

Novas regras do Marco Civil da Internet entram em vigor e ampliam deveres de plataformas digitais

03.09.2026 11 minutos de leitura

Profissionais relacionados

Felipe Palhares

Fernanda Villela

Áreas relacionadas

Proteção de Dados e
Cybersecurity

Assuntos

Informativos Proteção de Dados e
Cybersecurity

Em resumo

Os Decretos nº 12.975/2026 e nº 12.976/2026, em vigor desde 20 de julho de 2026, regulamentam o Marco Civil da Internet e substituem a lógica reativa de responsabilização por um modelo de prevenção, monitoramento e gestão de riscos sistêmicos. O Decreto nº 12.975/2026 impõe deveres como a guarda da porta lógica de origem, representante legal no Brasil, dever de cuidado, procedimentos de notificação e remoção, regras de publicidade digital e transparência. O Decreto nº 12.976/2026 cria um regime específico de proteção às mulheres no ambiente digital, com prazos reduzidos de remoção e restrições ao uso de inteligência artificial em conteúdo íntimo. A ANPD passa a ter competências regulatórias e fiscalizatórias sobre o novo regime.

Em 21 de maio de 2026, foram publicados, no Diário Oficial da União os Decretos nº 12.975/2026 e nº 12.976/2026 (em conjunto definidos como “Decretos MCI”), que regulamentam aspectos centrais do Marco Civil da Internet (Lei nº 12.965/2014) e consolidam parte relevante das diretrizes estabelecidas pelo Supremo Tribunal Federal (STF) nos Temas 987 e 533 de repercussão geral, a respeito da responsabilização de provedores de aplicações de internet por conteúdos publicados por terceiros.

Os Decretos MCI, que entraram em vigor no dia 20 de julho de 2026, representam uma mudança significativa na governança das plataformas digitais, ao substituir uma lógica predominantemente reativa de responsabilização por um modelo baseado em deveres de prevenção, monitoramento e gestão de riscos sistêmicos.

Contexto: o que mudou após a decisão do STF

O antigo regime previsto no art. 19 do Marco Civil da Internet estabelecia que os provedores de aplicações somente poderiam ser responsabilizados civilmente por conteúdos gerados por terceiros caso descumprissem ordem judicial específica de remoção.

No julgamento dos Temas 987 e 533, o STF declarou a inconstitucionalidade parcial por omissão do art. 19 do MCI, adotando a interpretação de que o modelo não oferecia proteção suficiente a direitos fundamentais e à democracia em situações envolvendo conteúdos ilícitos. A Corte passou a exigir atuação mais diligente das plataformas digitais em situações

envolvendo conteúdos criminosos ou ilícitos, estabelecendo um regime de responsabilização progressivo e de natureza subjetiva.

Para mais detalhes sobre o tema, acesse o nosso informativo “Constitucionalidade do Artigo 19 do Marco Civil da Internet”.

Os Decretos MCI foram editados para regulamentar esse novo cenário regulatório.

Principais obrigações introduzidas pelo Decreto nº 12.975/2026

Dever de guarda da porta lógica de origem

Como ponto de partida, o Decreto nº 12.975/2026 determina a manutenção da porta lógica de origem por parte de provedores de aplicação e de conexão, além do dever de guarda dos registros de conexão e de acesso. Essa obrigação encerra de maneira definitiva discussão frequente na esfera judicial, uma vez que provedores argumentavam que a guarda da porta lógica não era mandatária.

Com o Decreto nº 12.975/2026, o dever de guarda da porta lógica de origem passa a não depender de requisição prévia, incidindo automaticamente sobre cada provedor.

Obrigatoriedade de representante legal no Brasil

O Decreto nº 12.975/2026 introduz um conjunto abrangente de obrigações aplicáveis aos provedores de aplicações de internet, incluindo a exigência de manutenção de sede e de representante legal no Brasil. O representante legal constituído deve ter poderes para responder perante autoridades administrativas e judiciais, prestar informações relativas ao funcionamento da plataforma, cumprir determinações judiciais e responder por eventuais sanções impostas ao provedor.

Dever de cuidado e gestão de riscos sistêmicos

O conceito de “dever de cuidado” foi expressamente incorporado no texto do Decreto nº 12.975/2026. Provedores de aplicações de internet são responsabilizados quando houver falha sistêmica na adoção de medidas adequadas para indisponibilizar imediatamente o rol taxativo de conteúdos referido em seu art. 16-B. Esses conteúdos são relacionados, entre outros, a casos de terrorismo, induzimento, instigação ou auxílio ao suicídio ou à automutilação, racismo, homofobia, misoginia, crimes sexuais contra pessoas vulneráveis, exploração sexual e crimes graves contra crianças e adolescentes, tráfico de pessoas e atos antidemocráticos.

O teor da norma esclarece, contudo, que a mera existência desses conteúdos, de maneira isolada, não é suficiente para caracterizar falha sistêmica. A avaliação da ocorrência de falha sistêmica considerará a efetividade dos mecanismos de prevenção ou remoção utilizados pela plataforma.

Ademais, sem prejuízo do rol taxativo de crimes que demandam dever de cuidado, provedores de aplicações de internet têm a responsabilidade de

monitorar, identificar, avaliar e gerenciar riscos sistêmicos decorrentes ou potencializados por suas atividades.

Notificação e indisponibilização de conteúdo criminoso

Outra mudança relevante diz respeito aos procedimentos de notificação de conteúdos ilícitos ou criminosos. Os provedores de aplicações passam a ser obrigados a manter canais de denúncia permanentes e acessíveis para o recebimento e tratamento de notificações. A notificação deverá identificar o conteúdo ou eventual conduta criminosa ou ilícita, bem como a respectiva decisão judicial, nos termos do art. 16-J, o notificante e o fundamento que a legitima, se cabível.

A partir da notificação, o respectivo recebimento deverá ser confirmado, o conteúdo reportado deverá ser analisado e as decisões adotadas deverão ser comunicadas, de forma fundamentada, ao notificante e, exceto no caso de não remoção do conteúdo objeto de notificação, também ao usuário responsável pela publicação.

O novo modelo procura compatibilizar maior agilidade no enfrentamento de condutas ilícitas ou criminosas com garantias mínimas referentes ao devido processo e à liberdade de expressão, exigindo justificativas para decisões de remoção ou manutenção de conteúdos e assegurando mecanismos de contestação.

Embora o regime atual amplie as hipóteses em que conteúdos criminosos poderão ser removidos mediante notificação, o modelo tradicional do art. 19 do MCI permanece aplicável aos crimes e atos ilícitos contra a honra.

O conteúdo gerado por terceiros que configure crime, conforme a legislação nacional, deverá ser indisponibilizado em resposta às notificações recebidas. Nos casos de crime contra a honra, continua necessária ordem judicial específica para fins de remoção e responsabilização do provedor de aplicações.

A responsabilidade administrativa do provedor de aplicações, quando alegada a não remoção de conteúdo criminoso, deverá considerar a atuação diligente, proporcional e célere em relação à notificação recebida. Assim, a apuração de responsabilidade não poderá ser embasada exclusivamente na manutenção ou retirada do conteúdo objeto da notificação.

Publicidade digital e impulsionamento de conteúdo

O Decreto nº 12.975/2026 também introduz um regime específico para anúncios e conteúdos impulsionados. Os provedores de aplicações que disponibilizam ferramentas de anúncio ou impulsionamento pagas deverão implementar mecanismos para impedir a contratação de conteúdos criminosos ou ilícitos e manter registros dos anúncios e respectivos anunciantes pelo prazo mínimo de um ano, contado da data de encerramento da veiculação.

Além disso, a responsabilidade é objetiva em situações envolvendo conteúdos ilícitos veiculados em anúncios, impulsionamentos pagos ou por mecanismos artificiais de distribuição. É admitido, contudo, o afastamento da responsabilidade quando comprovadas a atuação diligente e a remoção do conteúdo em tempo razoável.

Transparência e autorregulação

Adicionalmente às novas obrigações relacionadas à moderação de conteúdo, os provedores de aplicações deverão editar termos e condições de uso, bem como outras formas de autorregulação, como políticas internas e procedimentos, para refletir as exigências do novo regime regulatório. O Decreto nº 12.975/2026 determina que sejam fornecidas informações, ao menos, sobre o sistema de notificações e o devido processo.

As plataformas também deverão ampliar seus mecanismos de transparência, mediante a elaboração e divulgação periódica de relatórios contendo informações sobre notificações extrajudiciais recebidas, medidas de moderação implementadas, anúncios veiculados e conteúdos impulsionados em seus serviços.

Esses documentos deverão ser publicados, divulgados ao público e revisados periodicamente.

Regime específico de proteção às mulheres no ambiente digital

Prazos diferenciados para a remoção de conteúdo

O Decreto nº 12.976/2026, por sua vez, institui um conjunto de medidas voltadas à prevenção e ao combate à violência online contra mulheres. A norma estabelece obrigações específicas para provedores de aplicações em casos envolvendo violência contra mulheres em ambiente digital, incluindo divulgação não autorizada de conteúdo íntimo, perseguição digital, ameaças, violência psicológica, entre outros crimes e condutas ilícitas praticadas em razão da condição do sexo feminino por meio da internet.

Entre as principais novidades está a previsão de prazos reduzidos para tratamento dessas ocorrências. Conteúdos íntimos divulgados sem consentimento deverão ser removidos em até duas horas após a notificação da vítima ou do seu representante. A indisponibilização do conteúdo íntimo deve ser integral, devendo o seu reenvio ser automaticamente bloqueado.

Já conteúdos manifestamente ilegais contra mulheres deverão ser removidos em até seis horas, e em até vinte e quatro horas aqueles relacionados à violência em ambiente digital. Também foi estabelecido o dever de comunicar o notificante acerca da justificativa de não remoção e dos meios para a contestação da decisão. Recebida a contestação da decisão, o provedor de aplicações tem o prazo de vinte e quatro horas para restaurar ou retirar o conteúdo, e informar a decisão ao notificante e ao responsável pela publicação.

Utilização de inteligência artificial em conteúdo íntimo

O Decreto nº 12.976/2026 ainda dedica especial atenção aos riscos decorrentes do uso de inteligência artificial (IA) ou de qualquer outro recurso equivalente, proibindo a geração e a modificação de conteúdo íntimo de terceiros com uso dessas tecnologias.

Ademais, os provedores de aplicações que disponham de funcionalidades baseadas em IA ou outras tecnologias capazes de alterar imagem ou som da

vítima deverão implementar salvaguardas técnicas e procedimentais destinadas a identificar e bloquear solicitações que possam resultar na criação desse tipo de material.

Ampliação do papel da Agência Nacional de Proteção de Dados

Uma das alterações mais relevantes é a atribuição de competências regulatórias e fiscalizatórias à Agência Nacional de Proteção de Dados (ANPD), que passa a ter um papel central relacionado ao cumprimento dos deveres impostos aos provedores de aplicações pelos Decretos MCI.

Nesse sentido, espera-se que a ANPD edite regulamentações complementares para disciplinar, por exemplo, aspectos operacionais relacionados à gestão de riscos, procedimentos de notificação, mecanismos de transparência e critérios de avaliação da atuação diligente dos provedores de aplicações.

Próximos passos

A entrada em vigor dos Decretos nº 12.975/2026 e nº 12.976/2026 inaugura uma nova fase da regulação de plataformas digitais no Brasil. Em conjunto com a decisão do STF sobre o art. 19 do Marco Civil da Internet, as normas impõem novos deveres de governança e ampliam significativamente as expectativas regulatórias relacionadas, por exemplo, à moderação de conteúdo, publicidade digital, gestão de riscos e proteção de usuários.

Isso significa que a expansão das obrigações introduzidas pelos Decretos MCI, somada à atuação da ANPD, tende a elevar significativamente o nível de maturidade regulatória esperado dos provedores de aplicações de internet.

Nesse contexto, é recomendável que empresas sujeitas ao Marco Civil da Internet revisem seus modelos de governança e seus processos internos para assegurar aderência ao novo regime e, consequentemente, reduzir a exposição a riscos materiais e reputacionais.

Pontos principais

Quando os Decretos MCI entraram em vigor?

Os Decretos MCI, que entraram em vigor no dia 20 de julho de 2026, representam uma mudança significativa na governança das plataformas digitais, ao substituir uma lógica predominantemente reativa de responsabilização por um modelo baseado em deveres de prevenção, monitoramento e gestão de riscos sistêmicos.

O provedor de aplicações precisa manter representante legal no Brasil?

O Decreto nº 12.975/2026 introduz um conjunto abrangente de obrigações aplicáveis aos provedores de aplicações de internet, incluindo a exigência de manutenção de sede e de representante legal no Brasil. O representante

legal constituído deve ter poderes para responder perante autoridades administrativas e judiciais, prestar informações relativas ao funcionamento da plataforma, cumprir determinações judiciais e responder por eventuais sanções impostas ao provedor.

Em quanto tempo conteúdo íntimo divulgado sem consentimento deve ser removido?

Entre as principais novidades está a previsão de prazos reduzidos para tratamento dessas ocorrências. Conteúdos íntimos divulgados sem consentimento deverão ser removidos em até duas horas após a notificação da vítima ou do seu representante. A indisponibilização do conteúdo íntimo deve ser integral, devendo o seu reenvio ser automaticamente bloqueado.

Já conteúdos manifestamente ilegais contra mulheres deverão ser removidos em até seis horas, e em até vinte e quatro horas aqueles relacionados à violência em ambiente digital. Também foi estabelecido o dever de comunicar o notificante acerca da justificativa de não remoção e dos meios para a contestação da decisão. Recebida a contestação da decisão, o provedor de aplicações tem o prazo de vinte e quatro horas para restaurar ou retirar o conteúdo, e informar a decisão ao notificante e ao responsável pela publicação.

O regime do art. 19 continua valendo para crimes contra a honra?

Embora o regime atual amplie as hipóteses em que conteúdos criminosos poderão ser removidos mediante notificação, o modelo tradicional do art. 19 do MCI permanece aplicável aos crimes e atos ilícitos contra a honra.

O conteúdo gerado por terceiros que configure crime, conforme a legislação nacional, deverá ser indisponibilizado em resposta às notificações recebidas. Nos casos de crime contra a honra, continua necessária ordem judicial específica para fins de remoção e responsabilização do provedor de aplicações.

O que os Decretos MCI preveem sobre uso de inteligência artificial em conteúdo íntimo?

O Decreto nº 12.976/2026 ainda dedica especial atenção aos riscos decorrentes do uso de inteligência artificial (IA) ou de qualquer outro recurso equivalente, proibindo a geração e a modificação de conteúdo íntimo de terceiros com uso dessas tecnologias.

Ademais, os provedores de aplicações que disponham de funcionalidades baseadas em IA ou outras tecnologias capazes de alterar imagem ou som da vítima deverão implementar salvaguardas técnicas e procedimentais destinadas a identificar e bloquear solicitações que possam resultar na criação desse tipo de material.

Qual é o papel da ANPD no novo regime?

Uma das alterações mais relevantes é a atribuição de competências regulatórias e fiscalizatórias à Agência Nacional de Proteção de Dados (ANPD), que passa a ter um papel central relacionado ao cumprimento dos deveres impostos aos provedores de aplicações pelos Decretos MCI.

Nesse sentido, espera-se que a ANPD edite regulamentações complementares para disciplinar, por exemplo, aspectos operacionais relacionados à gestão de riscos, procedimentos de notificação, mecanismos de transparência e critérios de avaliação da atuação diligente dos provedores de aplicações.

Profissionais que aliam visão jurídica e visão de mercado



Felipe Palhares



Fernanda Villela