

A INCONSTITUCIONALIDADE DO ART. 19 DO MARCO CIVIL
DA INTERNET: breve análise do julgamento do STF

Demócrito Reinaldo Filho
Desembargador do TJPE

1. Introdução

O Supremo Tribunal Federal (STF) concluiu, na tarde da última quinta-feira (dia 26.06.25), o julgamento de dois recursos extraordinários¹ em que se discutia a constitucionalidade do art. 19 da Lei n. 12.965/14 (conhecida como o "Marco Civil da Internet"). Esse artigo de lei confere uma completa imunização aos provedores de serviços digitais e controladores de plataformas digitais, pois estabelece que não podem ser responsabilizados civilmente por danos decorrentes de conteúdos ilícitos publicados por terceiros (usuários das plataformas) e só devem suprimir conteúdo após receber ordem judicial². A única exceção a essa regra está no art. 21 do próprio MCI, segundo o qual o provedor de aplicações de internet pode ser responsabilizado por imagens e vídeos contendo cenas de nudez ou de atos sexuais gerados por

¹ A questão foi debatida no RE 1.037.396-SP, tema 987 da repercussão geral, e no RE 1.057.258-MG, tema 533 da repercussão geral, relatado pelo Min. Luiz Fux.

² O art. 19 do MCI tem a seguinte redação:

"Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário."

terceiros se, quando notificado, não promover a remoção do conteúdo³.

A Corte Suprema entendeu que o artigo 19 do MCI é “parcialmente inconstitucional”, pois “não confere proteção suficiente a bens jurídicos constitucionais de alta relevância”, como a proteção dos direitos fundamentais e dos valores democráticos. Os ministros se reuniram na Presidência do STF, na quinta-feira em que ocorreu a sessão do Plenário, para estabelecer os pontos consensuais do julgamento, a fim de redigir as teses jurídicas com *repercussão geral*⁴. Elaboraram ao todo 14 enunciados, alguns com mais de um subitem⁵. A leitura dos enunciados das teses revela que o STF criou um regime de responsabilidades diversificado, que varia conforme o tipo de serviço prestado pelo provedor e a natureza dos conteúdos disseminados. Todos os esquemas jurídicos de responsabilização construídos na tese com *repercussão geral* do STF são baseados na responsabilidade fundada na culpa,

³ O art. 21 do MCI tem a seguinte redação:

“Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.”

⁴ Essa reunião foi necessária, porque o julgamento foi por maioria de votos e mesmo entre os ministros que votaram pela inconstitucionalidade do art. 19 do MCI houve divergências quanto aos fundamentos dos votos. Dentro do grupo majoritário que votou pela inconstitucionalidade, alguns enxergaram apenas inconstitucionalidade parcial, enquanto outros entenderam pela inconstitucionalidade integral do dispositivo. Uma minoria votou pela constitucionalidade. Oito ministros declararam o artigo 19 parcial ou totalmente inconstitucional. Foram eles: Dias Toffoli, Luiz Fux, Luís Roberto Barroso, Flávio Dino, Cristiano Zanin, Gilmar Mendes, Alexandre de Moraes e Cármen Lúcia. Os ministros André Mendonça, Edson Fachin e Nunes Marques votaram pela validade do artigo 19 e não endossaram a nova tese.

⁵ Confira a íntegra das teses de *repercussão geral* no seguinte link: https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/06/26205223/MCI_tesesconsensusadas.pdf

não existindo esquema de imputação de responsabilidade objetiva aos provedores de serviços e aplicações na internet⁶. As regras que conformam o novo regime jurídico estabelecido para os provedores de serviços digitais passam a valer para o futuro, ou seja, têm eficácia a partir do julgamento, não retroagindo para alcançar fatos e situações já constituídas⁷. Adiante apresentamos um resumo explicativo das teses aprovadas.

2. Crimes de injúria, difamação e calúnia

Em relação a conteúdos que possam causar danos à honra, à reputação ou a direitos da personalidade dos indivíduos, continua a valer a norma do art. 19 do MCI. Os provedores só podem ser responsabilizados (dever de pagar indenização) se descumprirem uma ordem judicial para remoção de conteúdo⁸. A Corte entendeu que responsabilizar diretamente o provedor, nessas hipóteses, poderia de alguma forma embotar a “liberdade de expressão”.

Nesse ponto, o julgado da Corte Suprema causou certa frustração, pois danos relacionados com direitos da personalidade (direito ao nome, à imagem, à intimidade e à privacidade) constituem a maioria dos conflitos decorrentes de publicações em plataformas de redes sociais e outros serviços onde os conteúdos são disponibilizados instantaneamente pelos usuários. O ideal teria sido fixar o regime do “*notice and take down*” para esses casos, em que os conteúdos são removidos pelo

⁶ O enunciado 12 da tese de repercussão geral estabelece que “não haverá responsabilidade objetiva na aplicação da tese aqui enunciada”.

⁷ Conforme a redação do enunciado 14 da tese de repercussão geral: “14. Para preservar a segurança jurídica, ficam modulados os efeitos da presente decisão, que somente se aplicará prospectivamente, ressalvadas decisões transitadas em julgado.”

⁸ É o que está expresso no enunciado 3.1 da tese de repercussão geral, nestes termos:

“3.1. Nas hipóteses de crime contra a honra aplica-se o art. 19 do MCI, sem prejuízo da possibilidade de remoção por notificação extrajudicial.”

provedor após notificação extrajudicial dos interessados (vítimas dos danos). Se não excluir o conteúdo apontado como ilícito ou prejudicial, depois de notificado, o provedor pode ser responsabilizado solidariamente com a pessoa (usuário) que fez a publicação. Tal regime garante a liberdade editorial do provedor de analisar a natureza do conteúdo, decidindo manter (ou não) o material informacional.

Ainda que tenha mantido a imunidade do provedor em relação a conteúdos que causem danos à reputação e à imagem das pessoas, o STF destacou que os controladores de plataformas e serviços de redes sociais podem fazer a remoção de conteúdos, de maneira voluntária, após serem notificados extrajudicialmente. Os provedores não são responsabilizados por conteúdos gerados por terceiros (usuários) que causem danos à reputação e honra das pessoas, mas podem fazer a remoção de maneira voluntária, após notificados pelo ofendido. No que tange, portanto, a conteúdos relacionados com danos à reputação e honra (direitos à intimidade e privacidade) das pessoas, os provedores continuam completamente imunizados.

Também ficou definido que, quando um fato ofensivo já reconhecido por decisão judicial for repetidamente replicado, todos os provedores deverão remover as publicações com idêntico conteúdo, quando notificados (extrajudicialmente). O beneficiário da decisão judicial não necessita ingressar novamente em juízo para obter nova ordem de retirada do material ofensivo, toda vez que for republicado em outra plataforma ou serviço de hospedagem⁹.

⁹ É o que está expresso no enunciado 3.2 da tese de *repercussão geral*, nestes termos:

“3.2. Em se tratando de sucessivas replicações do fato ofensivo já reconhecido por decisão judicial, todos os provedores de redes sociais deverão remover as publicações com idênticos conteúdos,

3. Crimes em geral

O STF estabeleceu outro esquema de responsabilização para os provedores quando se tratar de conteúdo informacional que constitua qualquer outra forma de crime, ilícito tipificado nas leis penais. O texto da tese de repercussão geral estatui que “o provedor de aplicações de internet será responsabilizado civilmente, nos termos do art. 21 do MCI, pelos danos decorrentes de conteúdos gerados por terceiros em casos de crime ou atos ilícitos, sem prejuízo do dever de remoção do conteúdo” (Enunciado 3). Em se tratando de conteúdo informacional publicado por terceiros (usuários da plataforma digital) que constitua qualquer espécie de ilícito penal, o provedor será responsabilizado solidariamente com o difusor do conteúdo se não tomar providências para removê-lo em tempo hábil. Se o provedor se mantiver inerte, depois de notificado (extrajudicialmente) da existência de material informacional que se enquadre em algum tipo penal, em seu sistema informatizado, será responsabilizado juntamente com o ofensor original.

Aqui se trata de uma responsabilidade baseada no conhecimento do ilícito, ou seja, o provedor só pode ser responsabilizado se, devidamente cientificado da existência do material informacional ilícito, não adotar as providências para removê-lo de seu sistema informatizado. Trata-se do *knowledge regime*, baseado na culpa do provedor que se mantém na inércia mesmo tendo ciência da ilicitude que ocorra no ambiente digital sob seu controle.

É aceitável que o controlador de uma plataforma ou sistema informatizado não pode, em regra, ser

independentemente de novas decisões judiciais, a partir de notificação judicial ou extrajudicial.”

responsabilizado pelo material informacional publicado e divulgado ao público instantaneamente, à falta de controle editorial, já que, nesses casos, quem faz a publicação do material não é ele, mas o usuário do sistema. O usuário é quem fornece o conteúdo, sem participação direta do mantenedor do site ou plataforma digital. Mas o operador do sistema permanece com o poder de retirar ou alterar o conteúdo da notícia ou informação. Embora não tenha sido ele que fixou a mensagem para o público, permanece com controle sobre a informação, devendo ser responsabilizado se permanecer inerte após tomar conhecimento do material informacional ilícito hospedado em seu sistema.

O esquema de responsabilização traçado no art. 21 do MCI da Internet também deve ser aplicado nos casos de contas e perfis falsos. É o que resulta dos termos em que foi redigida a tese de repercussão geral: “Aplica-se a mesma regra [art. 21 do MCI] nos casos de contas denunciadas como inautênticas” (parte final do Enunciado 3). Contas e perfis falsos (“perfis fakes”) são contas criadas em plataformas e serviços digitais com informações falsas ou com o propósito de se passar por outra pessoa, para fins de entretenimento, golpes, disseminação de informações incorretas ou para fins maliciosos. Elas podem ser usadas para uma variedade de atividades ilegais, incluindo golpes, difamação, assédio e até mesmo para influenciar eleições e mercados financeiros.

É de se entender que, na hipótese de contas ou perfis falsos, o provedor se submete ao sistema do “notice and takedown” (previsto no art. 21 do MCI) mesmo quando o conteúdo publicado por terceiros for de natureza difamatória, injuriosa ou caluniosa. O provedor do serviço digital ou controlador da plataforma deve ser responsabilizado se, após notificação, não retirar de “forma diligente” o conteúdo de caráter difamatório ou

calunioso. Se o provedor, ao receber a notificação, exclui a publicação realizada pelo utente da conta falsa, desaparece sua responsabilidade em relação às consequências danosas que ela possa produzir.

O STF deveria ter estabelecido um regime jurídico de reponsabilidade civil mais gravoso para as hipóteses de contas e perfis falsos. Deveria ter imputado um esquema de responsabilidade solidária ou subsidiária para o provedor, para esses casos. É que quase sempre não se descobre a verdadeira identidade do usuário do sistema informatizado que criou a conta ou perfil *fake*. Assim, se não se responsabiliza o provedor, a vítima do dano fica sem possibilidade de reparação, o que não se compatibiliza com a teoria da responsabilidade civil, que se baseia na ideia do prejuízo para justificar a reparação ao lesado. Alguém sempre deve reparar o prejuízo causado a outrem. Repugna ao Direito a possibilidade de haver prejuízo sem a devida e correspondente compensação patrimonial (responsabilização). Não se podendo identificar o ofensor direto, aquele que torna a informação (conteúdo ilícito) pública, o controlador do sistema informatizado utilizado para a difusão da informação deveria responder pela reparação. Em suma, nos casos em que não se consegue alcançar o editor direto da informação, como nas hipóteses das contas e perfis *fakes*, em que a identidade do verdadeiro editor da informação permanece oculta, o provedor do serviço digital ou controlador da plataforma deveria ser responsabilizado.

4. Presunção de responsabilidade

Foi erigido por meio do enunciado 4 da tese de *repercussão geral* um regime de presunção de responsabilidade, para certas situações em que o provedor tem um controle maior (prévio) sobre o conteúdo ou faz o

impulsionamento do material informacional de forma automatizada, utilizando tecnologia específica para essa tarefa. Ficou estabelecido que, quando se tratar de anúncios e impulsionamentos pagos ou rede artificial de distribuição (por meio de *chatbots* ou robôs), o provedor responde pelo dano causado pelo conteúdo ilícito, ainda que não tenha sido notificado¹⁰.

A presunção de responsabilidade civil ocorre quando a lei estabelece que, em determinadas situações, a obrigação de indenizar (responsabilidade civil) é atribuída a alguém sem que seja necessária a comprovação de culpa. Nesses casos, a lei presume a existência de certos elementos da responsabilidade civil, como o dano e o nexó causal, ou até mesmo a culpa, invertendo o ônus da prova. Os ministros do STF entenderam de aplicar a presunção de responsabilidade em duas situações: anúncios e impulsionamentos pagos e rede artificial de distribuição (por meio de *chatbots* ou robôs). A culpa do provedor, pelos danos causados pelo conteúdo impulsionado ou distribuído dessas maneiras, é presumida. Nessas duas situações, o provedor tem que indenizar a vítima (o lesado pelo conteúdo prejudicial ou ilícito), mas pode comprovar que "atuou diligentemente e em tempo razoável para tornar indisponível o conteúdo", para se eximir de responsabilidade. Se o operador da plataforma demonstra que "tomou as providências eficazes e tempestivas para remoção do conteúdo quando devidamente alertado, evidenciando uma atuação diligente conforme os padrões

¹⁰O enunciado 4 da tese de repercussão geral tem a seguinte redação: "4. Fica estabelecida a presunção de responsabilidade dos provedores em caso de conteúdos ilícitos quando se tratar de (a) anúncios e impulsionamentos pagos; ou (b) rede artificial de distribuição (chatbot ou robôs). Nestas hipóteses, a responsabilização poderá se dar independentemente de notificação. Os provedores ficarão excluídos de responsabilidade se comprovarem que atuaram diligentemente e em tempo razoável para tornar indisponível o conteúdo."

razoáveis esperados”, essa reação constitui causa excludente da responsabilidade.

A lógica da imposição desse regime um pouco mais gravoso (presunção de responsabilidade) para as situações de anúncios pagos e distribuição de conteúdo por meio de algoritmo de impulsionamento está na circunstância do prévio conhecimento do conteúdo. Se o provedor contrata com alguém a divulgação de um anúncio publicitário ou escolhe impulsionar certos conteúdos, é porque conhece de antemão a natureza desses conteúdos. A concepção jurídica para excluir a responsabilidade do provedor dos prejuízos causados por mensagens ou postagens dos usuários é que em regra ele não tem conhecimento da natureza nociva dos conteúdos. Só posteriormente, quando comunicado pela vítima, fica ciente do material informacional difundido no interior de seu sistema informatizado. Nas hipóteses de anúncio pago ou material impulsionado, a percepção é que o provedor já tem contato prévio com o conteúdo, antes de divulgá-lo ou impulsioná-lo. Assim, não se justifica que continue com isenção de responsabilidade, pois tem conhecimento prévio do material informacional.

Ainda assim, o STF foi muito tímido ao estabelecer somente uma “presunção de responsabilidade” que pode ser excluída simplesmente se o provedor, após notificado, promove a remoção do conteúdo em prazo breve. Deveria ter construído um regime de responsabilidade solidária para as hipóteses de conteúdo patrocinado (pago) ou impulsionado pelo próprio sistema (algoritmo ou sistema de distribuição) do controlador. Se o provedor, ao contratar o anúncio pago (e receber dinheiro pela publicação) ou escolher impulsionar determinada postagem, tem conhecimento prévio do conteúdo, deveria ser responsabilizado como o próprio editor (difusor) da informação. Na mídia tradicional, os editores da informação

respondem diretamente pelas consequências que possam produzir. O diretor da publicação assume a responsabilidade pelo seu conteúdo, porque, em razão do trabalho que empreende, está em condições de controlar as informações. Como a decisão de publicar (ou não) uma informação pertence ao editor, tratando-se de verdadeira faculdade, decorre daí que exerce poder de controle sobre ela. Desse poder de controle decorre a responsabilidade pela publicação de informações danosas. A pressuposição é de que, se decide publicar alguma coisa, é porque tem conhecimento da natureza da informação publicada. Por essa razão, responde solidariamente com o fornecedor da informação.

O mesmo padrão de um editor da informação deveria ser estendido aos provedores de aplicações na Internet que recebem por anúncios publicados em seus sistemas ou quando decidem pelo impulsionamento de certos conteúdos (ainda que de maneira automatizada). Quando libera para publicação um anúncio pago ou impulsiona (privilegia) determinado conteúdo (ainda que não receba vantagem financeira pelo impulsionamento), o provedor tem poder de controle sobre a informação (anúncio pago ou conteúdo impulsionado). Portanto, em casos de anúncios pagos e conteúdos escolhidos para difusão impulsionada (privilegiada), deveria haver responsabilidade solidária entre a pessoa que paga o anúncio (anunciante) e a que permite a publicação (o provedor) e recebe dinheiro por isso. Da mesma forma, esse padrão de responsabilização deveria ser adotado em todos os casos em que o provedor, para fins de monetização ou não, impulsiona (e privilegia) determinados conteúdos dentro de seu sistema informatizado, utilizando tecnologias de distribuição informacional.

5. Crimes graves

O STF estabeleceu um "dever de cuidado" para os provedores em relação à circulação de conteúdos informacionais que constituam crimes graves (Enunciado 5). Na lista do que considerou "crimes graves", a Corte incluiu: (a) condutas e **atos antidemocráticos** que se amoldem aos tipos previstos nos artigos 296, parágrafo único, 359-L, 359-M, 359-N, 359-P e 359-R do Código Penal; (b) crimes de **terrorismo** ou preparatórios de terrorismo, tipificados pela Lei nº 13.260/2016; (c) crimes de **induzimento, instigação ou auxílio a suicídio ou a automutilação**, nos termos do art. 122 do Código Penal; (d) incitação à **discriminação em razão de raça, cor, etnia, religião, procedência nacional, sexualidade ou identidade de gênero** (condutas homofóbicas e transfóbicas), passível de enquadramento nos arts. 20, 20-A, 20-B e 20-C da Lei nº 7.716/1989; (e) **crimes praticados contra a mulher** em razão da condição do sexo feminino, inclusive conteúdos que propagam ódio ou aversão às mulheres (Lei nº 11.340/06; Lei nº 10.446/02; Lei nº 14.192/21; CP, art. 141, § 3º; art. 146- A; art. 147, § 1º; art. 147-A; e art. 147-B do CP); (f) **crimes sexuais contra pessoas vulneráveis, pornografia infantil e crimes graves contra crianças e adolescentes**, nos termos dos arts. 217-A, 218, 218-A, 218-B e 218-C do Código Penal e dos arts. 240, 241-A, 241- C, 241-D do Estatuto da Criança e do Adolescente; g) tráfico de pessoas (CP, art. 149-A).

Quanto a esse rol taxativo de conteúdos que configuram de **crimes graves**, o provedor tem uma obrigação geral de vigilância para evitar a "circulação massiva" desse tipo de material informacional em seus sistemas informatizados. Nesse ponto, o STF parece ter atribuído para os provedores, em relação a conteúdos com ilicitude acentuada ou visível (crimes graves) o regime da "due diligence" (diligência devida), que exige que realizem

monitoração de seus sistemas e adotem providências quando necessário. Prevê a remoção proativa pelos provedores de conteúdos nitidamente ilegais, para evitar que aconteça “falha sistêmica”¹¹. Esta ocorre quando deixam “de adotar adequadas medidas de prevenção ou remoção dos conteúdos ilícitos” graves, “configurando violação ao dever de atuar de forma responsável, transparente e cautelosa”¹².

A responsabilidade do provedor, quanto ao dever de vigilância proativa em relação aos **crimes graves** listados, somente se caracteriza na hipótese de “falha sistêmica”, não podendo sofrer sanções diante da “existência de conteúdo ilícito de forma isolada, atomizada”, situação que “não é, por si só, suficiente para ensejar a aplicação da responsabilidade civil” por quebra do “dever de cuidado” na monitoração de crimes graves¹³. A falha do “dever de cuidado” só se caracteriza diante de “circulação massiva” de conteúdos definidos como crimes graves, não ensejando a responsabilidade do provedor quando o aparecimento desses crimes ocorre em dimensão mínima, em uma ou outra oportunidade. Todavia, ocorrendo caso isolado de circulação de conteúdo informacional que configure **crime grave**, uma vez o provedor notificado da existência desse material, deve removê-lo sob pena de responder

¹¹ Conforme Enunciado 5.1:

“5.1 A responsabilidade dos provedores de aplicações de internet prevista neste item diz respeito à configuração de falha sistêmica.”

¹² Conforme Enunciado 5.2:

“5.2 Considera-se falha sistêmica, imputável ao provedor de aplicações de internet, deixar de adotar adequadas medidas de prevenção ou remoção dos conteúdos ilícitos anteriormente listados, configurando violação ao dever de atuar de forma responsável, transparente e cautelosa.”

¹³ Conforme Enunciado 5.4, de seguinte redação:

“5.4. A existência de conteúdo ilícito de forma isolada, atomizada, não é, por si só, suficiente para ensejar a aplicação da responsabilidade civil do presente item. Contudo, nesta hipótese, incidirá o regime de responsabilidade previsto no art. 21 do MCI.”

solidariamente com o editor direto da informação (usuário do sistema ou plataforma)¹⁴.

Tudo indica que o STF tenha se inspirado, nesse ponto, no *Digital Services Act* (DSA), a legislação europeia que regula a responsabilidade dos provedores de conteúdo e serviços na Internet. Foi esse o primeiro texto legislativo que, a fim de garantir que os serviços digitais não sejam utilizados de forma abusiva para atividades ilícitas e que os prestadores operam de forma responsável, criou obrigações de "devida diligência" (*due diligence*) para os provedores. Foi o DSA europeu que, ao aumentar as obrigações dos controladores de grandes plataformas, criou para eles obrigações de devida vigilância em relação a conteúdos nitidamente ilícitos, atribuindo-lhes a gestão dos riscos de funcionamento, para evitar o "risco sistêmico"¹⁵.

Provavelmente, essa nova obrigação de monitoração de conteúdos que configurem **crimes graves**, tal qual instituída agora pelo STF, não terá efetividade imediata no Brasil. A Corte não indicou os órgãos que ficariam encarregados da fiscalização da gestão do "risco sistêmico" das grandes plataformas e provedores de serviços digitais. Para reforçar a garantia de aplicação do regulamento e observância das obrigações (de devida diligência) pelos provedores, o DSA europeu criou os coordenadores dos serviços digitais (*digital services*

¹⁴ É o que está estabelecido no Enunciado no 5.4 da tese de *repercussão geral*: "A existência de conteúdo ilícito de forma isolada, atomizada, não é, por si só, suficiente para ensejar a aplicação da responsabilidade civil do presente item. Contudo, nesta hipótese, incidirá o regime de responsabilidade previsto no art. 21 do MCI."

¹⁵ Para saber mais sobre o *Digital Services Act* (DSA), sugerimos a leitura do nosso artigo "O *Digital Services Act* (1ª. parte) - A proposta legislativa europeia mantém a imunidade legal dos provedores de serviços na internet", publicado no site *Jus*, em 05.03.22, acessível em: <https://jus.com.br/artigos/96199/o-digital-services-act-1-parte-a-proposta-legislativa-europeia-mantem-a-imunidade-legal-dos-provedores-de-servicos-na-internet>

coordinators), que são as principais autoridades nacionais designadas pelos Estados-Membros da UE para reforçar a aplicação do regulamento (artigo 38.º), bem como instituiu o *Comitê Europeu dos Serviços Digitais*, um grupo consultivo independente de coordenadores dos serviços digitais (art. 47.º). Os coordenadores dos serviços digitais auxiliam a *Comissão Europeia* (braço executivo da UE) a fiscalizar e fazer cumprir as normas da *Lei de Serviços Digitais* (DSA). A gestão dos riscos de funcionamento das grandes plataformas é supervisionada por órgãos do Estado, que atuam na fiscalização da gestão do risco sistêmico. Autoridades e agentes estatais ficam encarregados da inspeção e auditoria de sistemas de moderação de conteúdos, sistemas de recomendação e publicidade das grandes plataformas, de forma a evitar a ocorrência de falhas sistêmicas.

Sem a criação no Brasil, à semelhança do que ocorreu na União Europeia, de uma estrutura de órgãos encarregados de fiscalizar a gestão do “risco sistêmico” das grandes plataformas, é pouco provável que a instituição do dever de vigilância de conteúdos que configurem as práticas de **crimes graves** tenha alguma efetividade. A simples criação de obrigações de “devida vigilância” para os provedores de serviços digitais, sem a instituição de um arcabouço de órgãos estatais de supervisão, para garantir a observância desses novos deveres, pode resultar desprovida de aplicabilidade concreta.

Outro ponto que precisa ser alertado é que a tese de *repercussão geral* do STF não diferencia os serviços e plataformas digitais de acordo com o tamanho. Parece que a obrigação de monitoração e vigilância de conteúdos que configurem **crimes graves** foi estabelecida indistintamente para todos os prestadores de serviços digitais e controladores de plataformas digitais, independentemente do porte ou natureza. A atribuição dessa

obrigação de maneira indistinta pode dificultar o desenvolvimento de pequenas e médias empresas que prestem serviços na internet. O DSA europeu só estabelece esse tipo de obrigação, de maneira a evitar o chamado “risco sistêmico”, para as plataformas digitais de grande dimensão (*very large online platforms*)¹⁶.

Outro ponto desnecessário está presente no enunciado 5.5 da tese de repercussão geral. Esse item prevê que quando o provedor realiza por sua própria iniciativa - já que tem a obrigação de vigilância em relação a crimes graves - a remoção de conteúdo que lhe pareça nitidamente ilegal, nasce para a pessoa que fez a publicação (usuário da plataforma) o direito de requerer judicialmente o restabelecimento do material informacional removido, desde que demonstre ausência de ilicitude¹⁷.

Atribuir direito aos usuários das plataformas digitais (redes sociais) de contestar e eventualmente ter a informação republicada eliminada ou ao menos diminuir sensivelmente o poder editorial dos provedores e, conseqüentemente, a responsabilidade pelas conseqüências do conteúdo postado. Com efeito, os usuários passam a ter o direito de recorrer à Justiça para recolocar conteúdo removido, mas não para responsabilizar o provedor pela decisão tomada durante o processo de moderação de conteúdo. Tanto é assim que a parte final (do enunciado 5.5) da tese de repercussão geral estabelece que “ainda que o conteúdo seja restaurado por ordem judicial, não haverá imposição de indenização ao provedor”. O usuário passa a

¹⁶ O DSA classifica como *very large online platforms* (ou VLOPs) aquelas que têm mais de 45 milhões de usuários por mês na União Europeia.

¹⁷ Conforme estabelece o enunciado 5.5 da tese de repercussão geral:

“5.5. Nas hipóteses previstas neste item, o responsável pela publicação do conteúdo removido pelo provedor de aplicações de internet poderá requerer judicialmente o seu restabelecimento, mediante demonstração da ausência de ilicitude. Ainda que o conteúdo seja restaurado por ordem judicial, não haverá imposição de indenização ao provedor.”

ter o direito de contestar a decisão tomada pelo provedor na atividade de moderação de conteúdo e recorrer a órgãos judiciais para impugnar a decisão. Ao invés de flexibilizar a imunidade legal dos provedores dos serviços de hospedagem de conteúdo, a tese com repercussão geral terminou reforçando essa imunidade, ao "estatizar" a atividade de moderação de conteúdos.

É errada a visão de que a atividade de moderação de conteúdos desenvolvida pelos provedores pode limitar ou cercear a liberdade de expressão (*freedom of expression*) dos usuários. Não existe esse potencial conflito, pela simples razão de que os usuários (editores direto da informação) não têm direito de publicar o que quiserem, já que as plataformas são sistemas informatizados privados, e a relação entre eles e o controlador (proprietário) é regulada pelas normas de um contrato (termos de uso) privado.

Redes sociais, sistemas de edição de conteúdo instantâneo, não são espaços públicos, à semelhança de uma rua ou praça pública, onde qualquer um pode ter acesso e se expressar livremente, sem qualquer tipo de limitação quanto ao conteúdo de suas manifestações. São sistemas informatizados privados, gerenciados por empresas privadas, que coletam, analisam e monetizam os dados das pessoas e outras informações que circulam no interior de seus domínios digitais. O Poder Público não tem nada que interferir na atividade de moderação de conteúdos desempenhada pelos controladores de plataformas de serviços on-line, que hospedam conteúdo editado por terceiros (usuários do sistema).

É verdade que algumas dessas estruturas de comunicação digital adquiriram domínio dos mercados onde atuam, mas isso não as transforma em "espaços públicos". O problema do monopólio que grandes empresas de tecnologia

exercem sobre determinados setores de serviços na rede mundial de comunicação pode ser combatido de outras formas¹⁸.

6. Provedores de serviços de e-mail, mensageria e videoconferência

No enunciado 6 da tese de *repercussão geral*, o STF resolver atribuir a imunidade prevista no art. 19 do MCI a provedores de serviços e aplicativos específicos: a) de transmissão de arquivos e mensagens ("eletronic-mail"); b) aplicativo de mensagens instantâneas (serviços de mensageria); e c) aplicativos que permitem a realização de reuniões fechadas por vídeos ou voz¹⁹.

Os aplicativos e serviços de *email* permitem o envio, recebimento e gerenciamento de mensagens eletrônicas. São ferramentas essenciais para a comunicação, tanto pessoal quanto profissional, oferecendo funcionalidades como organização de mensagens, anexos, listas de contatos e, em alguns casos, calendários e outras ferramentas de colaboração (por exemplo, o *Gmail*, o *Outlook* e o *Yahoo!*). Os sistemas e aplicativos de mensageria atuam como intermediários que facilitam a transferência instantânea de mensagens de texto entre dois ou mais usuários, facilitando comunicação imediata e fluida. Além do envio de texto, muitos sistemas oferecem recursos como

¹⁸ Com a atualização das leis que regulam a competição na economia, para criar mecanismos legais que equilibrem a competição no âmbito das redes digitais, por exemplo. Esse inclusive é o objeto de outro texto aprovado pela UE, o *Digital Markets Act (DMA)*.

¹⁹ A redação do enunciado 6 da tese de *repercussão geral* é a seguinte: "6. Aplica-se o art. 19 do MCI ao (a) provedor de serviços de e-mail; (b) provedor de aplicações cuja finalidade primordial seja a realização de reuniões fechadas por vídeo ou voz; (c) provedor de serviços de mensageria instantânea (também chamadas de provedores de serviços de mensageria privada), exclusivamente no que diz respeito às comunicações interpessoais, resguardadas pelo sigilo das comunicações (art. 5º, inciso XII, da CF/88)."

compartilhamento de arquivos, chamadas de áudio e vídeo e integração com outras plataformas (por exemplo, o *WhatsApp* e o *Telegram*). Serviços e aplicativos para videoconferência são aqueles que permitem a realização de reuniões fechadas por vídeo ou voz. A maioria das ferramentas disponibilizadas no mercado oferece também recursos de gravação e transcrição de reuniões e permitem que os participantes compartilhem suas telas para apresentar documentos, slides ou outras informações (por exemplo, o *Zoom*, o *Google Meet* e o *Microsoft Teams*).

Desde muito, a doutrina e jurisprudência estrangeira já isentavam de responsabilidade os intermediários da comunicação eletrônica que se limitam a prestar serviços de transmissão de mensagens. Reconhece-se que o provedor desses serviços atua como um mero conduto para o tráfego da informação, em situação equivalente à da companhia telefônica. Na transmissão de mensagens eletrônicas o provedor comercial não exercita controle editorial e, portanto, não pode ser responsabilizado como se editor fosse de potenciais mensagens difamatórias ou conteúdos ilícitos. O provedor assume uma posição de passividade nessas situações, não podendo ser compelido a vistoriar o conteúdo de mensagens em cuja transmissão não tem participação nem possibilidade alguma de controle. O sistema eletrônico de comunicação serve apenas de conduto para o transporte da informação de uma caixa postal (eletrônica) para outra, funcionando como mero transportador das informações.

Os transportadores de informações, a exemplo das empresas telefônicas, jamais foram responsabilizados pelo conteúdo proveniente de terceiros que circula em suas linhas. Idealmente falando, é a pessoa do remetente que transmite a mensagem e é ela a responsável pelo conteúdo. As linhas de transmissão da empresa servem

apenas de conduto para essa operação. Sem possibilidade de controle do conteúdo das mensagens circulantes em seu sistema, a responsabilidade do provedor somente pode surgir a partir do momento em que tome conhecimento do caráter danoso da informação (se não adota nenhuma iniciativa para fazer cessar a propagação do ilícito).

O STF entendeu de consagrar esse tipo de concepção jurídica no enunciado 6 da tese de *repercussão geral*, não só para os provedores de serviços de e-mail, mas também para os serviços e aplicativos de mensageria e videoconferência. É razoável estender o mesmo tratamento dado aos provedores de serviços de gerenciamento de e-mails aos prestadores de serviços de mensageria e videoconferência, por se encontrarem estes em posição análoga àqueles primeiros. Os provedores de serviços de mensageria e videoconferência, a exemplo do serviço de gerenciamento de e-mails, podem ser entendidos como meros transportadores da informação, sendo seus sistemas utilizados como simples conduto para a comunicação eletrônica entre os usuários. Não têm, em princípio, controle efetivo sobre o conteúdo das mensagens, vídeos e imagens que circulam em seus sistemas.

A única falha na tese jurídica erigida pelo STF, nesse ponto, foi conferir aos provedores desses serviços uma imunização completa, ao estabelecer para eles o regime do ainda sobrevivente art. 19 do MCI. Embora se conceba que os provedores desses serviços de comunicação eletrônica (serviços de e-mail, mensageria e videoconferência) não têm, em princípio, controle da informação que os usuários transmitem em seus sistemas, a responsabilidade dessa categoria de prestadores de serviços digitais pode surgir a partir do momento em que, alertados pelo interessado, tomam conhecimento do caráter

danoso de uma tal informação e não adotam nenhuma iniciativa para fazer cessar a propagação do ilícito.

7. Marketplaces

Marketplace é uma plataforma on-line que reúne diversos vendedores (lojas ou indivíduos) em um único local, permitindo que os compradores encontrem e comparem produtos de diferentes fornecedores. É como um *shopping center* virtual, onde cada loja é um vendedor diferente. Não atuam na transmissão, arquivamento ou hospedagem da informação (conteúdos), mas como locais ou subespaços on-line para o comércio eletrônico de produtos (em sua maioria físicos).

Por isso, o STF estabeleceu um regime jurídico diferenciado para essa categoria de prestadores de serviços on-line. Como participam da cadeia de fornecimento de produtos, para eles ficou estabelecido que se submetem às normas do CDC²⁰. Em regra, *marketplaces* não atuam como transportadores ou hospedeiros da informação, não são desenhados precipuamente para servir como ferramenta para envio de mensagens ou publicação de comentários pelos usuários. Mas fica a ressalva de que, se o controlador de *marketplace* fornece, em algum subespaço da plataforma, serviço para publicação de conteúdo informacional diretamente pelos usuários, aí nessa situação o esquema jurídico de responsabilidade civil aplicável será um daqueles outros que foram elaborados na tese de repercussão geral, a depender do conteúdo publicado.

8. Obrigações adicionais

²⁰ A redação do enunciado 7 da tese de repercussão geral é a seguinte: "7. Os provedores de aplicações de internet que funcionarem como marketplaces respondem civilmente de acordo com o Código de Defesa do Consumidor (Lei nº 8.078/90)."

Nos enunciados 8 a 11 são criadas obrigações adicionais para os controladores de plataformas e prestadores de serviços digitais. O STF traçou um conjunto de “obrigações gerais” que se aplicam a todo prestador de serviço na internet, notadamente no que se refere a deveres de “transparência” e mecanismos de “supervisão” da atividade dos provedores de serviços on-line. As obrigações não foram repartidas entre os diversos prestadores de serviços on-line, mas estabelecidas como obrigações gerais para qualquer provedor, independentemente do tamanho e da natureza dos serviços que preste. Como a complexidade da arquitetura da rede mundial de comunicação hoje permite o aparecimento de serviços digitais variados, seria de esperar que o STF estabelecesse obrigações específicas para certos conjuntos de prestadores de serviços on-line, mas, da leitura dos enunciados, fica claro não haver distinção em relação a qualquer espécie de provedor ou controlador de sistema informatizado (plataforma); as obrigações adicionais se aplicam a todos, indistintamente.

O sistema de “responsabilidade limitada” dos provedores de serviços on-line foi complementado com obrigações relacionadas essencialmente à atividade de moderação de conteúdo e funcionamento dos algoritmos de direcionamento da informação e publicidade. Como obrigações gerais adicionais, estão previstas para todos os prestadores de serviços digitais:

a) o dever de editarem normas de auto-regulação que disciplinem sistemas de notificações, devido processo e obrigação de apresentar relatórios de transparência relativos a notificações extrajudiciais, anúncios e impulsionamentos²¹;

²¹ É o que está previsto no enunciado 8 da tese de repercussão geral:

b) a obrigação de disponibilizar a usuários e a não usuários canais específicos de atendimento, preferencialmente eletrônicos, acessíveis e amplamente divulgados nas plataformas de maneira permanente²²;

c) a obrigação de constituir e manter sede e representante no país, cuja identificação e informações para contato deverão ser disponibilizadas e estar facilmente acessíveis nos respectivos sítios. O representante do provedor que atue no Brasil deve ser necessariamente pessoa jurídica, com poderes para: (i) responder perante as esferas administrativa e judicial; (ii) prestar às autoridades competentes informações relativas ao funcionamento do provedor, às regras e aos procedimentos utilizados para moderação de conteúdo e para gestão das reclamações pelos sistemas internos; aos relatórios de transparência, monitoramento e gestão dos riscos sistêmicos; às regras para o perfilamento de usuários (quando for o caso), à veiculação de publicidade e ao impulsionamento remunerado de conteúdos; (iii) cumprir as determinações judiciais; (iv) responder e cumprir sanções, multas e afetações financeiras em que o representado incorrer, especialmente por descumprimento de obrigações legais e judiciais²³.

"8. Os provedores de aplicações de internet deverão editar autorregulação que abranja, necessariamente, sistema de notificações, devido processo e relatórios anuais de transparência em relação a notificações extrajudiciais, anúncios e impulsionamentos."

²² É o que está previsto no enunciado 9 da tese de repercussão geral:

"9. Deverão, igualmente, disponibilizar a usuários e a não usuários canais específicos de atendimento, preferencialmente eletrônicos, que sejam acessíveis e amplamente divulgados nas respectivas plataformas de maneira permanente."

²³ O enunciado 11 da tese de repercussão geral tem a seguinte redação:

"11. Os provedores de aplicações de internet com atuação no Brasil devem constituir e manter sede e representante no país, cuja identificação e informações para contato deverão ser disponibilizadas e estar facilmente acessíveis nos respectivos sítios. Essa representação deve conferir ao representante, necessariamente pessoa jurídica com sede no país, plenos poderes para (a) responder perante as esferas administrativa e judicial; (b) prestar às autoridades competentes informações relativas ao funcionamento do provedor, às regras e aos procedimentos utilizados para moderação de conteúdo e para gestão das reclamações pelos sistemas internos; aos relatórios de transparência, monitoramento e gestão dos riscos sistêmicos; às regras

10. Conclusão:

Para os prestadores de serviços na internet, por serem intermediários da comunicação eletrônica, se convencionou estabelecer um sistema de "responsabilidade limitada" em razão da concepção de que o provedor não tem "obrigação geral de vigilância" sobre as informações que os usuários do sistema transmitem ou armazenam, nem uma "obrigação geral de procurar ativamente fatos ou circunstâncias que indiquem ilicitudes". Simplesmente atua provendo a infra-estrutura técnica para transmissão ou hospedagem da informação, atividade que não acarreta uma coobrigação de controle de conteúdo, de zoneamento visando à exclusão de informação ou material ilícito. Prevaleceu um princípio geral de irresponsabilidade do provedor por material ilícito, depositado pelos usuários ou que de qualquer forma transita em seu sistema informático.

Essa concepção se formou e se consolidou há quase três décadas, quando a internet tinha arquitetura completamente diferente. Naquela época (na primeira metade dos anos 1990), quando o canal gráfico da internet (a *web*) começou a se popularizar e começaram a aparecer os serviços (aplicações) que permitiam a transmissão de mensagens e postagens pelos próprios usuários, havia uma preocupação de não sobrecarregar os provedores de serviços no nascente "cyberspace". Apregoava-se que uma responsabilização mais pesada poderia causar um "chilling effect" nas embrionárias tecnologias da informação, em prejuízo da inovação. As empresas que iniciavam seus negócios por meios eletrônicos

para o perfilamento de usuários (quando for o caso), a veiculação de publicidade e o impulsionamento remunerado de conteúdos; (c) cumprir as determinações judiciais; e (d) responder e cumprir eventuais penalizações, multas e afetações financeiras em que o representado incorrer, especialmente por descumprimento de obrigações legais e judiciais."

eram ainda poucas e pequenas. O ciberespaço era um ambiente para amadores, onde os sites mais visitados eram gerenciados por adolescentes. Havia ainda um forte discurso libertário, defendendo o "ciberespaço" como um mundo paralelo, onde os estados-nação não teriam como impor suas leis, que deveria ser um ambiente completamente livre da "tirania dos governos".

Com o crescimento do "comércio eletrônico", essa realidade mudou completamente. O capitalismo floresceu nesses novos espaços, com as corporações empresariais se estabelecendo e impondo seus interesses. Mas o crescimento se deu de forma assimétrica, surgindo as grandes empresas de tecnologia, que dominam vastos nacos do ciberespaço e do comércio eletrônico. O discurso dos libertários e crentes em um mundo sem regras, sem as "amarras do poder estatal", onde as pessoas poderiam desfrutar de um ambiente de completa liberdade, para se expressarem da maneira que quisessem, terminou favorecendo o surgimento dos monopólios digitais. Esse ambiente sem regras mais rígidas (para a responsabilização dos provedores) e o discurso libertário também contribuiu para o aumento da criminalidade na rede mundial de comunicação. Essa também foi a causa do surgimento do problema da desinformação (*fake news*), a disseminação de conteúdos e informações falsas em plataformas e aplicações na internet, ameaçando a regularidade de eleições e o próprio regime democrático.

Com essa nova configuração da rede e o domínio da economia digital por poucas e grandes corporações (as chamadas *Big Techs*), nos últimos anos se intensificou a discussão sobre a necessidade de impor maiores obrigações para os provedores de aplicações na internet, com a revisão e atualização do quadro regulatório. A maioria dos países havia adotado o "knowledge regime", que estabelece a responsabilização do

provedor apenas quando tenha conhecimento do conteúdo prejudicial ou ilícito e não tome providências. Aos poucos se formou um entendimento pela necessidade de adotar obrigações adicionais, imputando dever de vigilância quando se tratar de conteúdos visivelmente ilícitos e altamente nocivos para os direitos fundamentais das pessoas e para os valores e princípios democráticos. Nos EUA se acendeu o debate sobre a necessidade de flexibilizar a imunidade conferida aos provedores pela *Section 230* da Lei de Decência nas Comunicações (*Communications Decency Act*)²⁴. Na União Europeia se iniciaram as discussões para a reforma da Diretiva sobre comércio eletrônico (Diretiva 31/2000/CE)²⁵, que terminou sendo substituída pelo DSA (*Digital Services Act*).

No Brasil, trilhamos caminho inverso. A jurisprudência do STJ já tinha assentado a obrigação do provedor de, uma vez notificado, realizar a remoção do conteúdo prejudicial ou ilícito em 24 horas, sob pena de responsabilização solidária com o responsável pela publicação. Já tínhamos construído, pela via jurisprudencial, um modelo do “regime do conhecimento” (*knowledge regime*) para responsabilizar os provedores de aplicações na Internet. Mas em abril de 2014 foi aprovada a Lei 12.965, que ficou conhecida como o “Marco Civil da Internet”.

Embora o Marco Civil da Internet (MCI) tenha trazido alguns avanços, criando regras para proteção de

²⁴ A *Section 230* do *Communications Decency Act*, lei aprovada em 1996 pelo Congresso dos EUA, criou uma espécie de porto seguro (*safe harbor*) para os provedores de serviços na internet, isentando-os de responsabilidade por conteúdo produzido pelos usuários de suas plataformas. Uma vez comunicados do teor da publicação, os provedores devem remover o conteúdo danoso, sob pena de responsabilização.

²⁵ A Diretiva (UE) 2000/31/CE, conhecida como Diretiva do Comércio Eletrônico, também previa como princípio geral a não responsabilização do provedor por conteúdo produzido pelos usuários, mas com a ressalva de que, tomando conhecimento do conteúdo danoso ou ilícito, deveria removê-lo. Foi substituída pela Lei dos Serviços Digitais (DSA).

dados pessoais e erigindo princípios em defesa da privacidade, o seu art. 19 conferiu uma completa imunização aos provedores, isentando-os de qualquer responsabilidade por conteúdos danosos e ilícitos que transitam em seus sistemas. Livrou os prestadores de serviços na internet de qualquer obrigação de moderação de conteúdos e definiu que ficavam só obrigados a cumprir ordem judicial. Eliminou qualquer dever de moderação para os provedores, pois cumprir ordem judicial já é obrigação de qualquer pessoa, física ou jurídica. Com isso, se criou uma imunização completa para os provedores, que ficaram sem responsabilidade editorial (ainda que postergada) e desobrigados de adotar qualquer iniciativa de combate a conteúdos ilícitos.

O STF perdeu a oportunidade de aniquilar o art. 19 do MCI, que continua a ser adotado para certas situações. Foi louvável o esforço e dedicação dos ministros, conduzidos pelo Presidente da Corte, na tentativa de fornecer, por via da tese de *repercussão geral*, um quadro regulatório provisório, enquanto o Congresso Nacional não elabora leis mais abrangentes sobre o assunto. Mas deixar sobreviver, ainda que parcialmente, o dispositivo questionado não atende às necessidades dos tempos atuais. O STF deveria pelo menos ter estabelecido como pedra de toque fundamental, para o balizamento de responsabilidades dos provedores, o regime do conhecimento (*knowledge regime*) para todas as hipóteses de difusão de conteúdos danosos, com o acréscimo de obrigações de vigilância para conteúdos visivelmente ilícitos (crimes graves). Isso pelo menos colocaria o regime jurídico brasileiro em pé de igualdade com o *DSA* europeu. As grandes empresas de tecnologia já utilizam ferramentas de inteligência artificial para análise de conteúdos e não

seria irrazoável atribuir-lhes um dever de vigilância mais rígido.

A Corte Suprema também poderia ter depurado as obrigações conforme o tamanho e natureza do provedor, impondo mais rigor nos deveres das grandes plataformas digitais, em reconhecimento à assimetria do poder das grandes corporações em relação às pequenas e médias empresas que prestam serviços na internet. O STF terminou conferindo a mesma carga de obrigações às grandes empresas de tecnologia e aos pequenos provedores. Esse ponto poderá ser aperfeiçoado na futura legislação que vier a tratar do tema.

Recife, 29 de junho de 2025.