

input_

novos desafios na responsabilidade de provedores de aplicações de internet

**implicações para a economia digital e o
comércio eletrônico após a decisão do
Supremo Tribunal Federal sobre o Marco
Civil da Internet**

setembro, 2026

ficha técnica

equipe do projeto

francisco brito cruz (coordenador)

fernando gallo

helenal maluf

vinicius harada

apoio

mercado livre

como citar este documento?

BRITO CRUZ, Francisco (coord.); MALUF, Helena; e HARADA, Vinicius. *Novos desafios na responsabilidade de provedores de aplicações de internet*. Input, São Paulo: 2026.

sumário executivo

Este documento sintetiza os debates de duas oficinas sobre a responsabilidade de provedores de aplicações de internet após a decisão do STF acerca do art. 19 do Marco Civil, realizadas em São Paulo em 27 de abril de 2026 e 10 de agosto de 2026 sob a Regra de *Chatham House*, com cerca de 35 participantes do setor privado, do setor público, da academia e da sociedade civil em cada uma.

O diagnóstico transversal é que **o novo regime ampliou significativamente os deveres atribuídos aos provedores, mas deixou em aberto parte relevante dos parâmetros necessários para orientar seu cumprimento.** Conceitos como dever de cuidado, atuação diligente, falha sistêmica, riscos sistêmicos e dúvida razoável passam a ocupar posição central na responsabilização das plataformas, sem que esteja ainda suficientemente definido o que cada um deles exige na prática. A consequência é um ambiente em que provedores, autoridades administrativas e Judiciário podem adotar métricas e expectativas distintas sobre a mesma obrigação, aumentando a insegurança jurídica e produzindo incentivos à remoção preventiva de conteúdos e ofertas legítimas, podendo gerar, por consequência, um aumento de litígios judiciais.

Um primeiro eixo das discussões examinou, portanto, os deveres de cuidado e de diligência. As discussões apontam para a necessidade de tratá-los predominantemente como deveres de adoção de processos, mecanismos e salvaguardas adequados, e não como uma garantia de eliminação integral de conteúdos ilícitos. O documento explora, nesse contexto, alternativas para conferir maior objetividade à supervisão, como a ancoragem do dever de cuidado na boa-fé objetiva, o uso de métricas de prevalência e de parâmetros qualitativos sobre a arquitetura de moderação, além da consideração das limitações técnicas, da escala dos serviços e dos diferentes modelos de negócio. Também são discutidos problemas específicos do comércio eletrônico, especialmente a necessidade de distinguir danos de consumo, sujeitos ao regime próprio do CDC, de danos relacionados ao conteúdo e à circulação de discurso, regulados pelo Marco Civil.

O segundo eixo trata do novo papel das notificações extrajudiciais. A principal questão é impedir que o regime se converta, na prática, em uma obrigação automática de remoção. A “dúvida razoável” aparece como mecanismo essencial para preservar um modelo de notice and action, no qual a notificação desencadeia um dever de análise e resposta, mas não necessariamente de indisponibilização. As oficinas identificaram, contudo, riscos relevantes de instrumentalização das notificações por concorrentes, associações ou outros atores, assim como dificuldades causadas por pedidos massivos, pouco individualizados ou baseados apenas em palavras-chave, hashtags e hashes. Nesse cenário, as oficinas enfatizaram a importância da identificação precisa do conteúdo, da preservação de sua análise contextual e da distribuição adequada dos deveres entre quem formula a requisição, quem determina a medida e quem a deve executar. O objetivo é evitar que a plataforma seja transformada, simultaneamente, em investigadora, autoridade

técnica e julgadora de controvérsias cuja resolução depende de informações ou competências detidas pelo próprio Estado, transferindo-lhe, na prática, o exercício de poderes de polícia atribuídos às autoridades estatais.

Um terceiro eixo aborda a governança institucional do novo regime. A atribuição de novas competências à ANPD pode contribuir para a formação de um centro regulatório capaz de produzir parâmetros técnicos mais estáveis, mas sua atuação ocorre em um ambiente já caracterizado pela multiplicidade de autoridades administrativas. O desafio, portanto, não é apenas atribuir competências, mas construir coordenação e alguma forma de deferência a parâmetros regulatórios tecnicamente fundamentados. Essa discussão também evidencia que o cumprimento dos novos deveres não depende somente das plataformas: quando se exige verificação automatizada de licenças, registros ou autorizações públicas, por exemplo, é necessário que o próprio Estado disponibilize bases de dados estruturadas, atualizadas e tecnicamente consumíveis.

A partir desses diagnósticos, o documento propõe uma agenda voltada à densificação e à previsibilidade do novo regime. Em conjunto, essas propostas partem de uma mesma premissa: a efetividade do novo regime de responsabilidade depende menos da expansão abstrata das obrigações e mais da construção de parâmetros institucionais, técnicos e procedimentais capazes de torná-las executáveis. O desafio aberto pela decisão do STF é, assim, transformar categorias jurídicas amplas em um sistema previsível de incentivos e responsabilidades, capaz de enfrentar conteúdos e atividades ilícitas sem produzir, como efeito colateral, sobreexatidão, insegurança para atividades econômicas legítimas ou fragmentação da governança digital brasileira.

Índice

introdução.....	6
apresentação do projeto e cenário.....	6
premissas de trabalho e método.....	6
I. desafios na devida diligência e no dever de cuidado.....	8
escopo dos deveres de cuidado e diligência.....	8
entre obrigações “de resultado” e “de meio”.....	9
parâmetros para aferição “sistêmica” e seus desafios.....	10
limitações operacionais no cumprimento das obrigações e suas consequências.....	11
riscos sistêmicos vs. falha sistêmica.....	12
proteção de grupos vulneráveis.....	12
como fica o regime jurídico da responsabilidade civil no comércio eletrônico?.....	13
II. notificações extrajudiciais.....	15
instrumentalização de notificações extrajudiciais para fins abusivos..	16
desafios em notificações enviadas por autoridades públicas.....	16
o encaminhamento de dados ao Poder Público.....	17
a “dúvida razoável”.....	17
requisitos para localização inequívoca do conteúdo.....	18
III. governança, enforcement e o papel do setor público.....	20
a ANPD como autoridade para o ambiente digital: tensões e riscos...	20
visões sobre uma agenda de deferência regulatória.....	21
dados públicos como insumo para o cumprimento de deveres de provedores.....	22
IV. recomendações e convergências.....	24
autorregulação para padronização técnica.....	24
agenda de deferência regulatória para segurança jurídica.....	24
agenda de adequação e ações no Poder Público.....	25
agenda de densificação regulatória do dever de cuidado e atuação diligente.....	26
agenda de detalhamento do regime de notificações extrajudiciais.....	27

introdução

apresentação do projeto e cenário

Este documento de síntese apresenta e organiza as principais ideias discutidas em duas oficinas sobre a responsabilidade de provedores de aplicações de internet após a decisão do Supremo Tribunal Federal (STF) sobre o artigo 19 do Marco Civil da Internet, com foco em seus efeitos para a economia digital e o comércio eletrônico. **A organização e o financiamento das oficinas contaram com o apoio do Mercado Livre.**

A primeira oficina teve como objeto central de discussão o cenário aberto em resposta ao julgamento do Supremo Tribunal Federal (STF) sobre os temas de repercussão geral nºs 987 e 533, que tocavam a constitucionalidade do artigo 19 do Marco Civil da Internet (Lei nº 12.965/2014). Em junho de 2025, ao analisar dois recursos extraordinários,¹ a Corte deliberou pela inconstitucionalidade parcial e progressiva do artigo 19 do MCI, determinando que o artigo não conferia proteção suficiente a bens jurídicos constitucionais de alta relevância. A tese fixada no julgamento, dessa forma, alterou significativamente o quadro geral da responsabilização de provedores de aplicação de internet.

Posteriormente, em maio de 2026, o Poder Executivo editou os Decretos nº 12.975 e nº 12.976/2026. O primeiro versou sobre deveres gerais dos provedores de aplicações de internet e alterou o decreto regulamentador do MCI, publicado em 2016²; o segundo institui medidas específicas de enfrentamento à violência contra mulheres no ambiente digital.³ Em junho de 2026, também colaborando para a posterior alteração do novo cenário regulatório, o STF julgou os embargos de declaração em face dos recursos extraordinários. Com efeito, uma série de temas destacados pelos participantes no primeiro encontro foram tratados nos textos dos decretos e na decisão do STF. Por essa razão, optou-se por realizar uma segunda oficina.

Esse novo regime jurídico ainda está sendo assimilado por agentes como tribunais, empresas, sociedade civil e academia. Suas implicações práticas para a economia digital (seus incentivos, modelos de negócio e dinâmica concorrencial) e para liberdade de expressão são objeto de incerteza e foi para mapear essas implicações que as oficinas foram organizadas. Os encontros permitiram (i) coletar percepções práticas e teóricas de diferentes atores sobre o cenário aberto pela decisão do STF, bem como (ii) mapear recomendações e teses prospectivas acerca de como promover mais previsibilidade nesse quadro.

premissas de trabalho e método

Ambas as oficinas foram realizadas presencialmente em São Paulo, em 27 de abril de 2026 e 10 de agosto de 2026, respectivamente, com duração entre 10h00 e 17h00. Cada encontro reuniu cerca de 35 participantes de diferentes setores – advogados e advogadas da iniciativa privada, pesquisadores acadêmicos, representantes do setor público e integrantes de organizações da sociedade civil –, todos com atuação em temas situados na intersecção entre direito, tecnologia, mercados digitais e regulação de plataformas. As oficinas foram estruturadas em sessões temáticas. Cada sessão contou com uma abertura com falas norteadoras do tema a ser abordado, seguido de um debate mais amplo aberto a todos os participantes. **As oficinas foram realizadas sob a regra de *Chatham House*, de maneira que este documento de síntese não identifica os participantes e tampouco a autoria de cada ideia.**

Como exposto, a **organização e o financiamento das oficinas contaram com o apoio do Mercado Livre**. No entanto, este documento não reflete necessariamente a visão da empresa, mas o relato dos debates ocorridos nas oficinas.

As oficinas não tiveram como objetivo endossar a decisão dos temas 987 e 533 ou, ainda, os decretos editados pelo Poder Executivo, mas sim discutir suas implicações

¹ Os RE 1.037.396 e o RE 1.057.258.

² Decreto nº 8.771/2016.

³ Decreto nº 12.976/2026.

práticas entre setores. A primeira premissa do trabalho, assim, é que a discussão destas implicações **não exclui participantes que tenham visões críticas sobre decisões judiciais ou do Executivo.**

A segunda premissa é que o julgamento, a edição dos decretos e a decisão sobre os embargos de declaração consolidaram um novo ponto de partida para o debate sobre responsabilidade de provedores **que exige respostas sobre como operacionalizar esses conceitos e normas na prática institucional.** Desta forma, as reflexões e recomendações apresentadas no decorrer deste documento resultam do acúmulo dos debates realizados ao longo de todo esse processo, oferecendo uma contribuição a um ecossistema regulatório em plena construção.

I. desafios na devida diligência e no dever de cuidado

Os conceitos de “dever de cuidado” (associado à obrigação de indisponibilização imediata de determinados conteúdos que configurem crimes listados na tese editada pelo STF) e de “atuação diligente” (associada à presunção relativa de culpa no caso de anúncios e impulsionamentos pagos determinada na tese do STF) figuraram entre os conceitos mais debatidos nas oficinas. A centralidade do tema decorre, em grande medida, de sua indeterminação, visto que se tratam de categorias ainda em construção, de aplicação variada em jurisdições estrangeiras.

escopo dos deveres de cuidado e diligência

De maneira transversal nas oficinas realizadas, os participantes convergiram em torno de uma preocupação com a dificuldade de interpretação das categorias de dever de cuidado e de outros termos, como atuação diligente. A indeterminação semântica do conceito de dever de cuidado foi apontada como um fator de potencial insegurança jurídica, na medida em que dificulta a delimitação clara das responsabilidades dos provedores e a previsibilidade das decisões judiciais e administrativas. Nesse sentido, os participantes sublinharam a importância de que o dever de cuidado seja progressivamente consolidado a partir de parâmetros mais precisos, orientando condutas e servindo de referência consistente tanto para o setor privado quanto para a regulação administrativa e adjudicação.

Um exemplo de preocupação acerca do escopo do dever de cuidado pode ser visto através de debate ocorrido na segunda oficina a partir de duas partes do regime de responsabilidade de provedores estabelecido pelo STF e detalhado nos referidos decretos. Nesta ocasião, alguns participantes apontaram diferenças significativas entre o dever constante no artigo 16-B presente no Decreto 12.975/2026, referente ao cuidado para “indisponibilização imediata” de conteúdos que configuram crimes graves (indicando a “falha sistêmica” como caso de descumprimento), e as obrigações constantes nos artigos 16-K e 16-L do mesmo instrumento, que atribui presunção de responsabilidade (ou, conforme o julgamento dos embargos, *presunção de culpa*) quando da falta de comprovação de que “atuaram diligentemente e em tempo razoável para indisponibilizar o conteúdo” (sem figurar a ideia de “falha sistêmica”, por exemplo). Esses dois dispositivos provocaram os participantes da oficina a se indagar se o novo regime não obriga as plataformas a executar *dois deveres de diligência* diferentes.

Ainda na esteira do debate sobre a limitação do dever de cuidado e de atuação diligente, foi sugerido por participantes que os conceitos sejam interpretados juridicamente a partir da noção clássica do direito civil de boa-fé objetiva.⁴ Nesse sentido, foi questionado o uso acrítico da noção importada de *duty of care*, em detrimento de uma leitura fundada nos deveres anexos que a civilística brasileira consolidou ao longo de décadas: lealdade, transparência, cuidado e sigilo. Esses quatro deveres, ancorados na doutrina e pela jurisprudência como desdobramentos da boa-fé objetiva nas relações contratuais, ofereceriam um substrato dogmático adequado para a compreensão do dever de cuidado no contexto digital. Nessa leitura possível, o dever de cuidado não seria uma categoria autônoma ou inaugurada pela decisão do STF, mas uma “herança” da boa fé objetiva. Ancorar o debate nessa matriz civilista foi visto por alguns participantes como uma estratégia juridicamente adequada para construir, com base no dever de cuidado, um dique de contenção contra um incentivo generalizado para que provedores removam conteúdo legítimo, ou que sejam incentivados a promoverem remoções indiscriminadas. A remissão firme à boa-fé objetiva combateria esse estímulo à remoção sempre que presente algum mínimo grau de incerteza sobre a licitude dos conteúdos, com todos os riscos que isso implicaria para os direitos fundamentais envolvidos nesta decisão.

⁴ Um aspecto central da boa-fé objetiva é a geração de deveres anexos à relação contratual, obrigações que não estão expressamente previstas no contrato, mas decorrem do próprio princípio e são amplamente reconhecidas pela doutrina e jurisprudência brasileiras. Os principais deveres anexos consolidados incluem: o dever de lealdade (agir com honestidade e sem intenção de prejudicar a outra parte), o dever de transparência (fornecer informações relevantes e não omitir fatos essenciais), o dever de cuidado (atuar com diligência para evitar danos à contraparte) e o dever de sigilo (preservar informações confidenciais obtidas no curso da relação). A violação desses deveres, mesmo na ausência de cláusula contratual expressa, pode gerar responsabilidade civil.

Alguns participantes também identificaram tentativas de expansão interpretativa do conceito de dever de cuidado para além de seus contornos originais. Foi relatado que autoridades administrativas e associações setoriais já estão operacionalizando, na prática, um verdadeiro "transplante" dessa noção para a esfera da proteção de dados pessoais, tomando a decisão do STF como fundamento habilitador. Essa leitura ampliada do dever de cuidado, contudo, tem avançado de forma difusa e sem contornos normativos precisos, navegando por searas temáticas, como a da privacidade e do tratamento de dados, que possuem arcabouço regulatório próprio e consolidado. Participantes oriundos da academia e do setor privado levantaram, dessa forma, ceticismo quanto à necessidade de se trazer o conceito de dever de cuidado para a esfera de aplicação da Lei Geral de Proteção de Dados (LGPD), diante de deveres já consolidados pelo diploma.

Em termos de escopo, outro tema debatido foi a relação entre o modelo de monetização das plataformas e a extensão de seu dever de diligência. A premissa de que aquele que auferir o bônus deve arcar com os ônus derivados de sua atividade foi discutida por alguns participantes com apelo a que essa ilação seja feita com cautela, no sentido de que sua aplicação exige maior precisão conceitual sobre quais são, concretamente, o bônus e o ônus em questão no debate sobre plataformas digitais, e qual a pertinência de sua referência para a determinação da alocação e da medida adequada de responsabilidade decorrente do dever de diligência.

Neste caso, um exemplo marcante do debate foi a distinção entre o conteúdo orgânico e o conteúdo impulsionado. Mais especificamente, quando uma plataforma lucra diretamente com a distribuição artificial de determinado conteúdo por meio de redes de anúncios ou posts pagos, argumentou-se que o vínculo entre a plataforma e esse conteúdo é qualitativamente distinto daquele em que, por exemplo, usuários fazem anúncios espontâneos como "conteúdo orgânico" nos ambientes mantidos pelo provedor. Neste caso, tratar-se-ia ainda de um anúncio em sentido amplo, mas não no sentido estrito de conteúdo impulsionado pela plataforma e tampouco conteúdo com o qual ela lucra. Neste ponto, integrantes das oficinas sugeriram que é justo e proporcional que regimes de responsabilidade distintos incidam sobre cada cenário, com um regime mais estrito sobre casos em que a plataforma tem controle efetivo sobre a atividade remunerada e proveito econômico direto dela.

entre obrigações “de resultado” e “de meio”

Diante da decisão do STF, o dever de cuidado ganhou força enquanto nova lente para casos em que plataformas devem ser responsabilizadas em caso de “falha sistêmica” na obrigação de “indisponibilizar imediatamente” conteúdo que configure determinados crimes graves listados pela Corte. A “atuação diligente” também se destacou, por sua vez, como parâmetro para afastar a presunção de culpa relativa em casos de danos decorrentes de impulsionamentos e anúncios pagos.

Nas oficinas, participantes chamaram a atenção para diferentes interpretações sobre estes conceitos que se relacionavam com as ideias de “obrigação de resultado” ou “obrigação de meio”. Aquela, com foco nas consequências, parte da ideia de que o cumprimento do dever de cuidado se dá a partir da análise dos “resultados” desejáveis pelo dever de cuidado, ou seja, pelo grau que um conteúdo ilícito é acessível e exibido aos usuários da plataforma. A segunda, com foco em condutas, parte da compreensão do dever de cuidado como um dever de adotar determinados mecanismos e procedimentos esperados de um provedor de aplicação de internet, capazes de indicar que há grau suficiente de segurança na prevenção ou remoção de conteúdos ilegais. Neste último modelo, o parâmetro para avaliação de infrações ao dever de cuidado repousaria sobre a solidez da arquitetura de moderação desenvolvida pelas plataformas para evitar ilicitudes, e não pela simples detecção de tais conteúdos.

Ao discutir a edição dos decretos nº 12.975 e 12.976, participantes da segunda oficina apresentaram suas disposições como evidência de que o dever de cuidado constituiria predominantemente uma “obrigação de meio”, mencionando que seu cumprimento seria aferido mediante o emprego de metodologias e de esforços aprovados pelo regulador para

evitar a circulação ampla de conteúdo ilegal. Isto também se reflete no caso de impulsionamentos e anúncios pagos, indicando a comprovação de “atuação diligente”.

No entanto, alguns participantes da oficina expuseram a preocupação de que a compreensão do dever de cuidado como obrigação de meio possa colidir com a noção de “falha sistêmica” (conectada especificamente ao dever de cuidado no caso de crimes graves, e não à atuação diligente no âmbito da publicidade paga ao provedor).

Para ilustrar essa incerteza, foram lembrados pronunciamentos ao longo do julgamento no Supremo Tribunal Federal que, embora não tenham constado no texto definitivo da tese, sugeririam uma leitura finalística da responsabilidade. Sob essa perspectiva mais estrita, a constatação de um volume expressivo de conteúdos ilícitos em circulação bastaria para caracterizar a ineficácia do sistema e deflagrar a responsabilização da plataforma, convertendo a avaliação dos meios em uma verificação retrospectiva de resultados.

Desse modo, apontou-se a existência de uma zona de indeterminação que tensiona a aplicação do dever de cuidado, uma vez que a sua qualificação como padrão procedimental convive com uma pressão voltada ao controle quantitativo de publicações pelo conceito de falha sistêmica. Essa indeterminação interpretativa gera a possibilidade de que a verificação de conformidade abandone o exame da higidez dos processos internos de moderação e passe a exigir uma garantia de erradicação de irregularidades, levando o debate, novamente, para o escopo de uma obrigação de resultado.

Como se verá adiante, emergiu como dúvida entre os participantes quais seriam as métricas mais adequadas para atestar a falta de êxito “sistêmico” da plataforma, o que gerou percepções de incerteza jurídica e abertura para discricionariedade na fiscalização. Em especial, esta dúvida se conectou, na discussão das oficinas, à compreensão de que a obrigação prescrita às plataformas pelo dever de cuidado não recai sobre a fiscalização individual de conteúdos ilegais analisados isoladamente, como afirmado de forma explícita pela tese publicada pelo STF e pelo próprio novo artigo 16-B, §3º, agora parte do Decreto 8.771/2016.

parâmetros para aferição “sistêmica” e seus desafios

Uma série de intervenções de participantes ocorreram no bojo do debate sobre as melhores métricas para aferição de falha (ou êxito) sistêmico no âmbito do novo regime de responsabilização estabelecido pelo STF e detalhado nos decretos publicados pelo Poder Executivo. Neste ponto, o mesmo artigo 16-B do Decreto 8.771/2016, em seu §1º, aponta que incorre em “falha sistêmica” o provedor que não comprove medidas adequadas de prevenção e remoção que “forneçam, conforme o estado da técnica, os níveis mais elevados de segurança” (inciso I) e “inibam a circulação massiva dos conteúdos” ilícitos indicados (inciso II). Neste ponto, o debate circundou o possível significado regulatório do conceito de “circulação massiva”.

Essa abordagem partiria da premissa estabelecida na tese do STF e no citado artigo 16-B, §3º, do Decreto 8.771/2016 de que, diante da escala do ambiente digital, uma atuação responsável não pode ser aferida pela ausência absoluta de falhas, mas sim pela demonstração de que tais falhas representam episódios isolados, uma parcela residual e não representativa do universo total de conteúdos. Como se verá adiante, a padronização neste caso foi vista como chave para a consolidação de um ambiente de segurança jurídica.

Uma experiência aventada no debate nas oficinas foi a métrica de “prevalência” para aferição do êxito na diligência das plataformas na moderação de conteúdo. Implementada em um caso específico no âmbito do setor privado, a métrica estimaria o percentual de vezes que usuários visualizam eventual conteúdo ilícito/violador em oposição ao total de visualizações de qualquer tipo de conteúdo,⁵ representando uma primeira tentativa, no âmbito de um serviço, de produzir uma fração com numerador e denominador para escrutínio da atividade de moderação. Contudo, participantes relataram se deparar com desafios no acolhimento deste tipo de metrificação na discussão judicial de casos concretos, apontando mais uma

⁵ Douek, Evelyn, Content Moderation as Systems Thinking (Janeiro, 2022). Harvard Law Review Vol. 13. Disponível em: <https://harvardlawreview.org/print/vol-136/content-moderation-as-systems-thinking/>

vez para um terreno de incertezas quanto aos padrões técnicos aplicáveis para avaliação do nível de diligência e efetividade de sistemas de segurança implementados por diferentes provedores.

Participantes também debateram as lacunas estruturais quando da construção de parâmetros *ex ante* para aferição de “falhas sistêmicas”, especialmente quando da emergência de novas tendências comportamentais entre usuários, termos cifrados e mobilizações atípicas de conteúdo por usuários de plataformas. Esses fenômenos de inovação foram apontados como potencialmente capazes de contornar arquiteturas consolidadas de moderação, seja pela velocidade com que se disseminam, seja pela facilidade de se camuflarem em meio a discursos aparentemente lícitos.

Como ilustração concreta, citou-se o emprego da expressão “festa da Selma” no caso da articulação de atos em 8 de janeiro de 2023, evidenciando dificuldades para antever, de forma prévia e exauriente, conteúdos codificados que emergem de maneira imprevista no debate público e podem incorrer em ilícitos contidos na lista de dever de cuidado. A diversidade e a imprevisibilidade de tendências na produção de conteúdo foram apontadas, deste modo, como características das dinâmicas digitais também a serem consideradas pela regulação.

limitações operacionais no cumprimento das obrigações e suas consequências

Em razão da avaliação regulatória dos meios e, possivelmente, dos resultados da moderação de conteúdo, surgiu entre os participantes das oficinas uma discussão sobre as expectativas sobre as capacidades operacionais que recaem sobre diferentes provedores neste âmbito. De um lado, participantes relataram a percepção pelo poder público e pela sociedade civil de que a contratação massiva de novos trabalhadores parecia a resposta adequada para dar conta da verificação prévia de anúncios que escapam à detecção ou da moderação de conteúdo em geral. De outro, outras vozes apontaram para os obstáculos práticos que tornam essa expectativa difícil de conciliar com a realidade da economia digital, da complexidade e do volume exigido na atividade de moderação de conteúdo e de diferentes portes de provedores de aplicação de internet.

Paralelamente, o papel da inteligência artificial (IA) nesse processo de verificação e moderação suscitou também um debate relevante. Os participantes identificaram uma ambiguidade sobre o papel da IA: se, tradicionalmente, prevalece um ceticismo quanto ao uso de IA em contextos regulatórios, observa-se, ao mesmo tempo, uma tendência crescente de inúmeros atores sociais a defendê-la como solução capaz de superar todas as limitações operacionais da moderação, como se o recurso à IA permitisse, em tese, a verificação integral da totalidade dos anúncios e conteúdos veiculados. Em visão exposta especialmente por participantes do setor privado, tanto a contratação em larga escala de trabalhadores quanto o uso massivo de IA, quando apresentados como “soluções definitivas”, revelam-se propostas inviáveis e desconectadas das dinâmicas concretas do mercado digital. Destacaram, inclusive, que ambas as iniciativas acentuam a complexidade dos processos de atendimento a requisitos regulatórios, e que ambas suscitam questões adicionais que podem impactar negativamente as atividades voltadas a dar concretude ao dever de cuidado.

A partir destas pretensões de “solução definitiva”, participantes de diferentes setores discutiram a evolução jurisprudencial sobre um eventual dever de monitoramento prévio do conteúdo exibido aos usuários (citaram, assim, entendimento prevalente do Superior Tribunal de Justiça na última década, que considerava o tal dever de monitoramento prévio como alheio à essência dos serviços oferecidos pelas plataformas digitais). De maneira crítica, avaliou-se que essa interpretação parece hoje superada pela inclinação do Judiciário a reconhecer o monitoramento prévio como elemento constitutivo dos serviços digitais, ao menos se reservado a determinadas categorias de conteúdo mais sensíveis.

Nesse sentido, múltiplos participantes convergiram na percepção de que se faz necessário delimitar este dever de monitoramento prévio (agora conectado à ideia de dever de cuidado ou de atuação diligente), estipulando critérios objetivos sobre o que é exigível das plataformas, com atenção às limitações de suas capacidades técnicas e viabilidade dos modelos de negócios legítimos. Destacou-se que essa delimitação do monitoramento prévio

seria uma maneira de fortalecer e otimizar esforços na concretização da decisão do STF, em contraposição a um cenário atual de exigências erráticas entre diferentes autoridades (que atualmente adotam interpretações próprias e discrepantes entre si em relação ao que o dever de cuidado implica) e um nível de imprevisibilidade que prejudica a capacidade de as plataformas responderem adequadamente. Destacou-se também que essa delimitação é crucial para evitar que direitos fundamentais sejam, de forma desproporcional, fragilizados, em especial diante dos riscos do monitoramento prévio para a privacidade e a liberdade de expressão.

Do ponto de vista de plataformas de *marketplace*, tal moderação impactaria diretamente a fonte de renda de diferentes atores econômicos de diferentes portes, podendo mesmo implicar retaliações legais para a plataforma em decisões de remoção, incentivadas pelo dever de monitoramento prévio em seu desenho atual, carente de parâmetros mais objetivos.

riscos sistêmicos vs. falha sistêmica

Alguns participantes da segunda oficina também esboçaram a preocupação de interpretação de conceitos trazidos pela decisão do STF e aprofundados pelos decretos reguladores do MCI: a noção de riscos sistêmicos constante no artigo 16-C incluído no Decreto 8.771/2016. Enquanto em diplomas como o ECA Digital, pela própria natureza setorial da norma, os riscos a serem mitigados e tutelados pela moderação incluem o conteúdo passível de lesar crianças e adolescentes, participantes provocaram que não estão explícitos quais seriam os riscos sistêmicos mencionados pelo 16-C. O cenário comparativo também incluiu a referência ao *Digital Services Act* europeu e sua remissão a bens jurídicos a serem protegidos, como os processos eleitorais e a própria proteção da infância, concluindo-se que existe uma necessidade interpretativa de ancoragem desta atividade de detecção e mitigação de risco, sob pena de instrumentalização discricionária do dispositivo em diferentes hipóteses.

Outro ponto de tensão foi observado no fato de o artigo 16-C falar, de forma aberta, na detecção e mitigação de riscos, sem mencionar qualquer tipo de diferenciação por setor. Participantes da segunda oficina, dessa forma, questionaram a racionalidade e os benefícios de uma obrigação de mitigação de riscos universal e homogênea, tendo em vista as diferenças estruturais entre os modelos de negócios que sustentam as plataformas. Em termos práticos, portanto, alertou-se que os riscos vistos na atividade do comércio eletrônico são vastamente distintos daqueles vistos nas plataformas de redes sociais, por exemplo.

proteção de grupos vulneráveis

Houve consenso entre os participantes de que a operacionalização do dever de cuidado e o desenvolvimento de métricas de risco devem incorporar também a dimensão da vulnerabilidade diferenciada de grupos socialmente minorizados. Conteúdos que os vitimizam sistematicamente foram citados como categorias que demandam um escrutínio mais apurado por parte das plataformas, dada a recorrência e a gravidade dos danos que produzem.

Nesse sentido, foi sugerida uma abordagem de moderação em camadas, que reconheça a especificidade dos riscos enfrentados por ativistas, jornalistas e grupos historicamente vulneráveis, sem que isso implique a adoção de critérios arbitrários ou a supressão de discursos legítimos. A complexidade do tema foi ilustrada com o exemplo da disseminação não-consensual de imagens íntimas, em que a ilicitude não reside no conteúdo em si, mas na ausência de consentimento, exigindo, portanto, instrumentos de análise de contexto.

Vale a menção, nesse sentido, à abordagem do Decreto nº 12.976/2026 e seu enfoque no enfrentamento da violência contra mulheres no ambiente digital. A norma estabelece deveres específicos de moderação em camadas para essa categoria de conteúdo, incluindo prazos mais céleres de remoção, a obrigação de agir de ofício em casos de ataques coordenados e salvaguardas específicas para conteúdo íntimo gerado ou manipulado por inteligência artificial, reforçando a importância e a atualidade da abordagem proposta pelos participantes e evidenciando que a construção de parâmetros diferenciados para grupos em situação de vulnerabilidade segue como um ponto de atenção na esfera regulatória.

No âmbito deste decreto, participantes da oficina destacaram a necessidade de conferir maior densidade e delimitação aos conceitos normativos voltados ao enfrentamento da violência na internet. A atenção dos debatedores recaiu sobre a redação do artigo 3º, inciso II, que apresenta uma definição ampla de violência associada a um rol meramente exemplificativo de condutas e à previsão de prazos estritos para a atuação dos intermediários. Nesse contexto, delinear-se duas visões distintas acerca dos impactos práticos e regulatórios trazidos pelo dispositivo.

Por um lado, defendeu-se que o ato normativo teve o propósito legítimo de consolidar salvaguardas essenciais, assegurando que a proteção conferida pela legislação brasileira alcance de forma efetiva o espaço digital. Sob essa perspectiva, a previsão de um catálogo de hipóteses busca responder a desafios como o emprego de ferramentas de inteligência artificial para a manipulação de imagens íntimas e a ocorrência de assédio em redes sociais. A sistematização dessas condutas foi compreendida como um referencial para orientar a identificação rápida de agressões graves, reunindo ilícitos já previstos no ordenamento jurídico.

Por outro lado, manifestou-se preocupação com a indeterminação de categorias como ataques coordenados e condutas direcionadas a mulheres com visibilidade pública. Argumentou-se que a amplitude das definições pode induzir as plataformas a uma postura de remoção preventiva para afastar o risco de penalidades, gerando reflexos negativos sobre a liberdade de expressão. Em cenários que envolvem a cobertura jornalística, o debate político e o acompanhamento de mandatos eletivos, a ausência de balizas estritas para distinguir a ofensa ilícita da crítica contundente foi apontada como um elemento de incerteza capaz de ensejar a supressão de manifestações legítimas.

como fica o regime jurídico da responsabilidade civil no comércio eletrônico?

No âmbito dos deveres de diligência que envolvem ações proativas por parte de provedores de aplicação de internet, um dos principais temas debatidos entre os participantes foi a confusão gerada pelo regime jurídico aplicável ao comércio eletrônico e *marketplaces* estabelecido pela decisão do STF.

Como elemento de confusão, apontou-se que a tese fixada pelo Supremo possivelmente incorre em antinomia ao afirmar que não se admitirá a responsabilidade objetiva de provedores de aplicação de internet com a declaração de inconstitucionalidade parcial e progressiva do artigo 19 (item 12 da tese do STF), ao mesmo tempo em que institui que os provedores de aplicações de internet que funcionarem como *marketplaces* responderão civilmente de acordo com o Código de Defesa do Consumidor (CDC, Lei nº 8.078/1990) (item 7 da tese). Nesta hipótese, a atribuição de responsabilidade objetiva a *marketplaces* importaria também na implementação de um regime próprio de monitoramento ou filtragem prévia de conteúdo incompatível com o conteúdo da tese do STF, além de sequer estar previsto no ordenamento jurídico indicado pelo tribunal, qual seja, o CDC.

Participantes das oficinas apontaram que remeter todas os aspectos de responsabilização de *marketplaces* ao CDC seria, na prática, submetê-los a um regime de responsabilidade objetiva, o que contraria frontalmente a própria ressalva do item 12 da mesma tese. Estes participantes defenderam o afastamento da responsabilidade objetiva para os provedores quando não aplicáveis ao caso os elementos próprios das relações de consumo.

Assim, como um possível encaminhamento para promover clareza e segurança jurídica na interpretação da tese do STF, a discussão na oficina apontou para a necessidade de decisões judiciais que consigam diferenciar casos tipicamente abarcados pela legislação consumerista de casos governados especificamente por regras do Marco Civil da Internet sobre os quais dispõe a decisão do STF, sobretudo pelo aspecto do controle de conteúdo publicado por terceiros. Um critério proposto pelos participantes incluiu diferenciar danos estritamente de consumo, ligados a problemas de logística, entrega ou publicidade paga, de um lado, e danos de conteúdo, de outro, ou seja, aqueles ligados, por sua vez, à esfera do discurso.

O principal ganho conceitual e prático dessa divisão seria a separação clara entre os regimes de responsabilização, permitindo organizar os regimes propostos pela decisão do STF e

detalhados pelos decretos reguladores do MCI. Participantes da oficina, sob esse viés, destacaram que a consolidação formal desse tipo de diferenciação traria previsibilidade na aplicação pelas diferentes instâncias do Poder Judiciário e mais clareza para o setor privado e sociedade civil quanto a quando, de que modo e em quais circunstâncias operam os regimes de responsabilidade, demanda notável diante da pluralidade de regimes de responsabilização firmada na decisão do STF.

Na mesma toada de discussão sobre os principais riscos ao comércio eletrônico e à economia digital, participantes relataram a multiplicidade de casos nos quais provedores se vêem obrigados a identificar ilicitudes ou irregularidades técnicas em produtos cuja avaliação é desafiadora para os próprios órgãos estatais especializados.

Nestas situações, autoridades estariam delegando para atores privados uma atividade fiscalizatória do Estado (que, por sua vez, está mais equipado para conduzi-la por meio de tais órgãos especializados e do acesso a informações reportadas por força de inúmeras leis, materializadas, por exemplo, em obrigações tributárias ancilares). Relatou-se que a situação se agrava diante do entendimento que se dissemina de que plataformas de comércio eletrônico estariam sujeitas a um dever de monitoramento prévio de todo e qualquer anúncio ou conteúdo publicitário - incluindo, portanto, mais do que o monitoramento prévio de anúncios ofertados ou impulsionados mediante pagamento, como prescrito pelo texto da tese do STF e pelo artigo 16-K do Decreto 8.771/2016.

Como se verá nas seções adiante, o resultado apontado foi um cenário de insegurança jurídica significativa, em que as plataformas são levadas a antecipar o posicionamento de múltiplas autoridades sob pena de questionamento posterior, esbarrando em zonas cinzentas e matérias de alta complexidade técnica.

O que se observou, portanto, foi um incentivo de remoção de conteúdo ou de impossibilidade de comercialização de anúncios em caso de incerteza, o que favorece a sobre-remoção e ameaça a pluralidade de discursos (e, no âmbito comercial, ofertas) do ambiente digital. A crítica a tal fenômeno, na esfera do comércio eletrônico, foi ressaltada pelo fato de que a remoção preventiva ou indevida, para além de ferir a liberdade de expressão do usuário (como no caso de remoção indevida de conteúdo postado em redes sociais), pode atingir economicamente o anunciante, impactando o usuário em termos materiais e concretos. O exemplo de um microempreendedor ou pequeno vendedor lesado ou prejudicado pela remoção injustificada foi citado por parcela dos participantes para ilustrar um cenário em que bens jurídicos tão significativos quanto a liberdade de expressão, a tutela da concorrência e a livre iniciativa são atingidos por impactos não previstos da ação regulatória incerta. Importante assinalar, nessa esteira, que enquanto grandes empresas e vendedores possuem canais para reverter ou questionar suspensões indevidas, os pequenos lojistas tendem a serem mais impactados em razão de "falsos positivos" gerados por filtros preventivos, atingindo diretamente sua subsistência.

II. notificações extrajudiciais

A mudança no regime de responsabilidade das plataformas digitais promovida pela decisão do STF trouxe consigo implicações diretas sobre o funcionamento do regime de *notice and takedown*. Se antes o artigo 19 do Marco Civil estabelecia um modelo relativamente claro de acionamento das plataformas, o novo quadro suscitou questões sobre quem pode notificar, em que condições e com quais consequências, tanto para as plataformas quanto para os usuários afetados.

Os participantes das oficinas debateram sobre a nova natureza do regime de artigo 21 do MCI e em que medida se conformaria um novo regime “geral” de responsabilidade das plataformas. Um ponto central residiu na incerteza dessa transposição, dado que o artigo 21 foi concebido especificamente para disciplinar a divulgação não autorizada de conteúdo íntimo, e sua aplicação a outros ilícitos levanta questões ainda não resolvidas, como a de quem seriam os entes legitimados a produzir notificações extrajudiciais em contextos distintos daquele para o qual o regime foi originalmente desenhado. Um caso apontado como especialmente controvertido é o do conteúdo ligado ao discurso de ódio ou de natureza antidemocrática, cuja ilicitude produz danos de forma difusa e coletiva, sem que haja uma vítima claramente individualizável apta a exercer o papel de notificante pressuposto pela lógica do artigo 21.

Após a publicação dos decretos regulamentadores pelo Poder Executivo, a discussão aprofundou-se na natureza do regime de notificações proposto pelos arts. 16-D e 16-E do Decreto 8.771/2016.

De um lado, participantes apontaram a compreensão de que o paradigma apresentado pelo novo texto legal é o de *notice and action*, ou seja, uma sistemática em que do envio da notificação extrajudicial por vítima ou legitimado não decorre, necessariamente, a derrubada do conteúdo, devendo a plataforma tomar medidas para investigar a licitude e posicionar-se sobre a matéria, podendo manter o conteúdo notificado sem se sujeitar a responsabilização caso haja dúvida razoável. Em outros termos, plataformas não estão obrigadas a remover todo e qualquer conteúdo sujeito a notificação, cumprindo o conceito de dúvida razoável papel fundamental em garantir que as plataformas possam demonstrar que não se fizeram inertes ao conteúdo possivelmente ilegal.

Outra parcela de participantes, contudo, reconheceu que, sem parâmetros concretos para estabelecer o que constitui a dúvida razoável, tal previsão normativa pode se tornar esvaziada e estabelecer, em termos concretos e práticos, um ônus de remoção de conteúdo, transferindo o cenário para um regime de *notice and take down* aos moldes do discutido na primeira oficina.

Assim, diante da dificuldade técnica de aferir a regularidade do conteúdo, da própria incerteza quanto aos critérios de conduta para os provedores e da pressão pelo cumprimento de notificações extrajudiciais, ainda que controvertidas, diversos participantes da oficina enfatizaram a preocupação com o cenário em que a remoção de conteúdo tenda a se tornar a resposta padrão dos provedores. Mais especificamente, a preocupação expressa é de que o esforço de remoção extrapole o conteúdo indevido e produza *sobrerremoção*, levando à remoção também de conteúdo legítimo. Destacou-se o potencial lesivo dessa dinâmica para a liberdade de expressão, a qual deveria ser protegida e buscada mesmo em casos limítrofes ou de difícil classificação (por exemplo, da crítica jornalística a conteúdos que envolvam discurso de ódio, uma vez que a remoção indiscriminada de todas as postagens que veiculam um dado conteúdo poderia suprimir exatamente o discurso que o denuncia).

Nesse sentido, foi levantada a preocupação de que provedores orientados prioritariamente pela mitigação de riscos jurídicos possam ser levados a remover conteúdos minimamente questionáveis de forma preventiva, sem uma avaliação adequada de sua finalidade e contexto, invertendo, na prática, a lógica que deveria presidir a relação entre moderação de conteúdo e preservação do debate público. Representantes da sociedade civil também sublinharam que os efeitos da *sobrerremoção* são fortemente sentidos por ativistas e jornalistas, cujos conteúdos, por sua natureza polêmica ou denunciativa, são particularmente vulneráveis a classificações imprecisas por sistemas automatizados de moderação que não captam a finalidade ou o contexto do discurso.

instrumentalização de notificações extrajudiciais para fins abusivos

Considerando que o novo regime amplia o rol de hipóteses sobre as quais incide o regime de notificações, a discussão abarcou questionamentos sobre a ausência de barreiras para que atores econômicos se valham de notificações extrajudiciais para promover a remoção de anúncios lícitos de seus concorrentes, sob a justificativa de combate à pirataria ou a irregularidades técnicas, por exemplo. Diante desse quadro, foi manifestada preocupação acerca de como coibir que pessoas naturais e jurídicas instrumentalizem o mecanismo de notificações para fins alheios à vedação de conteúdo indevido. Destacou-se que qualquer solução nesse sentido também deve levar em conta que pedidos com propósito anticoncorrencial podem se originar não apenas de uma empresa concorrente como pessoa jurídica, mas mesmo de pessoas físicas, associações de classe e outras organizações que sejam instrumentalizadas para tal finalidade.

Além de usos anticoncorrenciais, os participantes também externaram preocupação com outros tipos de instrumentalização a que a ampliação do regime de notificações torna os provedores suscetíveis. Em especial, destacou-se o risco de que pessoas naturais ou jurídicas denunciem anúncios por questões puramente de preferência ou ideologia, como forma de manifestar sua oposição à venda daquele produto. Como levantado nas oficinas, casos como estes não deveriam constituir uma base suficiente para remoção do conteúdo e consequente impedimento da venda, mas, na prática, pela abertura das hipóteses em que o regime passa a ser admitido, o cenário de sobre remoção pode ocorrer. Assim, no limite da interpretação literal do novo quadro regulatório, ofertas de produtos lícitos estariam sujeitas a serem suprimidas por mero desagrado a um único consumidor.

Nesse sentido, participantes também destacaram o risco de que pedidos de remoção de conteúdo encubram outros conflitos de interesse que nem sempre são imediatamente visíveis. Um exemplo citado foi de conteúdo envolvendo menores de idade, para os quais a narrativa de "proteção da criança" chega a ser invocada por responsáveis legais solicitando a derrubada do conteúdo, mas cujo interesse real pode ser a preservação da própria reputação familiar diante de críticas sobre a forma como expõem seus filhos nas plataformas. Nesses casos, a remoção solicitada poderia não corresponder ao melhor interesse do menor, mas à conveniência de quem, originalmente, autorizou e se beneficiou de sua exposição. Essa dimensão do debate reforçou os questionamentos sobre os limites do papel de provedores como executores de pedidos de remoção em contextos nos quais a identificação do interesse legítimo a ser protegido é, por si só, uma tarefa complexa.

desafios em notificações enviadas por autoridades públicas

Conexo a esse cenário, participantes também identificaram uma tendência de expansão do escopo das notificações extrajudiciais formuladas por entes governamentais. A percepção compartilhada foi de que a tese do STF, combinada com as balizas ainda em processo de consolidação decorrentes do novo regime, tem criado um ambiente de ambiguidade interpretativa que, na prática, amplia progressivamente o alcance das requisições de remoção por agentes públicos. Nesse contexto, foram relatadas situações em que as notificações avançam sobre conteúdos cuja ilicitude não é evidente ou incontroversa.

A essa percepção somou-se uma preocupação de ordem operacional relativa à forma como parte dessas notificações vem se apresentando. Participantes relataram o envio, por parte de atores governamentais, de listas contendo centenas de itens a serem removidos, frequentemente geradas a partir de buscas feitas por palavras-chave. Esse método, embora compreensível diante do volume de conteúdo circulante nas plataformas, suscitou interrogações por parte dos participantes acerca do contexto em que as palavras-chave identificadas efetivamente ocorrem, e, por consequência, sobre a adequação e a legalidade de todas as remoções solicitadas.

Um ponto de tensão adicional relatado por participantes do setor privado diz respeito a desafios na interlocução com as autoridades notificantes, sejam elas de caráter técnico ou não. Diante de pedidos de remoção inespecíficos ou mesmo possivelmente equivocados quanto ao conteúdo tido como indevido, cabe aos provedores contestar tais pedidos sob o fundamento de que o conteúdo em questão seria lícito e, mais do que isso, que sua remoção

seria prejudicial e injustificada aos seus usuários (inclusive os que seriam anunciantes, no caso de *marketplaces*).

No entanto, segundo os participantes, tais contestações dificilmente recebem respostas fundamentadas por parte dos órgãos requisitantes (em certos casos, não há qualquer resposta), assim colocando os provedores diante de um dilema prático. De um lado, haveria a opção de manter o conteúdo e sujeitar-se ao risco de responsabilização. De outro lado, teriam a alternativa de remover o conteúdo preventivamente, sob o risco de cercear direitos do usuário publicador do conteúdo (sua expressão ou sua capacidade de oferecer produtos lícitos em um *marketplace*, por exemplo) e de, no limite, também serem responsabilizados em ação judicial movida pelo usuário que teve sua publicação removida.

Diante desse dilema, tais participantes relataram que as plataformas frequentemente se veem pressionadas a optar pela remoção preventiva de conteúdo, o que ameaça a preservação de conteúdos legítimos e incorre no já relatado risco de sobre-remoção, outro tema central do debate.

o encaminhamento de dados ao Poder Público

No âmbito das discussões sobre os fluxos de notificação e cooperação com o Poder Público, debateu-se a interpretação a ser dada ao novo artigo 16-H do Decreto nº 8.771/2016, que importa no encaminhamento de informações sobre condutas criminosas para autoridades. Com efeito, o artigo representa uma inovação em relação à tese do STF sobre o tema 987 que recebeu atenção na segunda oficina realizada.

Parte dos participantes sugeriu que o mecanismo de compartilhamento extrajudicial de dados deve buscar inspiração em experiências consolidadas no direito comparado, a exemplo do modelo norte-americano do *National Center for Missing and Exploited Children*. A finalidade dessa abordagem seria autorizar o encaminhamento direto e célere de dados unicamente em conjunturas emergenciais, caracterizadas por risco iminente à vida e à integridade física, sendo os casos de ameaças de ataques armados em escolas citados como exemplo paradigmático destes momentos emergenciais.

Integrantes da oficina expressaram ressalvas quanto à redação ampla e indeterminada conferida ao dispositivo, alertando para os riscos decorrentes de uma interpretação flexível do artigo. Argumentou-se que a ausência de balizas procedimentais estritas pode converter uma ferramenta voltada à resposta emergencial e extraordinária em uma rotina de monitoramento ativo e vigilância preventiva pelas plataformas. Sob essa perspectiva crítica, reforçou-se que o repasse de informações de autoria e registros de conexão sem determinação judicial deve ser condicionado a parâmetros regulatórios objetivos, preservando as garantias constitucionais de privacidade e o devido processo legal.

a “dúvida razoável”

O conceito de dúvida razoável foi amplamente valorizado pelos participantes da segunda oficina como um instrumento indispensável para o equilíbrio e a operacionalização do novo regime de notificações. No modelo de *notice and action*, a dúvida razoável foi descrita como uma salvaguarda proporcional que impede a conversão da notificação extrajudicial em uma obrigação de remoção imediata. No âmbito do comércio eletrônico, argumentou-se que a delimitação desse instituto é fundamental para conter incentivos à remoção indevida de ofertas lícitas, evitando que intermediários privados sejam forçados a assumir funções judicantes sobre temas controversos ou que exigem expertise técnico-regulatória e assegurando que as plataformas possam analisar a procedência das denúncias com a devida cautela jurídica.

No que diz respeito à aplicação prática da dúvida razoável, os debates na oficina delimitaram duas searas principais de incidência do conceito. A primeira delas abrange as hipóteses de incerteza técnica, nas quais a verificação da regularidade da oferta presente na publicação depende de informações detidas pelo Poder Público. Foram citados como exemplos, assim como na discussão exposta cima sobre os deveres das autoridades, os anúncios de locação imobiliária cuja conformidade pressupõe a checagem de dados municipais de zoneamento e políticas habitacionais, bem como a oferta de produtos sujeitos à fiscalização de agências

reguladoras que não mantêm repositórios estruturados para consulta. Nessas situações, a ausência de informações impede que o provedor ateste a (i)licitude por meios próprios, legitimando a manutenção do conteúdo sob o amparo da dúvida razoável.

A segunda seara compreende os cenários de incerteza jurídica e contextual, com ênfase em publicações associadas à liberdade de expressão, matérias jornalísticas e manifestações de crítica pública. Abrangeria, assim, as controvérsias que envolvem eventuais erros informativos ou interpretações conflitantes sobre ilicitude que estejam suscitando entendimentos jurisprudenciais diversos, por exemplo. Com efeito, participantes sustentaram que a existência de dissensos no próprio Poder Judiciário acerca da ilicitude de determinados discursos representa uma evidência de dúvida razoável, servindo como baliza para evitar que as plataformas realizem a supressão preventiva de manifestações legítimas diante de notificações extrajudiciais.

requisitos para localização inequívoca do conteúdo

No âmbito das discussões sobre a materialização das notificações extrajudiciais, a oficina explorou uma tensão crescente sobre o papel da URL (*Uniform Resource Locator*) como instrumento de identificação de conteúdos ilícitos. Tradicionalmente concebida como unidade básica de referência / padrão ouro nas ordens de remoção, a URL tem sido progressivamente desafiada e substituída por outros métodos de identificação do conteúdo, como hashtags, palavras-chave e correspondências por hash. Essa transição foi descrita pelos participantes como uma mudança estrutural no modo como as autoridades públicas têm materializado suas requisições.

Ainda que se admita que a mudança tenha um intuito válido de reagir à velocidade e escala com que conteúdos ilícitos são replicáveis no ambiente digital hoje, é notável que os novos métodos de identificação de conteúdo passariam a operar com um grau de imprecisão e incerteza para o usuário consideravelmente maior. No caso de *hashtags*, por exemplo, trata-se de uma técnica que pode ser livremente empregada por qualquer usuário, em qualquer tipo de conteúdo, para aumentar o alcance da sua publicação e conectá-la a determinado público, ainda que não haja relação entre as palavras em hashtag e o conteúdo efetivo da publicação.

Para alguns participantes das oficinas, essa discussão assume contornos ainda mais concretos no âmbito do comércio eletrônico, pois a ausência de indicação de URLs em ordens ou notificações torna significativamente mais complexa a individualização de um produto irregular em meio a milhares de anúncios similares, convertendo o cumprimento de tais ordens de remoção em tarefa de difícil cumprimento.

Ainda, uma consequência central identificada por determinados participantes em relação ao progressivo abandono do modelo baseado em URLs é o esvaziamento da análise contextual para remoção de conteúdo. Neste caso, apontam que a URL permite compreender o exato entorno contextual da publicação, essencial para uma análise proporcional à conduta e ao conteúdo em questão. Estes participantes apontaram que o tema ganha especial relevância a partir do item 3.2 da tese do STF, segundo o qual "conteúdo idêntico" ao já reconhecido como ofensivo por decisão judicial sujeita as plataformas à remoção por notificação judicial ou extrajudicial.

Quais seriam os critérios para um conteúdo ser considerado idêntico a outro? Na visão de determinados participantes, essa formulação aberta corre o risco de negligenciar nuances inerentes ao discurso. Um mesmo conteúdo pode assumir significados radicalmente distintos conforme o enquadramento e a perspectiva sob os quais é apresentado, seja em um registro jornalístico, crítico, irônico ou de *counter-speech*. No caso dos *marketplaces*, a mera coincidência de palavras-chave entre dois produtos não garante que sejam idênticos e pode, inclusive, indicar intuítos opostos. É a análise contextual e pormenorizada de cada anúncio que permite distinguir, por exemplo, entre um produto que faz apologia ao crime e outro que o denuncia - diferenças frequentemente sutis. Descartar o contexto inviabiliza essa distinção, o que configura uma preocupação central para os participantes, pelo potencial de suprimir discussões legítimas nas plataformas, elevar o índice de falsos positivos e produzir efeitos colaterais significativos sobre a liberdade de expressão.

Para além do diagnóstico sobre a erosão do modelo baseado em URL, os participantes se voltaram a uma questão prospectiva acerca de quais critérios deverão orientar a identificação de conteúdos ilícitos em um ambiente digital em acelerada transformação. Se a migração para *hashtags*, palavras-chave e correspondências por *hash* já representa um desafio considerável em termos de precisão e contextualização, o avanço dos ambientes de IA generativa torna esse problema ainda mais complexo.

Nesses novos serviços, o próprio conceito de conteúdo identificável por uma unidade discreta de referência perde progressivamente sentido, na medida em que o conteúdo pode ser gerado de forma dinâmica, personalizada e irrepetível, dificultando ainda mais a tarefa de identificação. Embora ideias tenham sido esboçadas enquanto novas abordagens participantes sinalizaram que a eventual “superação” do paradigma da URL exige a construção de novos critérios de identificação que sejam, em algum grau, precisos, tecnicamente viáveis e juridicamente seguros.

As oficinas também refletiram tensões entre a celeridade esperada no cumprimento das ordens de remoção e a necessidade de um devido processo estruturado na verificação da ilicitude do conteúdo, com salvaguardas aos direitos e garantias individuais dos usuários. Os participantes sublinharam a dimensão jurídica dessa tensão, na medida em que o modo como as requisições de remoção são formuladas e transmitidas tem reflexos diretos sobre a qualidade e a proporcionalidade das remoções efetivamente realizadas.

Nesse contexto, os participantes discutiram como deve ser distribuído, entre os diferentes atores envolvidos no processo de notificação, o ônus de identificar com precisão o conteúdo considerado ilícito e o alcance das medidas solicitadas. A preocupação manifestada foi evitar que essa tarefa recaia exclusivamente sobre um único elo da cadeia, especialmente sobre o provedor responsável por processar notificações ou cumprir ordens judiciais. Nesse sentido, foram considerados pertinentes modelos que distribuam de forma mais clara os deveres de identificação, fundamentação e execução entre os atores que participam do processo, desde a formulação da requisição até o seu cumprimento.

III. governança, *enforcement* e o papel do setor público

Ao longo da oficina, emergiram um conjunto de percepções sobre o crescente protagonismo de diferentes órgãos públicos em temas digitais e sobre o papel cada vez mais relevante que diversas instâncias regulatórias têm sido chamadas a desempenhar, um quadro que evidencia a oportunidade, e mesmo a necessidade, de fortalecer espaços de articulação capazes de coordenar e orientar essa atuação, hoje difusa.

No Poder Executivo Federal, identificou-se que essa atuação tem se distribuído entre órgãos como a Agência Nacional de Proteção de Dados (ANPD), instituição em processo de ampliação de competências com a entrada em vigor do ECA Digital e dos próprios decretos reguladores do MCI, o Conselho Administrativo de Defesa Econômica (CADE), a Agência Nacional de Telecomunicações (Anatel), a Advocacia-Geral da União, estendendo-se ainda para os órgãos de defesa do consumidor e os diversos ministérios e secretarias do Poder Executivo, refletindo a transversalidade adquirida pela agenda nos últimos anos e sua pluralidade institucional.

A esse cenário foi acrescentada a participação do Poder Judiciário, especialmente do STF, exemplificada no próprio julgamento sobre o artigo 19 do MCI, e do Tribunal Superior Eleitoral, o qual assumiu papel de destaque na regulação de conteúdo digital, alcançando por vezes questões que transcendem o domínio estritamente eleitoral. Diferentes instâncias do Judiciário também foram mencionadas por serem já bastante invocadas (em tendência possivelmente ampliada pelo novo regime regulatório) a apreciar questões digitais de notável complexidade técnica. A supressão da necessidade de ordem judicial descumprida para a caracterização de danos individuais trazida pela decisão do STF, associada à facilidade de propositura de ações em larga escala com o auxílio de ferramentas de IA, foram apontados como fatores novos que devem ter efeitos significativos nos próximos anos.

a ANPD como autoridade para o ambiente digital: tensões e riscos

Um dos grandes pontos de debate entre os participantes da segunda oficina foi a governança institucional do novo regime de regulação e o *enforcement* das normas legais. De modo geral, podem ser descritas duas visões sobre o novo momento após a decisão do STF e os decretos editados pelo Executivo.

De um lado, alguns participantes interpretaram a designação da ANPD como um possível fator de um regime mais centralizado, menos fragmentado e com maior segurança jurídica (foi apontado como um elemento positivo o fato que a designação da ANPD acompanhou a tendência já estabelecida na regulação do ECA Digital e permitiu que as novas regras do Marco Civil da Internet fossem harmonizadas com os marcos legais já existentes). Sob esse viés, portanto, a centralização de competências regulatórias e fiscalizatórias na ANPD opera como um movimento central na garantia de segurança jurídica e efetividade das normas, ainda que em um processo gradual de construção de regulação e legitimidade da instituição.

Outros participantes, contudo, elencaram ceticismo quanto à ideia de que o *enforcement* da ANPD poderá encerrar, em curto ou médio prazo, uma tendência de fragmentação institucional e sobreposição na atuação de autoridades públicas. O exemplo do período imediatamente subsequente à aprovação da LGPD foi citado como um momento de pluralidade de atores públicos em ação que demonstra como a descoordenação pode, sim, ocorrer. O caso da Lei Anticorrupção (Lei nº 12.846/2013) foi citado como um exemplo de regime legal que, permissivo da pluralidade de ações e vias institucionais para sua operacionalização, teria testemunhado um momento inicial de descoordenação, apenas enfrentado a partir da cooperação técnica entre diferentes instituições públicas.

Outro exemplo elencado pelos participantes aderentes a uma visão mais otimista do novo modelo de arquitetura institucional foi o do CADE e o desenvolvimento do sistema concorrencial brasileiro. A conclusão apresentada foi de que, apesar dos desafios na construção do Conselho, o CADE tornou-se, com o passar dos anos e por meio de esforços de seu corpo técnico e liderança política, uma autoridade administrativa importante e com legitimidade respeitada por outros atores públicos, em especial o Poder Judiciário,

apresentando um possível caminho a ser seguido pela ANPD. Outros participantes, contudo, objetaram essa interpretação, apontando que a trajetória institucional do CADE foi marcada por diversos desafios, inclusive conflitos de competência com o Poder Judiciário e revisão de decisões tomadas pela autarquia por outras instâncias, demonstrando que a fragmentação também foi uma tendência notável no desenvolvimento histórico da instituição. Tal visão crítica foi somada à ideia de que, já nos dias de hoje, a ANPD aparece como co-ré, junto de plataformas digitais, em ações civis públicas, indicando um possível confronto com a legitimidade regulatória e decisória da agência.

Assim, a fragmentação institucional foi vista por parte dos participantes como possibilidade real e séria, indicando que múltiplas autoridades, especialmente aquelas com presença em diferentes níveis federativos e descentralizadas, como Ministérios Públicos e Procons, se sobreponham na aplicação do Marco Civil, com interpretações dissonantes e variadas dos diversos conceitos indeterminados estabelecidos no direito brasileiro após a decisão no Supremo no tema 987.

No caso do Sistema Nacional de Defesa do Consumidor - cuja atuação descentralizada em centenas de Procons municipais e estaduais e entidades da sociedade civil decorre de competências normativas consolidadas pelo Código de Defesa do Consumidor e reconhecidas pelos aditivos de 2026 ao Decreto nº 8.771 de 2016 -, participantes destacaram a existência de uma sobreposição complexa entre a tutela de direitos prevista no Marco Civil da Internet e a legislação consumerista. Sem mecanismos que assegurem algum tipo de deferência aos parâmetros técnicos fixados pela ANPD, o ecossistema digital poderá estar exposto a exigências simultâneas e conflitantes no âmbito da moderação de conteúdos.

Outro ponto de tensão institucional destacado pelos participantes diz respeito à assimetria entre as dinâmicas e os prazos de atuação dos órgãos públicos envolvidos na governança digital. De um lado, a ANPD opera em um horizonte regulatório de médio e longo prazo, fundamentado em agenda regulatória, ritos deliberativos colegiados, tomadas de subsídios e consultas públicas voltadas à consolidação gradual de entendimentos técnicos. De outro lado, órgãos de cúpula da administração direta, a exemplo do Ministério da Justiça e da Advocacia-Geral da União, atuam sob um horizonte executivo vertical e concentrado na resposta imediata a crises concretas de segurança ou repercussão pública.

Os participantes enfatizaram, assim, que a ausência de canais de articulação formal entre a gestão mais emergencial conduzidas por atores públicos e o planejamento regulatório estrutural da ANPD também pode gerar insegurança jurídica e antinomias, submetendo os provedores a exigências operacionais divergentes formuladas de modo simultâneo pelo próprio Estado.

visões sobre uma agenda de deferência regulatória

A tensão sobre o grau de centralização ou fragmentação regulatória implicou debates sobre a pertinência de uma “deferência regulatória”, representada pela construção de legitimidade da ANPD em diferentes papéis. Este debate suscitou dúvidas relevantes acerca do grau de aceitação que suas orientações técnicas receberão de outros atores estatais, por exemplo.

Foi apontado que a opção da agência pela edição de guias orientativos em lugar de resoluções de caráter estritamente normativo, a exemplo do que ocorreu na implementação inicial do ECA Digital, levanta questionamentos sobre a força vinculante desses instrumentos perante o Poder Judiciário. A preocupação central reside na possibilidade de que juízes de primeiro grau e juzados especiais cíveis, por exemplo, desconsiderem as diretrizes técnicas emanadas pela autoridade, mantendo uma interpretação autônoma e fragmentada sobre o que constitui a devida diligência no cumprimento do dever de cuidado. Na emergência deste cenário, surgiu o questionamento de qual seria a devida diligência prescrita pela lei: se a exigida pelas instituições judiciais ou a recomendada pela ANPD em viés administrativo.

Diante da necessidade de estabilizar o ambiente regulatório sem aguardar os longos prazos de maturação observados historicamente em outras autarquias, discutiram-se ferramentas capazes de acelerar a legitimidade regulatória e decisória da ANPD. Os participantes convergiram sobre a mera edição de recomendações consultivas possivelmente não ser

suficiente para ancorar a autoridade da agência sobre padrões técnicos, metodologias de detecção e mitigação de risco e medidas de diligência, tornando necessária a mobilização de instrumentos regulatórios que conectem estes requerimentos e padrões técnicos a necessidades públicas prementes.

Soluções diversas para este problema foram levantadas nas oficinas, com divergência entre setores. Entre as propostas, destacou-se a implementação de ambientes experimentais de regulação, conhecidos como *sandboxes* regulatórios, por exemplo. De outro lado, propugnou-se pela regulamentação efetiva do acesso a dados por pesquisadores independentes, conforme previsto no artigo 31 do ECA Digital. Argumentou-se que a criação de uma comunidade científica capaz de auditar atividades dos reguladores, relatórios de transparência e examinar os sistemas de moderação conferiria respaldo empírico às decisões da agência, fortalecendo sua autoridade perante o Judiciário, permitindo que entes da sociedade civil e da academia atuem também como atores importantes do processo de construção da ANPD, não estando alienados ao seu desenvolvimento.

dados públicos como insumo para o cumprimento de deveres de provedores

Alguns aspectos da atuação do setor público foram apontados por participantes como condição indispensável para a viabilidade do regime de responsabilidade e para o exercício efetivo da devida diligência pelas plataformas. Participantes relataram que o cumprimento de deveres de fiscalização sobre anúncios, ofertas e registros comerciais esbarra, por vezes, na opacidade das próprias informações apresentadas por autoridades públicas. Agências e órgãos reguladores, a exemplo da Anvisa, Inmetro, Susep e ANTT, rotineiramente divulgam documentos administrativos e fiscalizatórios sem padronização ou atributos técnicos que viabilizem uma compreensão da regularidade (ou irregularidade) e a capacidade de viabilizar o processamento de dados em escala por ferramentas de moderação dos provedores, por exemplo.

Assim, no âmbito do comércio eletrônico, a indisponibilidade de bases de dados abertas e estruturadas foi vista como capaz de induzir práticas de remoção preventiva e indiscriminada de anúncios. Diante desse gargalo, defendeu-se que o Estado tem a obrigação de disponibilizar repositórios públicos oficiais e qualificados⁶ ou formatos de consumo equivalente que permitam aos endereçados pelas obrigações legais analisar a licitude do conteúdo. Ressaltou-se que, na ausência de bases públicas funcionais e consumíveis por sistemas automatizados, a incerteza técnica decorrente da omissão estatal pode ser reconhecida como hipótese de dúvida razoável, excepcionando o dever de derrubada do conteúdo. Em mesmo sentido, foi apresentada a importância de canais, sistemas ou infraestruturas que permitam o diálogo entre plataformas e autoridades e a troca de informações e dados necessários para a derrubada de conteúdo ilícito.

Neste tema, um exemplo que foi mencionado por alguns participantes foi a parceria técnica celebrada entre o Banco Central do Brasil, o Ministério da Justiça e plataformas digitais para a triagem de anúncios financeiros, examinada como um estudo de caso relevante sobre a interlocução público-privada, discutida em diversos momentos da segunda oficina. Nesse arranjo, a autoridade fornece uma listagem estruturada de instituições autorizadas a ofertar produtos financeiros, permitindo que a plataforma utilize essa base oficial como critério de validação prévia e filtro de entrada para a veiculação de determinados tipos de publicidade na internet.

Embora o modelo tenha sido reconhecido como um avanço prático no combate a fraudes e um exemplo relevante de cooperação público-privada, houve intervenções que defenderam cautela quanto à expansão indiscriminada deste modelo. Foi levantada preocupação sobre a viabilidade de exigir uma verificação prévia semelhante para todas as categorias de publicidade digital, diante da escala e da diversidade de produtos e serviços ofertados na internet. Além disso, ressaltou-se que intermediários de menor porte não contam com a infraestrutura técnica nem com os canais institucionais necessários para celebrar convênios específicos com órgãos estatais.

⁶ Diversas sugestões foram levantadas nesse ponto, com especial preocupação para a integração dos dados governamentais aos sistemas de moderação de provedores em escala.

Outro caso elencado como problemático foi a da falta de infraestruturas e sistemas de diálogo entre plataformas e autoridades públicas para analisar a licitude de conteúdos e anúncios disponibilizados online. Um exemplo citado, nesse sentido, foi o da falta de tecnologias para comunicação e repasse de informações nos casos envolvendo a locação de imóveis classificados como Habitações de Interesse Social (HIS) no município de São Paulo: na análise de alguns dos participantes, a ausência de sistemas de contato entre plataformas e o poder público contribuiu significativamente para a circulação dos anúncios irregulares.

IV. recomendações e convergências

Embora algumas das ideias já tenham sido esboçadas ao longo do documento, esta seção desenvolve as principais recomendações convergentes no debate como um norte para próximos passos na discussão regulatória e judicial sobre deveres e responsabilidades de provedores de aplicação de internet e seu impacto para a economia digital e o comércio eletrônico.

autorregulação para padronização técnica

As possíveis contribuições que iniciativas de autorregulação poderiam apresentar para a construção de padrões técnicos legítimos de avaliação da diligência de provedores de aplicação de internet emergiu como uma das propostas de maior alcance estrutural do debate da primeira oficina, sendo discutido tanto em suas dimensões institucionais quanto em suas implicações práticas para a moderação de conteúdo e a responsabilização das plataformas. Alguns participantes aludiram à experiência do Conselho Nacional de Autorregulamentação Publicitária - CONAR⁷, cuja capacidade de produzir decisões técnicas reconhecidas pelo Judiciário foi apontada como referência relevante.

O racional da proposta é que iniciativas coletivas, dotadas de legitimidade setorial e conhecimento técnico especializado, contribuiriam para preencher certas lacunas que subsistem após a decisão do STF, oferecendo uma instância de referência para a interpretação e aplicação do dever de cuidado, por exemplo. Em comparação com os termos de uso individuais de cada plataforma, um órgão dessa natureza conferiria às diretrizes de moderação maior legitimidade social e *accountability*.

Um elemento central da proposta foi a defesa de que tais iniciativas não adotem uma estrutura monolítica, mas se organizem a partir de anexos setoriais que contemplem as especificidades de segmentos distintos, como o comércio eletrônico, redes sociais e os buscadores. Essa arquitetura permitiria que cada setor fosse avaliado a partir de critérios adequados à natureza de seus serviços e aos riscos que lhe são próprios, evitando a aplicação uniforme de parâmetros para realidades muito distintas. Para o setor de comércio eletrônico, em particular, essa diferenciação foi vista como especialmente relevante, dado que os desafios de moderação de anúncios e produtos apresentam complexidades técnicas próprias, distintas daquelas enfrentadas por plataformas de natureza predominantemente comunicacional.

Além de sua função normativa, o órgão proposto desempenharia um papel relevante na produção de precedentes administrativos capazes de orientar a atuação do Judiciário, especialmente na primeira instância. Nesse sentido, a criação de um acervo de decisões e diretrizes sobre casos complexos, as chamadas "zonas cinzentas", como a definição de produtos irregulares ou a classificação de discursos limítrofes, foi apresentada como um dos principais ganhos esperados do modelo, na medida em que estabeleceriam parâmetros mais objetivos para a aferição do cumprimento de deveres legais e possíveis falhas sistêmicas dos sistemas desenvolvidos por plataformas.

agenda de deferência regulatória para segurança jurídica

Diante da escolha de arquitetura institucional feita pelo Decreto 12.975/2026 de centralizar as competências regulatórias de fiscalização, transferindo a edição de orientações sobre o *enforcement* do Marco Civil da Internet para uma agência reguladora (a ANPD), participantes das oficinas consideraram fundamental propor medidas para garantir a legitimidade da agência em suas novas funções e evitar a sobreposição de determinações contraditórias de uma pluralidade de autoridades públicas.

⁷ O CONAR é uma organização não governamental sem fins lucrativos fundada em 1980, por iniciativa de entidades representativas do mercado publicitário brasileiro em resposta à ameaça de aprovação de legislação federal de censura prévia à publicidade, surgindo como produto voluntário da auto-organização do mercado publicitário. Vale destacar como instrumento normativo do CONAR o Código Brasileiro de Autorregulamentação Publicitária, o qual estabelece as normas éticas aplicáveis à elaboração e veiculação de anúncios publicitários em qualquer meio. É importante notar que o CONAR não é um órgão estatal e não dispõe de poder coercitivo em sentido estrito.

1. **Sandboxes.** Uma medida sugerida para esse propósito consiste na implementação de ambientes experimentais de testes, conhecidos como *sandboxes* regulatórios. Esses espaços de experimentação controlada permitem a avaliação empírica do funcionamento de novos modelos de negócios, ferramentas de inteligência artificial e soluções de moderação, viabilizando a produção de normas fundamentadas na prática e a calibração de salvaguardas antes da edição de resoluções definitivas. Na opinião de parte dos participantes, testes e experimentos de tal natureza poderiam operar como salvaguardas diretas de legitimidade para eventuais normas gerais e vinculantes da ANPD.

2. **Pesquisa e expertise.** Outra medida destacada nas discussões com alguma convergência foi a aproximação da ANPD com pesquisadores e *experts*. Além de ampliar o controle social, a formação dessa rede autônoma de pesquisa fortalece a legitimidade técnica e a autoridade da própria ANPD perante outros entes públicos. A fundamentação de diretrizes regulatórias e pareceres em diagnósticos empíricos produzidos por acadêmicos confere respaldo às decisões da autoridade administrativa, afastando alegações de arbitrariedade e blindando seus atos contra a anulação em ações judiciais. A produção contínua de evidências científicas transforma a regulação em um processo dinâmico e participativo, no qual a deferência institucional aos entendimentos da agência passa a ser sustentada pela consistência técnica das avaliações produzidas pelo ecossistema de pesquisa.

3. **Coordenação e articulação institucional.** Ainda, os integrantes da oficina sugeriram maiores debates multissetoriais sobre a construção de uma agenda desta natureza, com objetivo de buscar coordenação institucional e instrumentos que permitam assegurar a diminuição da incerteza jurídica e de demandas conflitantes entre diferentes atores do Poder Executivo, entre diferentes esferas federativas ou, ainda, disputas que emergem da interação com o Judiciário.

agenda de adequação e ações no Poder Público

As oficinas apontaram para a relevância da construção de uma agenda de adequação por parte do Poder Público, com ações proativas destinadas a liderar a construção de um novo ambiente regulatório, com novos papéis e responsabilidades. Compõem esta agenda as seguintes discussões:

1. **Transparência nas requisições produzidas pelo Poder Público.** Os participantes assinalaram a assimetria existente entre as obrigações de transparência impostas às plataformas e a ausência de exigências equivalentes dirigidas aos próprios atores públicos. Enquanto a decisão do STF determina a publicação de relatórios de transparência pelas plataformas, não haveria previsão análoga obrigando órgãos públicos ou outras entidades setoriais a divulgar dados sobre o volume, os critérios e os resultados de suas notificações e pedidos de remoção.

Os participantes sugeriram que a incorporação dessa exigência ao modelo regulatório contribuiria para equilibrar o sistema, tornando o processo de notificação mais rastreável e criando condições para uma avaliação bem informada de sua efetividade e legitimidade, em particular ao permitir o escrutínio sobre a fundamentação das notificações encaminhadas por órgãos públicos. Mais do que um mero paralelismo formal, a transparência institucional por parte dos atores públicos colaboraria para o alinhamento de expectativas entre os diferentes envolvidos, fomentando um diálogo institucional mais qualificado e permitindo que as plataformas desenvolvam arquiteturas de moderação mais alinhadas, desde sua concepção, às tendências e prioridades que orientam a atuação do poder público. Esse alinhamento poderia, inclusive, resultar em maior efetividade no endereçamento de conteúdos ilícitos disseminados em larga escala.

2. **Produção de bancos de dados públicos e de protocolos padronizados para interlocução com o setor público.** Participantes apresentaram a recomendação de que a exigibilidade de rotinas automatizadas de devida diligência sobre ofertas,

anúncios e conteúdos seja expressamente condicionada à disponibilização, pelo poder público, de repositórios oficiais estruturados, integráveis por meio de interfaces de programação de aplicações legíveis por máquina. A imposição de deveres preventivos de checagem em larga escala pressupõe a existência de dados estatais plenamente compreensíveis - e preferencialmente legíveis por máquinas - sobre registros sanitários, homologações técnicas, cassações de licenças e autorizações setoriais etc. Desse modo, na ausência de tais bases de dados, a impossibilidade técnica de validação automatizada deve ser reconhecida como hipótese de dúvida razoável.

Em complemento a essa infraestrutura de dados, sugere-se a estruturação de canais institucionais permanentes de interlocução operacional entre as autoridades públicas e as plataformas digitais. Esse ambiente integrado de cooperação deve viabilizar o repasse de informações qualificadas pelos órgãos reguladores e o fornecimento de respostas a consultas formuladas pelos provedores a respeito de ofertas ou conteúdos de licitude duvidosa. O estabelecimento desse fluxo bidirecional de comunicação reduz o risco de bloqueios preventivos indiscriminados, que prejudicam irregularmente os usuários e anunciantes, assegurando que as medidas de contenção ou remoção de conteúdos sejam respaldadas por orientações estatais claras e consistentes com os limites da atuação privada.

3. Proporcionalidade nas parcerias voluntárias. Os participantes também apresentaram a recomendação de que os acordos bilaterais de cooperação firmados entre provedores e órgãos setoriais sejam compreendidos como práticas específicas e voluntárias, sem necessária conversão em padrão obrigatório para todos os segmentos da economia digital. A transposição desse arranjo para a totalidade dos setores do comércio e da publicidade revela-se, discutivelmente, inviável, tendo em vista a extrema heterogeneidade das atividades econômicas e a inexistência de cadastros públicos centralizados para a totalidade das categorias de produtos e serviços.

Sob a perspectiva concorrencial e em atenção ao princípio da proporcionalidade previsto no artigo 16-P do Decreto 12.975/2026, a generalização desse modelo também apresenta potencial de aprofundar assimetrias entre os agentes do mercado. A celebração de convênios customizados e a sustentação de integrações tecnológicas complexas exigem estrutura e contatos que podem não refletir a capacidade operacional de intermediários de menor porte, serviços regionais e novos entrantes. Desse modo, as parcerias institucionais devem ser incentivadas como experiências cooperativas necessárias para garantir a segurança de alguns segmentos, mas não como régua regulatória comum para todo o ecossistema digital.

agenda de densificação regulatória do dever de cuidado e atuação diligente

Foram localizadas convergências também sobre a necessidade de maior densidade em conceitos relevantes no novo regime de responsabilidade de provedores de aplicação de internet, em especial em seus deveres de diligência. Compõem esta agenda os seguintes pontos:

1. Dever de cuidado. Os participantes sublinharam a importância da edição de elementos mais concretos e precisos sobre o cumprimento do dever de cuidado. Para tanto, aventou-se que sua interpretação se ancore na noção clássica do direito civil de boa-fé objetiva, mobilizando os deveres anexos de lealdade, transparência, cuidado e sigilo, com o intuito de favorecer a recepção do conceito pelas instâncias judiciais e desincentivar a derrubada preventiva de conteúdos que suscitem qualquer grau de incerteza.

A essa diretriz somou-se a necessidade de discussão sobre métricas de referência para aferição da diligência das plataformas. Foi percebida convergência na busca por substituir a expectativa de "erro zero" por um parâmetro compatível com a escala e a complexidade das operações digitais, permitindo distinguir a plataforma inerte daquela que, de boa-fé, busca aprimorar seus mecanismos de moderação.

2. Aspectos qualitativos na supervisão do dever de cuidado. Um ponto levantado foi que a supervisão sobre o dever de cuidado seja sensível a argumentos de natureza qualitativa, superando a lógica estritamente quantitativa baseada na relação entre o número de notificações recebidas e o volume de conteúdos removidos. Como defenderam diferentes participantes, a aferição de conformidade por métricas puramente numéricas gera incentivos inadequados à sobre-remoção preventiva, penalizando condutas prudentes de triagem e estimulando o bloqueio automático de ofertas e manifestações legítimas com o intuito de atingir altos índices de resposta. Nesse sentido, a prestação de contas pode também concentrar-se na divulgação detalhada das metodologias empregadas nas ferramentas de moderação, nas diretrizes de governança interna e nos fluxos procedimentais adotados para a análise de denúncias complexas.

Ao documentar a fundamentação utilizada em hipóteses de dúvida razoável e os critérios seguidos diante de notificações controversas ou instrumentalizadas de má-fé, os provedores também passam a prestar contas sobre o cumprimento de seus deveres e de seu impacto para a expressão dos usuários. Dessa forma, a avaliação do intermediário pelo órgão regulador e pelo Poder Judiciário passa a ter como parâmetro a consistência dos processos de tomada de decisão e a higidez das salvaguardas implementadas, afastando a caracterização de falha sistêmica como violação a uma obrigação de resultado.

3. Diferenciar questões de consumo e de conteúdo. No âmbito da discussão sobre o lugar do comércio eletrônico e consumo, identificou-se uma proposta de tipologia: distinguir entre, de um lado, danos estritamente de consumo, associados a problemas de logística, entrega ou publicidade paga, sobre os quais incidiria o regime aplicável do CDC, e, do outro lado, danos de conteúdo, associados à esfera do discurso, sobre os quais incidiria o Marco Civil da Internet, nos termos da decisão do STF. A divisão funcionaria, portanto, como um critério ordenador para tribunais, órgãos administrativos e diferentes setores da sociedade, um passo especialmente relevante diante da pluralidade de regimes de responsabilização firmada na decisão do STF.

agenda de detalhamento do regime de notificações extrajudiciais

O novo papel que o regime de notificações extrajudiciais possui a partir da edição da tese do STF sobre o tema 987 suscitou também a recomendação de uma agenda de regulação mais extensiva sobre o tema, passando pelos seguintes vetores.

1. Padrões de diligência razoável frente às notificações. Uma convergência entre participantes surgiu na importância de que sejam editadas padronizações sobre a diligência esperada dos provedores quando do recebimento de notificações. Foram relatadas situações em que remoções realizadas em prazos exíguos, da ordem de vinte e quatro a quarenta e oito horas, ou o atendimento de parcelas significativas de listas extensas de pedidos de remoção não tiveram qualquer efeito de diminuição de sanção, que foi mantida tal como se a plataforma em questão não houvesse tomado qualquer ação em relação aos pedidos. A título de exemplo, seria ilógico pensar que é indiferente se uma plataforma removeu 0 ou 90 conteúdos a partir de um pedido de remoção de 100 itens, de modo que importa ao sistema de incentivos refletir essa diferença e distinguir esforços de cumprimento.

Diante desse quadro, a recomendação articulada pelos participantes foi de que a boa-fé, a celeridade da resposta e o esforço técnico demonstrado pelas plataformas sejam reconhecidos como fatores relevantes na graduação das sanções administrativas. Além de conferir maior previsibilidade ao ambiente regulatório, isso contribuiria para estimular o investimento contínuo em arquiteturas robustas de moderação e para consolidar uma cultura de compliance efetivo, em benefício tanto das plataformas quanto dos órgãos de controle e dos próprios usuários, conferindo às sanções o parâmetro da proporcionalidade de forma explícita.

2. Mecanismos de proteção contra o uso abusivo de notificações. Os participantes da oficina convergiram na ideia de regulamentação detalhada do artigo

16-F do Decreto 12.975/2026, com a estruturação de filtros procedimentais voltados a coibir o uso instrumental de denúncias extrajudiciais. A prática de notificações em massa formuladas com intuito desleal por concorrentes ou por outros atores agindo de má-fé representa uma estratégia irregular que necessita de freios legais na construção do novo regime do Marco Civil da Internet. Para mitigar esse risco, sugere-se a fixação de critérios de admissibilidade para as comunicações de ilicitude, evitando que denúncias genéricas promovam a remoção sumária de conteúdo ou produtos. De forma associada, integrantes da oficina propuseram a previsão de consequências jurídicas e sanções para agentes econômicos que utilizam reiteradamente canais de denúncia para distorcer o propósito das notificações.

3. Sinalizadores confiáveis (*Trusted flaggers*). Outra proposta debatida durante a oficina foi a criação de um mecanismo estruturado de credenciamento de notificantes qualificados (comumente referidos na literatura internacional como *trusted flaggers*) também para o novo regime estabelecido para o MCI (lembrando que a figura já é abrangida no âmbito do ECA Digital). A proposta consiste em atribuir um *status* diferenciado a determinadas entidades com expertise e legitimidade, cujas notificações seriam processadas pelas plataformas com prioridade e por meio de canais dedicados, incluindo compromissos de tempo de resposta mais céleres.

A lógica subjacente é de que a identificação formal desses grupos serve a uma dupla função: (i) garantir um padrão básico de qualidade à denúncia, ao vincular sua origem a entidades com reconhecida capacidade técnica, e (ii) inibir comportamentos abusivos, ao associar o *status* diferenciado a padrões de responsabilidade mais exigentes. Nesse sentido, argumentou-se que, à maior capacidade de influência sobre o sistema de notificações, deve corresponder um compromisso proporcional com critérios técnicos objetivos que justifiquem e legitimem esse *status*.

Por fim, o debate incluiu ainda a ideia de criação de ferramentas institucionais que permitam às plataformas construir uma memória estruturada das notificações formuladas por esses atores qualificados. A ideia é que o histórico de notificações dos *trusted flaggers* sobre determinados temas ou categorias de conteúdo possa funcionar como parâmetro de análise quando o mesmo tema for levantado por notificantes comuns, conferindo maior segurança e certeza a todos os envolvidos.

4. Retomada da URL e preservação da análise contextual. Como contraponto à tendência crescente de identificação de conteúdos ilícitos por hashtags, palavras-chave e correspondências por hash, os participantes recomendaram a retomada da URL como instrumento privilegiado de individualização nas ordens de remoção. Concebida como padrão ouro nessa identificação, a URL preserva o vínculo direto entre referência e conteúdo, devolvendo à plataforma e ao usuário a possibilidade de delimitar com clareza o objeto da remoção, em contraposição a métodos que operam por aproximação e tendem a alargar indevidamente o escopo das ordens, com consequências particularmente sensíveis para o setor de comércio eletrônico, em que a individualização de um anúncio irregular em meio a milhares de similares é tarefa inviável sem essa referência precisa.

Conexa a essa retomada, foi sublinhada a necessidade de preservar a análise contextual no cumprimento das ordens de remoção, particularmente diante do critério de "conteúdo idêntico" introduzido pelo item 3.2 da tese do STF. A recomendação dos participantes é que a aferição da identidade entre conteúdos não se reduza à coincidência formal de elementos textuais ou visuais tomados isoladamente, mas considere o enquadramento, a finalidade e o contexto em que cada peça é veiculada.

Ressaltou-se, ainda, que a responsabilidade pela precisão na identificação do conteúdo ilícito seja compreendida como compartilhada entre os elos da cadeia de notificação, desde a formulação da requisição até o seu cumprimento, e não como ônus exclusivo da plataforma executora, especialmente diante de novos desafios trazidos pela IA generativa à identificação de conteúdo.

Este documento buscou retratar o estágio atual do debate e informar próximos passos em aspectos da governança digital brasileira que guardam forte conexão com os marcos jurídicos recentes, sob a perspectiva de múltiplos atores atentos aos efeitos dessa decisão. Eventuais desdobramentos relativos à operacionalização das novas regras, longe de encerrar as questões aqui levantadas, reafirmam sua pertinência, visto que o quadro normativo segue em construção, e os temas debatidos pelos participantes continuarão a demandar atenção, aprofundamento e diálogo entre os múltiplos atores envolvidos. Os temas debatidos na oficina e aqui expostos certamente não foram exauridos e caberá acompanhar e seguir debatendo seus desdobramentos com o tempo.