementos para uma discussão acerca do papel do direito no avanço digital e em suas implicações na crise da democracia. Monografia de Conclusão de Curso (Bacharelado em Direito). Universidade Federal de Juiz de Fora, 2021.

106 RODRIGUES, T. M.; BONONE, L.; MIELLI, R. DESINFORMAÇÃO E CRISE DA DEMOCRACIA NO BRASIL: é possível regular fake news?. Confluências | Revista Interdisciplinar de Sociologia e Direito, v. 22, n. 3, p. 30-52, 2 dez. 2020.

107 AGUIAR, Thaís e outros. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís e outros. P. 10

108 DOS SANTOS, João Guilherme Bastos, e outros. WhatsApp, política mobile e desinformação: a hidra nas eleições presidenciais de 2018. Comunicação & Sociedade, 2019, 41.2: 307-334.

109 CENTER FOR DEMOCRACY & TECHNOLOGY. Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta. Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 de fevereiro de 2022. Pp. 20-21.

Referências

AGÊNCIA CÂMARA DE NOTÍCIAS; MUGNATTO, Sílvia. Grupo da Câmara conclui votação de relatório sobre combate às fake news. **Portal da Câmara dos Deputados** [Início / Comunicação / Notícias / Ciência, Tecnologia e Comunicações], 08 Dez. 2021, 12:18. Disponível em: https://www.camara.leg.br/noticias/836267-GRUPO-DA-CAMARA-CONCLUI-VOTACAO-DE-RELATORIO-SOBRE-COMBATE-AS-FAKE-NEWS. Acesso em: 30 Mar. 2022.

AGÊNCIA SENADO. Senado aprova projeto de combate a notícias falsas; texto vai à Câmara. **Senado Federal** [Senado Notícias / Matérias / Plenário], 30/06/2020 21h27; atu. 23h10. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/06/30/aprovado-projeto-de-combate-a-noticias-falsas. Acesso em: 30 Mar. 2022.

AGUIAR, Thaís; BIONI, Bruno; FAVARO, Iasmine; KITAYAMA, Marina; RIELLI, Mariana; VERGILI, Gabriela; ZANATTA, Rafael. **Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020.** São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís; BIONI, Bruno; MESQUITA, Hana; PIGATTO, Jaqueline; VERGILI, Gabriela.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO 9000: Sistemas de gestão da qualidade - Fundamentos e vocabulário**. Rio de Janeiro: ABNT, 2015.

BRASIL. Câmara dos Deputados. **Aperfeiçoamento da Legislação Brasileira - Internet**. Câmara dos Deputados [Início / Atividade Legislativa / Comissões / Grupos de trabalho / 56ª Legislatura (2019-2023) / Esta página], 23 Jun. 2020. Última Atualização: 23/02/2022 20:59:33. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/aperfeicoamento-da-legislacao-brasileira-internet. Acesso em: 30 mar. 2022.

BRASIL. Congresso Nacional. **Projeto de Lei nº 2630, de 2020** (Senador Alessandro Vieira - CIDADANIA/SE). Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Congresso Nacional [Congresso Nacional / Matérias Legislativas / Matérias Bicamerais], 13 Mai. 2020. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-2630-2020. Acesso em: 31 Mar. 2022.

BRASIL. Senado Federal. **Emenda Substitutiva Global nº 55/PLEN (ao PL nº 2.630, de 2020)**. Senador Alessandro Vieira (CIDADANIA/SE). Brasília, Senado Federal, 02 Jun. 2020. (P. 7) Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8117352&disposition=inline. Acesso em: 31 Mar. 2022.

CENTER FOR DEMOCRACY & TECHNOLOGY. **Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta.** Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto

de Referência em Internet e Sociedade. 15 de fevereiro de 2022. Disponível em https://bit.ly/3GKVY7e.

CHATTERJEE, Siddhant, **Disinformation and Beyond: Co-Regulatory Approaches for India, from the West.** 26 de fevereiro de 2021. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3853451.

COMISSÃO EUROPEIA. **Comunicação da comissão ao parlamento europeu, ao conselho, ao comitê econômico e social europeu e ao comitê das regiões: combater a desinformação em linha: uma estratégia europeia**. Bruxelas, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0236. Acesso em: 17 abr. 2022.

CURZI, Yasmin. ZINGALES, Nicolo. GASPAR, Walter. LEITÃO, Clara. COUTO, Natália. REBELO, Leandro. OLIVEIRA, Maria Eduarda. **Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2630/2020.** Rio de Janeiro: FGV Direito Rio, 2021. pp. 13-16.

DONEDA, Danilo; MACHADO, Diego (orgs.). **A criptografia no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2020.

DO VAL, Ronaldo Borges; VIANA, Thamirys Dias; GOUVEIA, Luis Borges. O uso de Blockchain na identificação de Fake News: ferramentas de apoio tecnológico para o combate à desinformação. **Brazilian Journal of Business**, 2021, 3.3: 2726-2742.

DOS SANTOS, João Guilherme Bastos e outros. WhatsApp, política mobile e desinformação: a hidra nas eleições presidenciais de 2018. **Comunicação & Sociedade**, 2019, 41.2: 307-334.

FIVE EYES. **International Statement: End-to-End Encryption and Public Safety.** 11 out. 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925601/2020.10.11_International_statement_end-to-end_encryption_and_public_safety_for_publication_final.pdf.

FRAGA-LAMAS, P., FERNANDEZ-CARAMES, T.M. Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. **IT Professional**. 22(2),9049288, 2020. pp. 53-59.

GALVÃO, Maria C.; RICARTE, Ivan L. M. Revisão sistemática da literatura: conceituação, produção e publicação. **Logeion: Filosofia da Informação**, [S.l.] , v. 6, n. 1, p. 57 - 73, set. 2019. P. 58. 7 - 73. Disponível em http://revista.ibict.br/fiinf/article/view/4835. Acesso em: 10 jun. 2021.

INDIA. Ministry of Electronics and Information Technology. **Comments Invited on Intermediary Guidelines.** Disponível em https://www.meity.gov.in/comments-invited-draft-intermediary-rules.

INDIA. Ministry of Electronics and Information Technology. **Counter Comments Invited on Comments Received by Public Stakeholders on the Draft Intermediary Guidelines.** Disponível em https://www.meity.gov.in/content/counter-comments-invited-comments-received-publicstakeholders-draft-“-information-technology.

INDIA. Ministry of Electronics and Information Technology. **Counter Comments on Public Comments on the Draft Intermediary Guidelines.** Disponível em: https://www.meity.gov.in/writereaddata/files/Counter_Comments_on_public_comments_on_draft_intermediary_guidelines.pdf.

INDIA. Ministry of Electronics and Information Technology. **Information Technology (Intermediaries Guidelines) Rules, 2011.** Disponível em https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf.

INDIA. Ministry of Electronics and Information Technology. **Note on withdrawal of the Draft National Encryption Policy.** Disponível em https://www.meity.gov.in/writereaddata/files/national-encryption-policy-govt_0.pdf.

INDIA. Ministry of Electronics and Information Technology. **Public Comments on the Draft Intermediary Guidelines Rules, 2018.** Disponível em https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf.

INDIA. Ministry of Electronics and Information Technology. **The Information Technology Act, 2000.** Disponível em https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

INDIA. Ministry of Electronics and Information Technology. **The Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018.** Disponível em https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

INDIA. Ministry of Electronics and Information Technology. **The Information Technology (Intermediary Guideline and Digital Media Ethics Code) Rules, 2021.** Disponível em https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf.

INDIA. Supreme Court of India. **Indian Express Newspapers ... vs Union Of India & Ors. Etc. Etc.** 06 dez. 1984. Disponível em: https://indiankanoon.org/doc/223504/.

INDIA. Supreme Court of India. **Justice K.S.Puttaswamy(Retd) ... vs Union Of India And Ors.** 24 ago. 2017. Disponível em: https://indiankanoon.org/doc/91938676/.

INTERNET SOCIETY. **Traceability and Cybersecurity: Experts’ Workshop Series on Encryption in India.** Internet Society, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-experts-workshop-series-on-encryption-in-india.

KAMAKOTI, V. **Report on Originator Traceability in WhatsApp Messages.** 31 jul. 2019. Disponível em https://www.medianama.com/wp-content/uploads/Dr-Kamakoti-submission-for-WhatsApp-traceability-case-1.pdf.

LANA, Alice de Perdigão; PERRONE, Christian; ARCHEGAS, João Victor. **Rastreabilidade de mensagens instantâneas e vigilância em massa.** Instituto de Tecnologia e Sociedade – ITS, 16 de julho de 2021. 28 p. P. 24. Disponível em https://itsrio.org/pt/publicacoes/rastreabilidade-de-mensagens-instantaneas-e-vigilancia-em-massa-pl-2630-2020/.

MAHESHWARI, R. CCAOIIndia. New IT Rules: Empowering Control or Controlled Empowerment? Deciphering the Intermedia. **Youtube**, 2021. Disponível em: https://www.youtube.com/watch?v=E8wkfidXaWs. Acesso em: 31 mar. 2022.

MARBOUH, D. et al., Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. **Arabian Journal for Science and Engineering**, v. 45, n. 12, 2020. pp. 9895-9911.

NARAYAN, Sidharth; KULKARNI, Amol. Understanding intermediary guidelines wrt encryption from the lens of consumer welfare. **CSI Transactions on ICT, 2021.** Disponível em: https://link.springer.com/content/pdf/10.1007/s40012-021-00339-2.pdf.

PAPI, Fernando G.; HÜBNER, Jomi Fred; DE BRITO, Maiquel. Instrumenting Accountability in MAS with Blockchain. In: **CARe-MAS@ PRIMA**. 2017. p. 20-34.

PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 19 de abril de 2022.

PIELEMEIER, Jason. Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?. **Utah L. Rev.**, 2020, 917.

PINHO FILHO, José Célio Belém de. **Desinformação e regulação de redes sociais digitais.** 2021. 170 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021. P. 67. Disponível em https://repositorio.idp.edu.br//handle/123456789/3391.

REUTERS. 'Five Eyes' security alliance calls for access to encrypted material. **Reuters**, 30 jul. 2019. Disponível em: https://www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199. Acesso em: 28 abr. 2022.

RIBEIRO, Márcio Moretto. Nota Técnica 10 – Rastreamento de mensagens virais no WhatsApp. **Monitor do Debate Político no Meio Digital.** Grupo de Políticas Públicas para o Acesso à Informação. São Paulo: Universidade de São Paulo, 2020. P. 5. Disponível em https://www.monitordigital.org/2020/08/17/nota-tecnica-10/.

RODRIGUES, T. M.; BONONE, L.; MIELLI, R. DESINFORMAÇÃO E CRISE DA DEMOCRACIA NO BRASIL: é possível regular fake news?. Confluências | **Revista Interdisciplinar de Sociologia e Direito**, v. 22, n. 3, p. 30-52, 2 dez. 2020.

SAMPAIO, R. F.; MANCINI, M. C. Estudos de Revisão Sistemática: um guia para síntese criteriosa da evidência científica. **Revista Brasileira de Fisioterapia**, São Carlos, v. 11, n. 1., p. 83-89, 2007.

SANSAD TV. Minister Ravi Shankar Prasad's remarks | Calling Attention on misuse of social media. **YouTube**, 26 jul. 2018. Disponível em https://www.youtube.com/watch?v=aU1m2O7We6E.

SCHULZE, M. Clipper meets Apple vs. FBI – a comparison of the cryptography discourses from 1993 and 2016. **Media and Communication**, v. 5, n. 1, p. 54-62, 22 mar. 2017.

SUGATHAN, Prasanth; SINGH, Apurva. **Tracing encrypted messages: an analysis of the law. CSI Transactions on ICT, 2021**. Disponível em https://link.springer.com/content/pdf/10.1007/s40012-021-00338-3.pdf.

TAILLON, Patrick. From veracity to traceability: A new Canadian legal framework for deliberative referenda. IN: BAUME, Sandrine; BOILLET, Véronique; MARTENET, Vincent (eds.) **Misinformation in Referenda**. Routledge, 2020. p. 257-280.

TRINDADE, Henrique de Oliveira. **Elementos para uma discussão acerca do papel do direito no avanço digital e em suas implicações na crise da democracia.** Monografia de Conclusão de Curso (Bacharelado em Direito). Universidade Federal de Juiz de Fora, 2021. P. 38. Disponível em https://repositorio.ufjf.br/jspui/handle/ufjf/12831.

UN. Human Rights Council. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; Secretariat. **Encryption and anonymity follow-up report: note / by the Secretariat (A/HRC/38/35/Add.5**). Genebra: UN, 13 July 2018. 18 p. Disponível em https://digitallibrary.un.org/record/1638475.

UNNIKRISHNAN, A. **Scope and Limitations of Subordinate Legislation Under IBC.** Disponível em https://ibbi.gov.in/uploads/resources/6ebf0b574193197ec88c562234877962.pdf.

WARDLE, C. and DERAKHSHAN, H. Information Disorder: Toward an interdisciplinary framework for research and policymaking. **Strasbourg Cedex: Council of Europe**, 2017. Disponível em: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html. Acesso em 26 abr. 2022.

Apêndice 1 - Corpus total de textos analisados

REFERÊNCIA	CATEGORIA	FONTE
MARBOUH, D., ABBASI, T., MAASMI, F., (...), JAYARAMAN, R., ELLAHHAM, S., Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. Arabian Journal for Science and Engineering 45(12), 2020. pp. 9895-9911.	Artigo científico	Bases de dados acadêmicas
FRAGA-LAMAS, P., FERNANDEZ-CARAMES, T.M. Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. IT Professional. 22(2),9049288, 2020. pp. 53-59.	Artigo científico	Bases de dados acadêmicas
FLOREZ, Z.J., LOGREIRA, R.C., MUNOZ, M., VARGAS, J.F., Architecture of instant messaging systems for secure data transmission. Proceedings - International Carnahan Conference on Security Technology, 2017, 7815685.	Trabalho publicado em anais de evento acadêmico	Bases de dados acadêmicas
PIELEMEIER, Jason. Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?. Utah L. Rev., 2020, 917	Artigo científico	Bases de dados acadêmicas

REFERÊNCIA	CATEGORIA	FONTE
TAILLON, Patrick. From veracity to traceability: A new Canadian legal framework for deliberative referenda. In: Misinformation in Referenda. Routledge, 2020. p. 257-280.	Artigo científico	Bases de dados acadêmicas
CHATTERJEE, Siddhant. Disinformation and beyond: Co-Regulatory Approachesfor India, from the West.	Artigo científico	Bases de dados acadêmicas
KIRAN, S. Disinformation: Spread, Impact and Interventions in Indian Context. The Indian Police Journal, 28.	Artigo científico	Bases de dados acadêmicasv
DURACH, Flavia; BÂRGĂOANU, Alina; NASTASIU, Cătălina. Tackling disinformation: EU regulation of the digital space. Romanian Journal of European Affairs, 2020, 20.1.	Artigo científico	Bases de dados acadêmicas
BOYD, Colin. Enforcing traceability in software. In: International Conference on Information and Communications Security. Springer, Berlin, Heidelberg, 1997. p. 398-408.	Trabalho publicado em anais de evento acadêmico	Bases de dados acadêmicas

REFERÊNCIA	CATEGORIA	FONTE
PAPI, Fernando G.; HÜBNER, Jomi Fred; DE BRITO, Maiquel. Instrumenting Accountability in MAS with Blockchain. In: CARe-MAS@ PRIMA. 2017. p. 20-34.	Artigo científico	Bases de dados acadêmicas
WOJCIK, Stéphanie. How Does eDeliberation work? A Study of French Local Electronic Forums. Grönlund Å., Andersen K., Rose J., Avdic A., and Hedström K. (eds). Understanding eParticipation. Contemporary PhD eParticipation research in Europe, Örebro University Library, pp.153-167, 2007. HAL Id: hal-00485913 https://hal.archives-ouvertes.fr/hal-00485913.	Artigo científico	Bases de dados acadêmicas
BARIK, Lalatendu Bidyadhara Kumar; BARIK, Nikita. WhatsApp Web QR code: Auto-change Frequency Analysis. Journal of Information Studies & Technology (JIS&T), 2021, 2021.2: 10.	Artigo científico	Bases de dados acadêmicas
PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3.	Relatório de pesquisa	Bases de dados acadêmicas

REFERÊNCIA	CATEGORIA	FONTE
DOS SANTOS, João Guilherme Bastos, et al. WhatsApp, política mobile e desinformação: a hidra nas eleições presidenciais de 2018. Comunicação & Sociedade, 2019, 41.2: 307-334.	Artigo científico	Bases de dados acadêmicas
DO VAL, Ronaldo Borges; VIANA, Thamirys Dias; GOUVEIA, Luis Borges. O uso de Blockchain na identificação de Fake News: ferramentas de apoio tecnológico para o combate à desinformação. Brazilian Journal of Business, 2021, 3.3: 2726-2742.	Artigo científico	Bases de dados acadêmicas
FURTADO, Renata Lira; OLIVEIRA, Jenifer Galdino de. O fenômeno da desinformação sob a perspectiva dos arquivistas brasileiros: o papel da competência em informação. Revista Informação em Pauta, Fortaleza, v. 5, n. 2, p. 107-131, jul./dez. 2020.	Artigo científico	Bases de dados acadêmicas
OLIVEIRA, Thaiane Moreira de.; QUINAN, RODRIGO ; GONCALVES, R. . ENTRE LEGITIMAÇÃO E ATAQUES POLÍTICOS: circulação de sentidos sobre desinformação entre lideranças políticas relacionada ao Covid-19 no Facebook. In: Compolítica, 2021, Remoto. Anais do 9 Congresso da Associação Brasileira de Pesquisadores em Comunicação e Política. Santa Catarina: Compolítica, 2021. v. 1. p. 1-25.	Trabalho publicado em anais de evento acadêmico	Bases de dados acadêmicas

REFERÊNCIA	CATEGORIA	FONTE
Curzi, Y., Zingales, N., Gaspar, W. B., Leitão, C., Couto, N., Rebelo, L., & Oliveira, M. E. (2021). Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2630/2020.	Nota técnica	Bases de dados acadêmicas
Rodrigues, T. M., Bonone, L., & Mielli, R. (2020). DESINFORMAÇÃO E CRISE DA DEMOCRACIA NO BRASIL: é possível regular fake news?. Confluências| Revista Interdisciplinar de Sociologia e Direito, 22(3), 30-52.	Artigo científico	Bases de dados acadêmicas
TRINDADE, Henrique de Oliveira. Elementos para uma discussão acerca do papel do direito no avanço digital e em suas implicações na crise da democracia. Monografia de Conclusão de Curso (Bacharelado em Direito). Universidade Federal de Juiz de Fora, 2021.	Monografia, dissertação ou tese	Bases de dados acadêmicas
FERNANDES, A. L., DE SIQUEIRA VALVERDE, D. N., CONSTANT, I. M., SARAIVA, R. L., VALOIS, R. C., & ARCANJO, L. Relatório amostral (norte-sul global) de conceitos relativos à responsabilidade civil de intermediários na internet. Recife: Instituto de Pesquisa em Direito e Tecnologia do Recife, 2021.	Relatório de pesquisa	Bases de dados acadêmicas

REFERÊNCIA	CATEGORIA	FONTE
SUGATHAN, Prasanth; SINGH, Apurva. Tracing encrypted messages: an analysis of the law. CSI Transactions on ICT, p. 1-5, 2021.	Artigo científico	Bases de dados acadêmicas
NARAYAN, Sidharth; KULKARNI, Amol. Understanding intermediary guidelines wrt encryption from the lens of consumer welfare. CSI Transactions on ICT, p. 1-6, 2021.	Artigo científico	Bases de dados acadêmicas
AGUIAR, Thaís; BIONI, Bruno; FAVARO, Iasmine; KITAYAMA, Marina; RIELLI, Mariana; VERGILI, Gabriela; ZANATTA, Rafael. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís; BIONI, Bruno; MESQUITA, Hana; PIGATTO, Jaqueline; VERGILI, Gabriela.	Nota técnica	Lista do GTNET
LANA, Alice de Perdigão; PERRONE, Christian; ARCHEGAS, João Victor. Rastreabilidade de mensagens instantâneas e vigilância em massa. Instituto de Tecnologia e Sociedade – ITS, 16 de julho de 2021. 28 p. Disponível em https://itsrio.org/pt/publicacoes/rastreabilidade-de-mensagens-instantaneas-e-vigilancia-em-massa-pl-2630-2020/.	Relatório de pesquisa	Lista do GTNET

REFERÊNCIA	CATEGORIA	FONTE
INTERNET SOCIETY. Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India. Internet Society, 27 nov. 2020. Disponível em: https://www.internetsociety.org/resources/doc/2020/traceability-and-cybersecurity-expertsworkshop-series-on-encryption-in-india/. Acesso em: 06 ago. 2021.	Relatório de seminários	Lista do GTNET
CENTER FOR DEMOCRACY & TECHNOLOGY. Olhando de fora para dentro: abordagens para moderação de conteúdo em sistemas com criptografia de ponta a ponta. Tradução: SANTARÉM, Paulo Renã da Silva. VIEIRA, Victor Barbieri Rodrigues. Instituto de Referência em Internet e Sociedade. 15 de fevereiro de 2022. Disponível em https://bit.ly/3GKVY7e.	Relatório de pesquisa	Inserção discricionária
PINHO FILHO, José Célio Belém de. Desinformação e regulação de redes sociais digitais. 2021. 170 f. Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021.	Monografia, dissertação ou tese	Inserção discricionária
SALTZER, J. SCHROEDER, M. The protection of information in computer systems," in Proceedings of the IEEE, vol. 63, 9 (1975), 1278-1308	Trabalho publicado em anais de evento acadêmico	Inserção discricionária

REFERÊNCIA	CATEGORIA	FONTE
KERR, Orin S.; SCHNEIER, Bruce. Encryption workarounds. Geo. LJ, v. 106, p. 989, 2017.	Artigo científico	Inserção discricionária
UN. Human Rights Council. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; Secretariat. Encryption and anonymity follow-up report: note / by the Secretariat (A/HRC/38/35/Add.5). Genebra: UN, 13 July 2018. 18 p. Disponível em https://digitallibrary.un.org/record/1638475.	Relatoria especial da ONU	Inserção discricionária
RIBEIRO, Márcio Moretto. Nota Técnica 10 – Rastreamento de mensagens virais no WhatsApp. Monitor do Debate Político no Meio Digital. Grupo de Políticas Públicas para o Acesso à Informação. São Paulo: Universidade de São Paulo, 2020.	Nota técnica	Inserção discricionária

Apêndice 2 - Formulário de análise

- E-mail
- Ano
- Referência ABNT
- Link da publicação
- Categoria
  marcar apenas uma opção

  > Artigo científico
  >
  > Declaração, carta aberta
  >
  > Relatório
  >
  > Nota técnica
  >
  > Jurisprudência
  >
  > Trabalho publicado em anais de evento acadêmico
  >
  > Monografia, dissertação ou tese
  >
  > Artigo de opinião
  >
  > Matéria de jornal
  >
  > Post de blog

- Escopo
  marcar apenas uma opção

  > Rastreabilidade
  >
  > Hacking governamental
  >
  > Varredura pelo lado do cliente

- Síntese
  Texto de resumo elaborado pela equipe do IRIS: deve incluir uma apresentação breve da proposta do trabalho, metodologia (ou ausência de indicação de metodologia), eventuais referências relevantes (citadas como base para o conceito ou posicionamento indicado no trabalho) e abordagem dada ao escopo analisado.

- Comentários

- Citações

- Observações

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE