



# LEGISLAÇÃO, ÉTICA E CONFORMIDADE

AULA 4



Prof. Jailson de Souza Araújo



## CONVERSA INICIAL

### Boas práticas nos negócios digitais e marco civil da internet

Nesta etapa, abordaremos temas relacionados às boas práticas e autorregulamentação de fornecedores de produtos e serviços digitais, bem como analisar temáticas relativas ao Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014), lei que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Analisaremos os fundamentos constitucionais do Marco Civil da Internet, os direitos e garantias dos usuários de internet e os deveres e responsabilidades dos provedores de conexão e de aplicação de internet, abordando o princípio da neutralidade de rede, a proteção da privacidade e dos dados pessoais e a guarda de registros de acesso a aplicações de internet na provisão de conexão e na provisão de aplicações.

Finalmente, serão apresentadas as possibilidades de provedores de aplicações de internet serem responsabilizados civilmente em virtude de danos decorrentes de suas atividades.

### TEMA 1 – BOAS PRÁTICAS COMERCIAIS, AUTORREGULAMENTAÇÃO E CONFORMIDADE NOS NEGÓCIOS DIGITAIS

Para Claudia Lima Marques (2009), a terceira revolução industrial, representada pela informatização e globalização da economia (também chamado de fenômeno da mundialização ou aproximação dos mercados e sociedades de consumo), trouxe uma crise de confiança que aumentou ainda mais a vulnerabilidade do consumidor.

Desde então, a produção despersonalizou-se totalmente e desterritorializou-se, tornando-se mundial. As marcas, o marketing e os mercados não conhecem mais fronteiras; o mundo virtual modificou hábitos de consumo, mudou o tempo deste, agilizou as informações e expandiu as possibilidades de publicidade, agravando os conflitos de consumo e a própria vulnerabilidade informacional, técnica, fática e jurídica do consumidor.

Diante dessa constatação, torna-se necessário que o fornecedor de produtos e serviços digitais ampare o consumidor em situações em que, a partir da exploração de vulnerabilidade, seus direitos possam ser violados ou estejam



ameaçados, colocando à sua disposição instrumentos e recursos tecnológicos para coibir e combater comportamentos abusivos no ambiente virtual sob sua gestão e responsabilidade técnica e jurídica.

De acordo com Efig (2004), sob a perspectiva do binômio segurança/adequação, todos os produtos e serviços colocados no mercado de consumo brasileiro devem ser seguros, adequados e corresponder às legítimas expectativas dos consumidores.

Nesse sentido, o consumo de produtos e serviços relacionados à tecnologia da informação e comunicação (TIC) devem ser adequados, notadamente sob a perspectiva da segurança e do respeito aos direitos fundamentais, garantindo ao consumidor que este não fique exposto a práticas inseguras ou nocivas, cabendo ao Estado, inclusive, restringir sua comercialização, quando este colocar em risco a vida, a saúde, a segurança e a dignidade do consumidor.

A adoção de boas práticas éticas e de conformidade empresarial nos negócios realizados pelas corporações fornecedoras de bens e serviços de consumo relacionados à TIC poderá se tornar uma atitude de sobrevivência em um mercado altamente competitivo e disputado, eis que a demanda por serviços digitais está crescendo substancialmente, inclusive em decorrência da migração de serviços tradicionais para plataformas digitais.

É importante destacar que um programa de conformidade empresarial demanda mais do que apenas o cumprimento da legislação aplicável ao setor. Requer a adoção de políticas e diretrizes que prezem pelo respeito ao cliente, por meio da adoção de um código de ética e de conduta corporativa que se materialize na transparência e na boa-fé na atuação da empresa em todas as etapas contratuais (pré-contratual, contratual e pós-contratual, conforme vimos em conteúdo anterior), prevenindo problemas e irregularidades, evitando a intervenção punitiva do Estado nas suas operações empresariais, e, por consequência, prestigiando e protegendo a confiança do consumidor.

Vivemos na era digital, e entre as suas consequências, constatamos inúmeras transformações econômicas e sociais na forma de se produzir, contratar e consumir, inclusive no ambiente virtual.

Tal fato demanda soluções estratégicas para evitar que o usuário de serviços e produtos digitais seja exposto a práticas abusivas, situação que poderá gerar consequências e repercussões negativas, inclusive no âmbito



judicial, por meio de aplicação de multas e de processos indenizatórios em face da empresa responsável pela plataforma digital.

Consequência ainda mais grave é a quebra da confiança do consumidor, algo absolutamente imprescindível em um ambiente repleto de empresas que buscam se estabelecer em um mercado altamente competitivo, com diversas *startups* recebendo investimentos para oferecer ao mercado produtos e serviços digitais inovadores e atrativos.

Nesse sentido, basta observar quantas empresas tiveram um relevante posicionamento no mercado e desapareceram por não terem conseguido manter a oferta de um produto ou de um serviço relevante aos seus clientes e consumidores, ou por ter perdido a confiança destes, sendo superados por concorrentes mais eficientes.

Em se tratando de empresas que ofertam produtos e serviços digitais, notadamente *startups*, a manutenção da confiança do mercado financeiro se torna ainda mais importante para assegurar novos investimentos, a partir da demonstração da sua capacidade de produzir valor e gerar lucro, e da sua base de clientes, por ofertar produtos relevantes, confiáveis e melhores que o da concorrência.

Portanto, há vários fatores que podem justificar a necessidade da adoção das práticas de conformidade empresarial, ou “*compliance*”, na oferta de produtos e serviços digitais.

Entre eles, podemos destacar a necessidade dos fornecedores em não perder participação de mercado para concorrentes melhor preparados ao atendimento das demandas de um consumidor cada vez mais exigente e consciente de seus direitos, evitar resultados econômicos negativos, e evitar a diminuição do valor de suas ações ou prejuízo ao valor de sua marca, por conta de eventual divulgação em redes sociais e em canais de reclamações relacionadas a práticas que configurem mau atendimento, permissividade ou tolerância a comportamentos abusivos no espaço virtual sob sua gestão e responsabilidade, contrariando as normas protetivas aos usuários, dispostas no Código Civil, no Código de Defesa do Consumidor, no Marco Civil da internet e na Lei Geral de Proteção de Dados Pessoais.

Para tanto, compete às empresas a adoção de ferramentas que permitam ao consumidor reclamar, de maneira simples, rápida e acessível sobre problemas decorrentes dos serviços prestados ou dos produtos fornecidos, bem



como na utilização inadequada de suas plataformas, quando estas forem utilizadas de maneira abusiva e contrária ao Direito.

Diante da reclamação do usuário, estar preparado para atender adequadamente as demandas apresentadas, resolvendo-as em um prazo razoável, preferencialmente abaixo do 30 dias estabelecidos no art. 18, parágrafo 1º, pelo Código de Defesa do Consumidor (Brasil, 1990), agindo com transparência em todas as etapas e encaminhamentos durante o atendimento e, acima de tudo, não transferindo responsabilidades, notadamente quando a solução do problema envolver parceiros comerciais, prestadores de serviços ou agentes externos.

Justifica-se tal orientação na medida em que a obrigação contratual se dá entre o consumidor e o fornecedor, e não entre o consumidor e os parceiros comerciais do fornecedor.

Além disso, o fornecedor é responsável pela atuação de seus parceiros comerciais, sendo solidário na solução de qualquer problema relacionado à atuação destes, nos termos do Código de Defesa do Consumidor.

Portanto, ainda que eventual tarefa possa ser delegada a terceiros, como o serviço de atendimento ao cliente (SAC), ou serviço de entregas, a responsabilidade por qualquer falha, problema ou prejuízo sempre será do fornecedor, podendo este, após resolver o problema do consumidor, buscar a devida reparação ou compensação com o seu prestador de serviço ou parceiro comercial.

Nesse sentido, é de fundamental importância a criação de canais de atendimento dedicados à apresentação de problemas, e para o oferecimento de denúncias, ouvidorias, para questões que envolvam a prestação do serviço ou a oferta do produto do fornecedor.

Considerando que o produto ou serviço digital ofertado pode envolver comportamentos e atitudes ilícitos ou inapropriados de terceiros no ambiente virtual sob a responsabilidade do fornecedor, torna-se fundamental que este ofereça ao consumidor opções para solicitar checagem de fatos (*fact-checking*), notadamente em ambientes coletivos, como redes sociais, jogos multiplayer online e demais serviços que envolvam ambiente colaborativo e interativo, ambientes tradicionalmente não supervisionados ou pouco moderados.

Justifica-se tal iniciativa na medida em que a realização de irregularidades e ilicitudes cometida nesses espaços, inclusive crimes contra a honra, como a



calúnia, a injúria e a difamação, previstos nos arts. 138 a 140 do Código Penal (Decreto-Lei n. 2.848, de 7 de dezembro de 1940), demandam supervisão e regramentos, para assegurar ao consumidor um ambiente seguro, livre de práticas abusivas e evitar crimes virtuais, conforme lhe assegura a legislação que o protege, inclusive, no ambiente virtual.

Desse modo, compete ao profissional de TI disponibilizar essas ferramentas no ambiente virtual sob sua responsabilidade, certificando-se de que estas funcionem adequadamente e que as denúncias apresentadas sejam rápida e rigorosamente apuradas e respondidas, analisando-as a partir dos critérios, regras e princípios estabelecidos na legislação vigente.

Diante da constatação de irregularidades, abusos, má-fé ou mesmo condutas ilícitas, a empresa responsável pelo ambiente virtual deverá adotar de imediato as providências necessárias para interromper essas práticas, minimizando os danos sofridos pelo usuário.

Além disso, é dever da empresa coibir e prevenir comportamentos abusivos no ambiente virtual, estabelecendo no termo de uso um código de conduta que desestimule tais práticas e que puna com rigor usuários que ajam descumprindo-o, agindo de maneira a causar danos materiais ou morais em outros usuários, notadamente crimes contra a honra (calúnia, injúria ou difamação), ou com práticas que promovam qualquer forma de discriminação, aptas a ferir a dignidade da comunidade que utiliza o ambiente virtual sob sua responsabilidade.

Consequentemente, a autorregulamentação, prevenção e aplicação de punições a quem descumpre o termo de uso do produto ou do serviço digital, por meio de supervisão, canais internos de moderação de conteúdo, serviço de atendimento ao consumidor (SAC) e ouvidoria, podem ser uma forma bastante eficiente para manter o ambiente virtual saudável, respeitando direitos e garantias fundamentais, previstos na Constituição, como a liberdade de expressão, a não discriminação e a proteção da dignidade da pessoa humana, estabelecendo um padrão de conduta ético e em conformidade com a legislação brasileira que regulamenta, inclusive, ambientes virtuais.

Dessa forma, a empresa fornecedora de produtos e serviços digitais reduzirá os riscos de vir a ser responsabilizada judicialmente em virtude de negligência, inclusive decorrente de omissão, diante do evento danoso realizado no ambiente sob sua responsabilidade, ou ao menos poderá atenuar as



consequências jurídicas decorrentes das medidas indenizatórias, ressarcitórias ou compensatórias, que lhe serão impostas, nos termos do Código Civil, do Código de Defesa do Consumidor (CDC), do Marco Civil da Internet (MCI), da Lei Geral de Proteção de Dados Pessoais (LGPD), e da legislação penal que tipificam crimes virtuais, temas que serão abordados em conteúdos posteriores.

## **TEMA 2 – FUNDAMENTOS CONSTITUCIONAIS DO MARCO CIVIL DA INTERNET**

Dada a importância socioeconômica da internet, a atuação do Estado, estabelecendo regras e diretrizes para seu uso, tornou-se necessária, na medida em que a internet é uma ferramenta apta a promover tanto o desenvolvimento quanto a violação de Direitos.

De acordo com Celso Antônio Pacheco Fiorillo (2015), o uso da internet no Brasil precisa ser interpretado a partir dos princípios, garantias, direitos e deveres fixados pela Constituição Federal Brasileira, notadamente a partir dos princípios fundamentais da Constituição, descritos nos arts. 1º ao 4º, que estabelecem como fundamentos da República Federativa do Brasil valores como a cidadania, a dignidade da pessoa humana, o trabalho e a livre iniciativa, com o objetivo de construir uma sociedade justa, livre e solidária, garantindo o desenvolvimento nacional e promovendo o bem de todos, sem preconceitos ou qualquer forma de discriminação.

Os valores constitucionais exemplificativamente mencionados necessariamente vinculam todas as normas e “marcos” normativos existentes no Brasil, inclusive o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014), legislação que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Portanto, o Marco Civil da Internet deve ser interpretado a partir dos princípios e valores estruturantes da Constituição Federal mencionados, tanto para definir os deveres dos provedores de acesso e dos provedores de aplicação quanto para assegurar os direitos dos usuários de internet.

De acordo com Damásio de Jesus (2014), uma das funções do Marco Civil da Internet é criar segurança jurídica, oferecendo base legal para o Poder judiciário julgar causas envolvendo internet e tecnologia da informação e Comunicação, evitando que sejam proferidas decisões judiciais contraditórias



sobre temas idênticos, algo recorrente antes da vigência do Marco Civil da Internet.

Adotando como premissa os princípios constitucionais mencionados, o Marco Civil da Internet adota como fundamento os seguintes valores, de acordo com seu art. 2º:

- A liberdade de expressão
- O reconhecimento da escala mundial da rede;
- Os direitos humanos
- O desenvolvimento da personalidade e o exercício da cidadania em meios digitais
- A pluralidade e a diversidade
- A abertura e a colaboração
- A livre iniciativa, a livre concorrência e a defesa do consumidor
- A finalidade social da rede

Destaca-se a importância dada a liberdade de expressão, no referido artigo, eis que a remoção de conteúdos na internet não será feita de maneira arbitrária, a partir da solicitação sem justificativas plausíveis e devidamente comprovadas relacionadas ao dano injusto supostamente causado ao reclamante.

Além disso, defende-se que a internet não tenha “dono”, pertencendo à humanidade como um todo, para a promoção dos direitos humanos, o exercício da cidadania e a não discriminação no ambiente digital.

Pretende-se que a internet seja livre, aberta e colaborativa, incentivando a inovação, a criação de novos modelos de negócios, oferta de serviços e o compartilhamento de informações, que possam favorecer a sociedade.

A disciplina do uso da internet no Brasil tem os seguintes princípios, de acordo com o art. 3º:

- I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
- II - proteção da privacidade;
- III - proteção dos dados pessoais, na forma da lei;
- IV - preservação e garantia da neutralidade de rede;
- V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
- VII - preservação da natureza participativa da rede;
- VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Mais uma vez, percebe-se a importância da proteção da liberdade de expressão, bem como a proteção dada à privacidade e à proteção dos dados





peçoais, uma vez que os serviços de internet demandam dados pessoais, e o manejo de deles possuem potencial de violar a privacidade do usuário, podendo gerar responsabilidade jurídica aos agentes, conforme será visto em conteúdo posterior, ocasião em que estudaremos a Lei Geral de Proteção de Dados Pessoais (LGPD).

Por sua vez, o art. 4º estabelece que o uso da internet no Brasil tem por objetivo a promoção:

- I - do direito de acesso à internet a todos;
- II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
- III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
- IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

O Marco Civil da Internet busca a promoção da inclusão digital, proporcionando a todos acesso à informação, ao conhecimento, à participação na vida cultural e política.

Bons exemplos podem ser observados a partir das iniciativas voltadas à transparência na administração pública, com a participação popular em audiências públicas e no acesso a portais de transparência disponíveis na internet, em que dados relativos a gastos públicos são divulgados para o devido acompanhamento e fiscalização por parte do cidadão.

Nesse sentido, Jailson Araújo (2021) defende que a divulgação de informações sobre a aplicação dos recursos públicos e a publicação de informações de interesse público viabilizam a adequada fiscalização pela sociedade dos gastos públicos, promovendo a transparência na administração pública. Entretanto, é fundamental que essas informações possam ser facilmente consultadas via internet, tal como propõe o Portal da Transparência, do Governo Federal, um portal<sup>1</sup> que disponibiliza informações sobre a aplicação de recursos públicos federais.

Da mesma forma, considerando a necessidade do desenvolvimento de novas habilidades e competências que tornem o cidadão apto aos desafios da sociedade digital, torna-se de grande importância a promoção da inovação e a difusão de novas tecnologias, inclusive para facilitar o acesso da rede, preferencialmente utilizando tecnologia que utilize padrões abertos que facilitem

---

<sup>1</sup> Disponível em: <<https://www.portaltransparencia.gov.br/>>. Acesso em: 13 set. 2022.



e reduzam o custo para promover a comunicação entre aplicações e base de dados.

O art. 6º estabelece como critérios para a adequada interpretação da Lei, conforme os valores a seguir descritos:

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

Para Fiorillo (2015), todas as leis devem ser interpretadas preliminarmente em face dos princípios fundamentais, direitos e garantias dispostos na Constituição Federal.

Tal regra, evidentemente, aplica-se ao Marco Civil da Internet, cuja interpretação observará preliminarmente os princípios constitucionais mencionados ao longo deste tópico, e somente levará em conta aspectos inerentes à natureza da internet que estejam de acordo com tais princípios.

### **TEMA 3 – DIREITOS E GARANTIAS DOS USUÁRIOS DE INTERNET**

O Marco Civil da Internet, por definição legal, considera que o acesso à internet é essencial ao exercício da cidadania, o que envolve direitos relacionados à inviolabilidade da intimidade e da privacidade, sua respectiva proteção jurídica e a inviolabilidade e sigilo das comunicações via internet, salvo por ordem judicial, conforme prevê o art. 7º, que assegura ao usuário os seguintes direitos e garantias:

- I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
- II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
- III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
- IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
- V - manutenção da qualidade contratada da conexão à internet;
- VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
- VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
- VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:



- a) justifiquem sua coleta;
  - b) não sejam vedadas pela legislação; e
  - c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
- IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
- X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (Redação dada pela Lei nº 13.709, de 2018)
- XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
- XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
- XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Interessante mencionar que, dada a importância do acesso à internet para o exercício da cidadania, a Lei prevê que o acesso do cidadão à internet não deve ser suspenso, salvo por débito com o provedor de conexão<sup>2</sup>, a qualidade da conexão, que deve ser estável e sem problemas, e o contrato de prestação de serviço de detalhar de maneira objetiva, completa e transparente, como seus registros de conexão e dados pessoais serão protegidos, bem como as práticas de gerenciamento da rede que possam afetar sua qualidade, inclusive a disponibilização regular da velocidade de conexão contratada.

O direito de exclusão se torna evidente, quando o Marco Civil da Internet estabelece ao fornecedor de aplicações o dever de excluir definitivamente os dados pessoais recebidos do usuário, após o término da relação contratual, ressalvadas as guardas de dados exigidos por lei, conforme será visto com mais detalhes em conteúdo posterior, sobre a Lei Geral de Proteção de Dados Pessoais.

Conforme determina o art. 8º, são nulas as cláusulas contratuais que violem, além dos direitos descritos, que:

- I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
- II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

---

<sup>2</sup> Ressalte-se a importância do acesso facilitado e gratuito à internet em bibliotecas e órgãos públicos, que permitam ao cidadão o acesso a informações relevantes sob o ponto de vista educacional e social.



Portanto, a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

## **TEMA 4 – DEVERES E RESPONSABILIDADES DOS PROVEDORES DE CONEXÃO E DE APLICAÇÃO DE INTERNET**

### **4.1 Da neutralidade de rede**

O Marco Civil da Internet estabelece em seu art. 9º que as empresas de telecomunicações responsáveis pela transmissão e roteamento de dados devem tratar de maneira isonômica qualquer pacote de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

Tal determinação estabelece o conceito de neutralidade de rede, procedimento que evita que determinadas empresas ou serviços sejam favorecidos ou recebam prioridade indevida, entregando-lhes, por exemplo, velocidade de conexão mais elevada ou tráfego de dados priorizado, em detrimento de concorrentes, por exemplo.

Para Victor Hugo Pereira Gonçalves (2017), as empresas de telecomunicação devem se abster de impedir e obstaculizar o acesso e a manutenção de concorrentes em suas redes, a fim de gerar competição de mercado benéfica aos consumidores.

Segundo Gonçalves, a neutralidade visa estabelecer condições igualitárias entre os concorrentes ao utilizarem estruturas de telecomunicações a fim de que se implementem a concorrência e a defesa do consumidor.

Somente se justificará tratamento prioritário para serviços de emergência. Sendo necessário discriminar ou degradar o tráfego nas hipóteses previstas em lei, tal providência será realizada sem causar dano aos usuários, que deverão ser informados de modo transparente sobre as práticas de gerenciamento de tráfego adotadas.

Finalmente, impõe-se ao provedor de conexão de internet a proibição de bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, interferindo ou examinando os hábitos de utilização de internet dos usuários, preservando-se o sigilo das comunicações e a privacidade.



## **4.2 Da proteção aos registros, aos dados pessoais e às comunicações privadas**

O art. 10 do Marco Civil da Internet estabelece que os dados pessoais e as comunicações privadas devem ser protegidos, preservando a intimidade, a vida privada, a honra e a imagem das partes direta ou indiretamente envolvidas.

O provedor responsável pela guarda de registros de conexão e de acesso a aplicações de internet somente serão obrigados a disponibilizar tais registros mediante ordem judicial.

Mesmo que o provedor de conexão e aplicação de internet não esteja sediado no Brasil, havendo coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações no Brasil, basta que ocorra ao menos um dos referidos atos mencionados em território nacional, que ao menos um computador (terminal) esteja situado no Brasil e que o provedor estrangeiro possua estabelecimento no Brasil para que o provedor seja obrigado a cumprir a legislação brasileira e observar os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, conforme determina o art. 11 do Marco Civil da Internet.

Os provedores devem prestar informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações, nos termos da LGPD, que será objeto de estudo de conteúdo posterior.

O art. 12 do Marco Civil da Internet prevê penalidades (advertência, multa de 10% do faturamento do grupo econômico no Brasil no seu último exercício, suspensão temporária até a proibição de exercício de atividades) em caso de descumprimento das disposições previstas nos arts. 10 e 11, relativas à proteção dos registros e dados pessoais e do conteúdo de comunicações privadas.

### **4.2.1 Da guarda de registros de conexão**

Provedores de acesso à internet são obrigados a manter os registros de conexão, sob sigilo, em ambiente controlado e segurança, pelo prazo de um ano, não podendo transferir tal responsabilidade para terceiros, conforme determina o art. 13 do Marco Civil da Internet.



De acordo com Gonçalves (2017), tais informações são importantes para a apuração de crimes e ilícitos civis, eis que elas auxiliam na identificação do(s) autor(es) das infrações por meio de informações cadastrais, registros de endereçamento de IP, aplicações utilizadas, horário de acesso, registro de dispositivos informáticos, geolocalização e a quantidade de dados trafegada.

Autoridades policial, administrativa ou o Ministério Público poderão requerer que os registros sejam armazenados por mais tempo.

Gonçalves critica tal possibilidade, na medida em que ela viabiliza uma forma de vigilância digital permanente e abusiva sobre o investigado, em prejuízo aos direitos fundamentais dos usuários.

Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata esse artigo deverá ser precedida de autorização judicial.

#### **4.2.2 Da guarda de registros de acesso a aplicações de internet na provisão de conexão**

Conforme prevê o art. 14 do Marco Civil da Internet, “na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet”.

Tal restrição objetiva evitar por parte dos provedores de conexão à internet, inclusive aqueles cuja contrapartida solicitada ao usuário pela disponibilização do serviço não é via remuneração financeira direta (mensalidades ou assinaturas), o monitoramento dos hábitos e padrões de acesso à internet dos usuários e consumidores, impondo o apagamento dos registros de acessos a sites e serviços na internet.

#### **4.2.3 Da guarda de registros de acesso a aplicações de internet na provisão de aplicações**

O provedor de aplicações de internet, ou seja, as empresas que prestam serviços ou ofertando produtos em determinado site ou portal de internet, deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, conforme determina o art. 15 do Marco Civil da Internet. Em conteúdo posterior, abordaremos com mais detalhes o dever legal dos fornecedores em proteger os



dados pessoais armazenados sob sua responsabilidade, sob a perspectiva da Lei Geral de Proteção de Dados Pessoais.

A autoridade policial, administrativa ou o Ministério Público poderão requerer a qualquer provedor de aplicações de internet o acesso aos registros, bem como determinar que estes sejam guardados, inclusive por prazo superior a 6 meses.

Finalmente, de acordo com o art. 17 do Marco Civil da Internet, a opção por não guardar os registros de acesso a conteúdo (aplicações de internet) não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

## **TEMA 5 – A RESPONSABILIDADE DO PROVEDOR DE APLICAÇÕES POR DANOS CAUSADOS POR CONTEÚDO GERADO POR TERCEIRO**

Na Seção III do Marco Civil da Internet, são estabelecidas regras de responsabilidade jurídica dos provedores diante de conteúdo produzido por terceiros, conforme prevê os arts. 18 a 21.

A primeira regra, prevista no art. 18, estabelece que “O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”.

De acordo com Gonçalves (2017), o provedor de conexão é responsável por disponibilizar um caminho lógico entre o aparelho do usuário (computador, celular, tablet etc.) para a internet, atribuindo endereço IP para navegar na internet e disponibilizando infraestrutura telemática para realizar o envio (*upload*) e o recebimento (*download*) de dados na rede.

Logo, para Gonçalves, dada a natureza do serviço prestado, o provedor de conexão à internet não tem, nem poderia ter, condições de ter acesso sobre os conteúdos gerados por terceiros, eis que sua atuação se limita a disponibilização de canal de comunicação entre os usuários e terceiros, não lhe competindo analisar conteúdos transmitidos.

O art. 19 do Marco Civil da Internet prevê a responsabilidade do provedor de aplicações de internet por danos causados por terceiros:

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.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Segundo Damásio de Jesus (2014), a necessidade de regulamentação sobre a responsabilidade do provedor de aplicações de conteúdo transmitido por seus clientes decorre de reiteradas decisões judiciais que condenaram indevidamente provedores de conteúdo, mesmo quando colaboravam com a autoridade judicial, identificando a autoria do crime eletrônico e removendo o conteúdo da internet, sob a justificativa de terem “disponibilizado o meio” para a divulgação do conteúdo ou “por não terem fiscalizado os conteúdos que hospedavam”.

Para Damásio de Jesus, o provedor de aplicação só será responsável por conteúdo gerado por terceiro se, após receber ordem judicial, recusar-se a adotar as medidas necessárias para tornar o conteúdo indisponível.

Além disso, o provedor de aplicação, se demandado judicialmente, deve fornecer o número de protocolo IP do criador do conteúdo ofensivo, permitindo, dessa forma, o afastamento de sua responsabilidade jurídica sobre o conteúdo ilícito produzido por terceiros.

Determinada judicialmente a remoção de conteúdo, o provedor de aplicações deverá dar ciência ao seu responsável, informando detalhadamente as razões que levaram à sua indisponibilização, conforme estabelece o art. 20 do Marco Civil da Internet:

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo,





salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

O solicitante da retirada do conteúdo poderá exigir que no lugar deste seja colocada a ordem judicial ou a justificativa para a remoção do conteúdo; neste último caso, geralmente, a menção expressa a violação ao termo de uso do provedor de aplicações.

É fundamental que a justificativa para a remoção de conteúdo seja detalhada, pois somente sabendo as razões que justificaram a retirada do conteúdo da internet é que o seu responsável poderá, se achar necessário, oportuno ou conveniente, exercer os direitos previstos nos princípios constitucionais do devido processo legal, o contraditório e a ampla defesa, evitando, inclusive, censura indevida.

Situação diversa ocorre quando o conteúdo que se pretende tornar indisponível tiver caráter privado, contendo cenas de nudez ou de natureza sexual, conforme estabelece o art. 21:

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.

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Tal hipótese permite que se dispense a exigência de ordem judicial para solicitar a retirada do conteúdo. Basta que a pessoa interessada na indisponibilização do conteúdo notifique extrajudicialmente o provedor do conteúdo, identificando detalhadamente o material que se pretende retirar e demonstrando ter legitimidade para exigir tal providência.

Trata-se do sistema “*notice and take down*”, ou seja, notificar e retirar imediatamente. Caberá ao provedor de aplicações verificar se o material possui ou não autorização para divulgação, e se há indícios do material causar prejuízos às pessoas envolvidas, causando-lhes danos em sua reputação e intimidade,



especialmente nas situações em que ficar evidenciada a prática de “*revenge porn*”, também chamada de “pornografia de vingança”, que possui nítido intuito de causar danos injustamente à pessoa exposta.

O art. 22 do Marco Civil da Internet prevê a possibilidade de o interessado solicitar judicialmente dados ao provedor de aplicações relativos a registros de acesso ou de conexão, com objetivo de preservar informações essenciais que servirão como provas importantes durante a instrução de um futuro processo judicial.

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Conforme prevê o parágrafo único do art. 22, os requisitos para o ajuizamento da demanda judicial envolvem a demonstração de indícios que efetivamente o interessado na medida judicial foi vítima de um ato ilícito. Não basta mera suspeita.

A medida deve ser muito bem justificada e o tempo que se pretende investigar, pois o acesso aos dados poderá causar violação de privacidade, relativizando o necessário sigilo de dados pessoais, conforme estudaremos em conteúdo posterior.

Finalmente, o art. 23 do Marco Civil da internet estabelece a importância do sigilo de informações recebidas, cabendo ao juiz tomar as providências necessárias para assegurá-lo, podendo inclusive determinar o segredo de justiça, inclusive para os pedidos de guarda de registro.

## **FINALIZANDO**

Nesta etapa, abordamos estratégias para viabilizar a autorregulamentação de fornecedores de produtos e serviços digitais, em busca não apenas do cumprimento da legislação que disciplina o setor, mas também da busca pela satisfação dos consumidores nesse relevante mercado.



Também analisamos os fundamentos constitucionais do Marco Civil da Internet, trazendo dados relacionados aos direitos e garantias dos usuários e os deveres e responsabilidades dos provedores de conexão e dos provedores de aplicações de internet.

Finalmente, apresentamos as possibilidades de provedores de aplicações de internet serem responsabilizados civilmente em virtude de danos decorrentes de suas atividades.

Esperamos que os conhecimentos apresentados sejam úteis e que facilitem a compreensão dos temas posteriores, ocasião em que analisaremos regras inerentes à LGPD e o direito à privacidade na era digital.



## REFERÊNCIAS

BRASIL. **Marco Civil da Internet**. Lei n. 12.965, de 23 de abril de 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>. Acesso em: 14 set. 2022.

\_\_\_\_\_. Lei n. 8.078, de 11 de setembro de 1990. **Diário Oficial da União**, Brasília, 12 set. 1990. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm)>. Acesso em: 14 set. 2022.

\_\_\_\_\_. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm)>. Acesso em: 15 set. 2022.

ARAUJO, J. de S. **Tripartição dos poderes e funções essenciais à justiça**. Curitiba: InterSaberes, 2021.

BENJAMIN, A. H. V.; MARQUES, C. L.; BESSA, L. R. **Manual de Direito do Consumidor**. 2. ed. São Paulo: Revista dos Tribunais, 2009.

EFING, A. C. **Fundamentos do direito das relações de consumo**. 2. ed. Curitiba: Juruá, 2004.

FIORILLO, C. A. P. **O Marco Civil da Internet e o meio ambiente digital na sociedade da informação**: Comentários à Lei n. 12.965/2014. São Paulo: Saraiva, 2015.

GONÇALVES, V. H. P. **Marco civil da internet comentado**. 1. ed. São Paulo: Atlas, 2017.

JESUS, D. de. **Marco Civil da Internet**: comentários à Lei n. 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014.

PORTAL DA TRANSPARÊNCIA. **Site Portal da Transparência**. Disponível em: <<https://www.portaltransparencia.gov.br/>>. Acesso em: 14 set. 2022.