

10 ANOS DO MARCO CIVIL DA INTERNET

Título

10 anos do Marco Civil da Internet

Realização

TozziniFreire Advogados

Autores

Ana Carolina de Paiva Monteiro
Ana Carolina Gaspar
Ana Carolina Katlauskas Calil
Bárbara Bassani de Souza
Bruna Borghi Tomé
Bruno Sá de Andrade
Carla do Couto Hellu Battilana
Clara Pacce P. Serva
Elias Marques de Medeiros Neto
Gabriela Vitiello Wink
Giovanni Paolo Falcetta
Helena Rocha Matos
Isabella Fontoura D'Angelo
Isabelle Ruiz Guero
João Vitor de Almeida Ramos
Júlia Viana
Laís Cury Rezende
Luciana Bazan Martins Bisetti
Luiz Renato Okumura
Luiza Sato
Marcela Waksman Ejnisman
Marco Aurélio Antas Torronteguy
Maria Eugênia Geve M. Lacerda
Maria Fernanda Seba Rahe
Marina Sayuri Kitayama
Marina Silveira Frank
Maurício de Carvalho Góes
Nicolas Eric Matoso Medeiros De Souza
Oswaldo Noce Dalla Torre
Patrícia Helena Marta Martins
Pedro Eroles
Pedro Vecci Biancardini
Rodrigo de Grandis
Shin Jae Kim
Sofia Kilmar
Stephanie Consonni De Schryver
Victor Hugo Callejon Avallone

Capa e diagramação

Samila Pacheco da Silva

Revisão

Allyne Pires

10 ANOS DO MARCO CIVIL DA INTERNET

2024

SUMÁRIO

/Prefácio

Capítulo 1 – Regulação da rede

Regulação da Internet e o futuro da rede

/Capítulo 2: Proteção de Dados e Segurança Online

Marco Civil e Proteção de Dados: consentimento e o caminho para regulação de proteção de dados no Brasil

Os desafios do combate às fraudes eletrônicas e a urgência de regulamentação do tratamento de dados na esfera criminal

O compartilhamento de dados na democratização do setor de Energia Elétrica

/Capítulo 3: Setores e Aplicações Específicas do Marco Civil da Internet

Direitos autorais e conexos e o Marco Civil da Internet

Marco Civil da Internet e eleições: desafios e perspectivas para o futuro

Direitos Humanos e Internet: promoção ou violação?

Open Finance e o Marco Civil da Internet

As normas sanitárias enquadradas pelo Marco Civil da Internet: um bug regulatório ou uma regulação viral?

Seguros: distribuição pela internet

A gestão e autenticidade dos livros societário digitais frente ao Marco Civil da Internet,

Protegendo seu investimento: considerações legais para potenciais compradores em operações de M&A envolvendo provedores de aplicações de internet à luz do Marco Civil da Internet

Compliance e transparência: a importância histórica e futura do MCI diante do desenvolvimento tecnológico

O potencial da inteligência artificial para moldar o futuro do comércio internacional brasileiro

/Capítulo 4: Marco Civil da Internet e Resolução de Disputas

Diálogos entre o Código de Processo Civil de 2015 e a internet

O valor probatório das mensagens eletrônicas no processo do trabalho

/Nosso autores

PREFÁCIO

Fernando Eduardo Serec

OLHARES SOBRE O PASSADO E O FUTURO DA GOVERNANÇA DIGITAL A PARTIR DA CELEBRAÇÃO DOS 10 ANOS DO MARCO CIVIL DA INTERNET

Em 23 de abril de 2014, há 10 anos, o Congresso Nacional promulgava a Lei Federal nº 12.965, marcando a história da governança digital no país e posicionando o Brasil como pioneiro na regulação das redes.

Originada do Projeto de Lei (PL) nº 2.126/2011, de relatoria do deputado Alessandro Molon, a legislação, que ficou popularmente conhecida como Marco Civil da Internet (MCI), foi fruto de um longo processo de criação colaborativa e multissetorial, que teve início em 2011 e reuniu especialistas dos mais diversos segmentos para discutirem as diferentes perspectivas com o intuito de alcançar um modelo equilibrado entre regulação e liberdade.

Acadêmicos, especialistas, professores, advogados, músicos, bibliotecários e artistas ilustram a representatividade social que marcou o processo de deliberação do texto da lei, que, destaca-se, foi muito semelhante ao proposto pela sociedade civil a partir de uma Consulta Pública realizada de forma online em 2009 com mais de 800 contribuições. Um verdadeiro fenômeno de participação social bem-sucedida.

A coalização inicial do MCI é um espelho da efetivação do essencial componente democrático na rotina legislativa e um exemplo claro da importância da articulação entre sociedade civil e o Estado para a criação de normas bem-sucedidas e que se prolongam no tempo.

Passados 10 anos, o MCI continua sendo um marco global, reconhecido, internacionalmente, pela sua força, sofisticação e qualidade. Trata-se de uma lei que, a partir da abordagem principiológica, protege a liberdade de expressão, o direito à privacidade e a neutralidade das redes.

Nesse aspecto, a legislação foi responsável por estabelecer princípios fundamentais que nortearam o desenvolvimento da internet no país, promovendo a inovação contínua, a inclusão digital e o respeito aos direitos fundamentais dos cidadãos.

Também conhecida como “Constituição da Internet”, o MCI trouxe segurança jurídica aos usuários, às empresas e ao Poder Público, incentivando o desenvolvimento econômico, atraindo investimentos e fomentando o crescimento do setor de tecnologia no Brasil.

Sem o prejuízo da importância de se discutir avanços, é preciso celebrar e reconhecer o legado do MCI e seu papel pioneiro e transformador na construção de uma internet livre, segura e inclusiva no Brasil, contando com reflexos no mundo todo.

Essa obra, escrita a muitas mãos, reúne artigos produzidos por profissionais de diversas áreas de TozziniFreire Advogados e se propõe a compartilhar olhares sobre o passado e futuro da governança digital no Brasil, a partir da análise da influência do Marco Civil nos novos modelos de negócios e nas práticas empresariais.

As reflexões aqui propostas vêm de profissionais que acompanham diariamente os reflexos da legislação em suas áreas de prática, auxiliando empresas dos mais diversos setores a navegarem por um ambiente jurídico multifacetado e dinâmico, conduzindo trabalhos expressivos que nos tornaram referência no ambiente jurídico.

Acreditamos que a união de diferentes pontos de vista nos diferencia na construção de soluções jurídicas inovadoras e contribui, ativamente, para o aprimoramento da sociedade brasileira.

Combinando conhecimento técnico, experiência de quase 50 anos de prática jurídica e visões de caráter estratégico e multidisciplinar, nossos profissionais estão, constantemente, atentos às transformações que permeiam a sociedade e os negócios, em busca da manutenção e fortalecimento de uma advocacia inovadora e pioneira.

Assim como expressou Carlos Drummond de Andrade no verso “não serei o poeta de um mundo caduco”, é preciso esforços conjuntos para a construção de normas não sujeitas à caducidade precoce que, por vezes, permeia a criação de leis em um mundo volátil, de constantes e rápidas transformações.

Convidamos você a embarcar nessa jornada de reflexão e celebração pelos 10 anos do Marco Civil da Internet.

Capítulo 1

/Regulação da rede

REGULAÇÃO DA INTERNET E O FUTURO DA REDE

Patricia Helena Marta Martins
Gabriela Vitiello Wink
Luciana Bazan Martins Bisetti
Nicolas Eric Matoso Medeiros De Souza

A partir do momento que os escândalos provocados pelas publicações feitas por Edward Snowden repercutiram no Brasil, o tema se tornou uma prioridade em razão da grave constatação de que o governo brasileiro havia sido espionado. Naquele momento, a proposta que se tornaria a Lei nº 12.965/2014 ou o Marco Civil da Internet (MCI) estava pendente de análise na Câmara dos Deputados há quase dois anos.

O MCI não era uma proposta do governo, mas sim da sociedade, que surgiu como alternativa à intitulada Lei Azeredo, um Projeto de Lei (PL) que propunha a regulação da internet. No entanto, por ter uma redação ampla, se aprovada, a Lei Azeredo provocaria um retrocesso no ambiente regulatório da internet no Brasil, já que criminalizava práticas de milhões de pessoas como a transferência de músicas entre dispositivos pessoais ou o desbloqueio dos celulares para uso em diferentes operadoras¹.

Como contraponto à essa proposta, as discussões com relação à proposta que originou o MCI ganharam força, seguindo por um caminho diverso da Lei Azeredo. Em vez de reprimir e punir, o MCI traduziu princípios fundamentais da Constituição Federal para a internet. O texto da proposta foi colocado em ampla discussão por meio de uma plataforma colaborativa (www.culturadigital.org/marcocivil), o que permitiu a ampla participação da sociedade. E não apenas foram considerados os comentários feitos formalmente via tal plataforma, como também todos aqueles mapeados por meio de redes sociais, artigos, textos publicados em blogs entre outras formas de contribuição.

Como resultado, o MCI aprovado promove a liberdade de expressão, a privacidade, a neutralidade da rede, fomenta o direito de acesso à internet, cria o regime de responsabilização dos provedores, desenhando uma estrutura de regulação crucial para a inovação.

1 LEITE, George S.; LEMOS, Ronaldo. Marco Civil da Internet. São Paulo: Editora Atlas, 2014.

Passados 10 anos de sua vigência, há diversas novas frentes de atuações que visam, de alguma forma, “re-regular” a internet.

O Congresso Nacional tem o tema em pauta, sendo a discussão de maior destaque a do PL nº 2.630/2020 (PL das Fake News), cujos objetivos são o fortalecimento da democracia, transparência dos provedores e controle na difusão de notícias falsas e discursos de ódio no ambiente virtual.

Seus principais pontos são: dever das plataformas de vetar contas inautênticas; divulgação de relatórios trimestrais de transparência sobre moderação de conteúdos; criação do Conselho de Transparência e Responsabilidade na Internet; possibilidade de provedores criarem instituição de autorregulação, certificada pelo conselho.

Já a reforma do Código Civil traz uma série de disposições com o objetivo de incorporar o Direito Digital ao Código Civil, considerando que as novas estruturas digitais modificaram as relações interpessoais, o trabalho, os negócios, o lazer, a educação e o acesso à informação. Sob a justificativa de que os provedores de aplicação de internet atualmente desempenham papel fundamental na organização e distribuição de informações, uma série de alterações tem sido discutidas no Congresso Nacional.

Dentre as alterações propostas, há disposições que regulam a relação dos provedores de aplicação, dispendo sobre (i) avaliação anual dos riscos sistêmicos decorrentes do funcionamento dos respectivos serviços dos provedores de aplicação; (ii) adoção de medidas de diligência para garantir a conformidade dos seus sistemas e processos com os direitos da personalidade e os direitos à liberdade de expressão e de informação e de medidas de moderação que respeitem esses direitos; (iii) divulgação dos termos de uso de forma clara e acessível, inclusive com relação às medidas de moderação; (iv) auditoria independente para avaliação do cumprimento das novas obrigações; (v) responsabilização das plataformas com relação aos anúncios nela veiculados e por danos decorrentes de conteúdos orgânicos, quando descumpridas as obrigações previstas em Lei.

No âmbito do Poder Executivo, destacam-se as ações da Secretaria Nacional do Consumidor (Senacon) do Ministério da Justiça e Segurança Pública (MJSP), que tem atuado sob a perspectiva da proteção dos consumidores no ambiente digital.

A Portaria MJSP nº 351/2023, por exemplo, dispôs sobre medidas administrativas a serem adotadas no âmbito do MJSP para fins de prevenção à disseminação de conteúdos ilícitos, prejudiciais ou danosos. De acordo com as suas disposições, fica a cargo da Senacon a instauração de processos administrativos para apurar a responsabilidade das plataformas no descumprimento do dever geral de

segurança e cuidado em relação à disseminação de conteúdos que incitam ataques no ambiente escolar ou que façam apologia a crimes.

Já as Notas Técnicas² editadas pela Senacon abordam como o órgão entende pela responsabilidade dos provedores em relação aos conteúdos e anúncios veiculados em seus serviços. Em que pese o disposto no artigo 19 do MCI, a Senacon entendeu que os provedores são responsabilmente solidários já que, no caso de anúncios, recebem pela veiculação, além do fato de que, assim como no caso de conteúdos orgânicos, os provedores moderam aquilo que pode ou não ser veiculado, atraindo o disposto no art. 14 do Código de Defesa do Consumidor (CDC).

Em outubro de 2023, houve a criação da Secretaria de Direitos Digitais (Sedig), estrutura responsável pela avaliação e proposição de medidas que tornem o ambiente cibernético mais seguro para os usuários, com implementação de ações de proteção de direitos em ambiente digital. Dentre suas atribuições, destaca-se o aperfeiçoamento da legislação relativa aos direitos no ambiente digital e a de cooperar com outros órgãos governamentais em debates sobre o tema. Dessa forma, a Sedig torna-se uma importante estrutura para a discussão de temas afetos aos direitos digitais, inclusive com relação à regulação da internet, competência que ficou a cargo da Secretaria de Assuntos Legislativos do Ministério da Justiça quando das discussões relativas à proposta que deu origem ao MCI.

No âmbito internacional, destaca-se a União Europeia (UE), que têm promovido a atualização dos seus normativos para o ambiente digital. Dentre essas atualizações, houve a aprovação do Regulamento UE 2022/2.065, denominado *Digital Service Act* (DSA), que regula o funcionamento dos provedores de aplicação que atuam na União Europeia. Tanto o DSA quanto as propostas brasileiras buscam enfrentar desafios comuns relacionados à regulação da internet e possuem semelhanças entre si. No entanto, há algumas lições que podem ser aproveitadas pelos normativos brasileiros em discussão no Congresso Nacional.

Um dos pontos polêmicos atualmente em discussão é a criação de uma estrutura do Governo Federal responsável pela regulação dos provedores no Brasil, algo que inexiste no DSA, que prevê apenas as autoridades competentes para fiscalizar o cumprimento das obrigações previstas no Regulamento e envolve diversas autoridades competentes (órgãos de defesa do consumidor, concorrenciais e de proteção de dados).

A criação de um órgão de regulação é prevista pelo PL das Fake News, que coloca como uma das suas competências a criação de uma série de diretrizes aos

2 Nota Técnica nº 5/2023/CGCTSA/DPDC/SENACON/MJ; Nota Técnica nº 11/2023/CGCTSA/DPDC/SENACON/MJ; e Nota Técnica nº 7/2023/CGCTSA/DPDC/SENACON/MJ.

provedores de aplicação, inclusive com relação à liberdade, responsabilidade, transparência, moderação, termos de uso, protocolos de segurança e análise e tratamento de riscos sistêmicos. Essa competência ampla com relação às diretrizes pode impedir que os provedores atuem de forma eficaz na moderação e com vistas a evitar a censura prévia, atingindo diretamente a liberdade de expressão dos usuários.

Ademais, é importante definir como ocorrerá a cooperação entre as autoridades brasileiras, para que haja uma atuação conjunta entre eles e com esse novo órgão regulador, de forma a não haver sobreposição de competências, fato que pode resultar em insegurança jurídica para os provedores de aplicação e no excesso de judicialização com relação às decisões dos órgãos, em especial as de cunho sancionatório.

Para além do PL das Fake News, há a discussão sobre se haveria a necessidade de criação de um novo órgão regulador ou se alguma das estruturas já existentes poderia exercer esse papel. A Agência Nacional de Telecomunicações (Anatel) já manifestou preocupação com temas relacionados à regulação da internet e sinalizou publicamente o seu interesse como órgão regulador da matéria.

Recente pesquisa conduzida pelo Comitê Gestor do Brasil (CGI.br)³ revelou ser controverso o apoio ao papel da Anatel como reguladora das plataformas digitais. Enquanto a Agência defende sua capacidade de exercício da função em razão dos seus poderes fiscalizadores e sancionadores, participantes da pesquisa conduzida pelo CGI.br afirmaram que as sanções aplicadas pela Anatel teriam baixa eficácia. Já aqueles que defendem a posição da Anatel, como associações ligadas a serviços de telecomunicações e de internet, argumentam que a agência possui expertise na atuação junto a provedores e operadoras.

Outro ponto que merece atenção é o regime de responsabilização dos provedores de aplicação. O PL das Fake News dispõe que os provedores podem ser responsabilizados civilmente, de forma solidária, pelos danos causados por conteúdos de terceiros, sejam eles impulsionados ou em caso de descumprimento do dever de cuidado. Na mesma linha, segue a Reforma do Código Civil com relação aos conteúdos de terceiros que foram impulsionados, mas que deixa de falar no dever de cuidado para inserir a responsabilidade em caso de descumprimento das obrigações previstas em Lei.

Na forma como atualmente prevista nas propostas brasileiras, o atendimento ao dever de cautela obrigará que os provedores de aplicação assumam a análise de legalidade dos conteúdos, função tradicionalmente exercida pelo Poder Judiciário.

3 CAPPI, Juliano; OMS, Juliana. Sistematização das contribuições à consulta sobre regulação de plataformas digitais. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2023.

Além disso, a responsabilização solidária com relação aos anúncios, previsto tanto pelo PL das Fake News quanto pela Reforma do Código Civil, volta a restringir os micros e pequenos empreendedores do acesso a formas de propaganda. Isso porque ambas as proposições geram uma burocratização adicional, fazendo com que os anúncios passem por revisão extensa e demorada, acarretando o aumento de custos para àqueles que desejam veicular anúncios por meios dos provedores de aplicação.

Parte do debate sobre regulação da internet tem ocorrido com base na falsa percepção de que os provedores de aplicação lucram com conteúdo ilegal e danoso, o que pode gerar uma regulação exagerada, indo em caminho contrário ao que a regulação deveria seguir.

A regulação da internet é desejada, mas alguns pontos presentes nas propostas brasileiras são preocupantes e demandam uma discussão aprofundada, com a participação de todos os atores envolvidos. Do contrário, as propostas podem representar em uma regulação não adequada, uma nova Lei Azeredo, ameaçando a internet livre, democrática, aberta e inovadora.

Capítulo 2

/Proteção de Dados e Segurança Online

MARCO CIVIL E PROTEÇÃO DE DADOS: CONSENTIMENTO E O CAMINHO PARA REGULAÇÃO DE PROTEÇÃO DE DADOS NO BRASIL

Marcela Waksman Ejnisman
Carla do Couto Hellu Battilana
Maria Eugênia Geve M. Lacerda

INTRODUÇÃO

A era digital transformou radicalmente a maneira como interagimos, comunicamos e fazemos negócios, trazendo consigo desafios inéditos relacionados à proteção de dados pessoais. À medida que a sociedade se torna cada vez mais conectada, a privacidade e a segurança dos dados pessoais emergem como questões importantes.

Este artigo aborda a evolução do consentimento desde a sua formulação no Marco Civil da Internet (MCI) até as exigências da Lei Geral de Proteção de Dados (LGPD), assim como as implicações práticas dessas mudanças para o mercado. Ademais, examinaremos como as organizações estão se adaptando a essas novas exigências e quais são as perspectivas futuras para a proteção de dados no Brasil.

Ao longo deste estudo, buscamos não apenas destacar os aspectos legais e técnicos envolvidos na proteção de dados pessoais, mas também refletir sobre a importância de criar uma cultura de privacidade que respeite os direitos dos indivíduos e promova práticas empresariais responsáveis. Nesse sentido, o diálogo contínuo entre o MCI e a LGPD serve como um modelo dinâmico para a adaptação às rápidas mudanças do cenário digital, oferecendo *insights* valiosos sobre como navegar coletivamente em direção a um futuro mais seguro e transparente no que diz respeito à proteção de dados pessoais.

BREVE PANORAMA HISTÓRICO DA PROTEÇÃO DE DADOS NO BRASIL

O Brasil precisava de uma lei que abordasse o uso da internet e a proteção de dados pessoais na era digital, criando um sistema de governança e regulando a atividade online. Foi nesse contexto que surgiu o Marco Civil da Internet (MCI), promulgado em 2014. Essa legislação foi pioneira ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a proteção de dados pessoais.

O MCI trouxe importantes inovações, como a exigência de consentimento expresso e informado para a coleta e tratamento de dados pessoais, a obrigatoriedade de informações claras sobre a utilização desses dados e o direito dos usuários de exigir a exclusão de seus dados pessoais ao término da relação com as empresas. Essas disposições representaram um avanço significativo na proteção da privacidade e dos dados pessoais no Brasil, estabelecendo um marco legal para a internet e servindo como base para a legislação subsequente.

Anos mais tarde, a Lei Geral de Proteção de Dados (LGPD) foi publicada com o intuito exclusivo de regular o tratamento de dados pessoais. Inspirada em modelos regulatórios internacionais, como o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia, a lei representou um passo significativo na consolidação dos direitos dos titulares de dados e na imposição de deveres específicos às organizações que tratam dados pessoais.

O panorama histórico da proteção de dados pessoais no Brasil demonstra uma evolução legislativa que partiu de princípios constitucionais gerais para a adoção de um marco regulatório específico para a internet e, posteriormente, para uma legislação abrangente focada na proteção de dados pessoais. Esse desenvolvimento reflete a crescente importância atribuída à privacidade e à proteção de dados pessoais na sociedade brasileira e a necessidade de adequação às dinâmicas globais de tratamento de informações na era digital.

CONSENTIMENTO NO MARCO CIVIL DA INTERNET

A noção de consentimento, conforme delineada no MCI, constitui um pilar fundamental para a proteção de dados pessoais na rede. O consentimento, nesse marco legislativo, é definido como a manifestação **livre, expressa e informada** pela qual o titular dos dados pessoais autoriza o seu tratamento para determinadas finalidades. Dessa forma, o MCI avança na proteção da privacidade ao exigir que

qualquer coleta, uso ou tratamento de dados pessoais na internet seja precedido de uma autorização clara e inequívoca do titular.

O consentimento é “livre” quando não é coagido e o titular possui efetivo poder de decisão, podendo optar, ou não, pelo tratamento. Ser “expresso” implica que as empresas devem obter a concordância do usuário de maneira ativa, não sendo suficiente a simples utilização de mecanismos passivos ou presumidos de aceitação. Por fim, o consentimento “informado” exige que a comunicação seja clara e acessível, fornecendo todas as informações necessárias para que o indivíduo compreenda a extensão e os efeitos do tratamento dos seus dados pessoais.

No entanto, observou-se uma tendência das empresas em elaborar políticas de privacidade *pro forma*, complexas e extensas, visando cumprir formalmente com a exigência de consentimento expresso e informado. Essa prática resulta em documentos repletos de jargões técnicos, dificultando que usuários compreendam plenamente as implicações da autorização que estão concedendo. Esse fenômeno evidencia a discrepância entre a intenção da lei de promover a transparência e a prática de submergir os usuários em um oceano de informações pouco compreensíveis.

Apesar dessa abordagem inicialmente formalista e pouco transparente, o cenário começou a mudar, especialmente diante do aumento da consciência global sobre a importância da proteção de dados. A repercussão de escândalos de violação de privacidade e a implementação de regulações internacionais mais rigorosas, como o GDPR, incentivaram uma mudança de atitude nas empresas.

Tornou-se claro o movimento crescente em direção à adoção de práticas mais éticas e transparentes no tratamento de dados pessoais, incluindo a elaboração de políticas de privacidade claras e a implementação de mecanismos de consentimento robustos.

Além disso, a pressão exercida tanto pela sociedade civil quanto por órgãos reguladores tem levado as empresas a reconhecer que a proteção de dados pessoais não é apenas uma exigência legal, mas um componente crítico da confiança do consumidor. Isso se reflete em um esforço para além do cumprimento normativo, visando a construção de uma relação mais transparente e respeitosa com os titulares dos dados.

COMPARAÇÃO ENTRE O CONSENTIMENTO NO MARCO CIVIL DA INTERNET E NA LEI GERAL DE PROTEÇÃO DE DADOS

A implementação da LGPD representou um avanço significativo na proteção de dados pessoais no Brasil, expandindo e detalhando os princípios já estabelecidos pelo MCI. Uma das diferenças fundamentais entre essas legislações reside no escopo de aplicação: enquanto o MCI foca na regulamentação do uso da rede, a LGPD tem um campo de aplicação mais amplo, abrangendo o tratamento de dados pessoais tanto no ambiente digital, quanto offline.

Dentro da LGPD, o consentimento mantém-se como um dos pilares para o tratamento de dados pessoais, mas não é mais visto como a única base legal possível. A lei estabelece diversas alternativas para o tratamento de dados, como o cumprimento de obrigação legal ou regulatória pelo controlador, a execução de políticas públicas, a realização de estudos por órgão de pesquisa, a proteção da vida ou da incolumidade física do titular ou de terceiro, entre outros. Essa diversidade de bases legais indica uma flexibilização na abordagem do tratamento de dados, reduzindo o protagonismo do consentimento em determinadas situações, onde outras hipóteses podem ser aplicadas para justificar o tratamento de dados pessoais.

A LGPD define o consentimento de maneira semelhante ao MCI, sendo a manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para um propósito determinado. O aspecto “inequívoco” do consentimento, que se aproxima da qualificadora “expresso” na redação do MCI, está relacionado à manifestação ativa de vontade do titular. Além disso, o consentimento “informado”, passa a ser aquele no qual o titular tem acesso claro e completo às informações sobre o tratamento de seus dados, incluindo a finalidade específica, a forma e a duração do tratamento, bem como informações sobre a possibilidade de não fornecer consentimento e as consequências dessa escolha.

Comparando as qualificadoras do consentimento entre a LGPD e o MCI, observamos que ambas as legislações valorizam a autonomia do titular dos dados e a transparência no tratamento de dados pessoais. No entanto, a LGPD avança ao detalhar mais explicitamente os critérios que tornam o consentimento válido, além de introduzir um espectro mais amplo de bases legais para o tratamento de dados, refletindo uma abordagem adaptável às diversas realidades do tratamento de informações.

MUDANÇAS PRÁTICAS OBSERVADAS PELO MERCADO A PARTIR DA NOVA INTERPRETAÇÃO DO CONSENTIMENTO

A nova interpretação do consentimento, impulsionada pela LGPD e pela evolução contínua do MCI, tem desencadeado uma série de mudanças práticas no mercado. Essas mudanças refletem o esforço das organizações em se adaptarem a um ambiente regulatório mais estrito e a uma sociedade cada vez mais consciente sobre a importância da privacidade.

Uma dessas mudanças práticas é a aplicação de princípios de *design thinking* e *legal design* nas políticas de privacidade. Essa abordagem visa tornar o conteúdo mais tangível, acessível e compreensível para os titulares dos dados. Com o auxílio de infográficos, linguagem clara e interfaces intuitivas, as organizações buscam garantir que os usuários compreendam seus direitos e as práticas de tratamento de dados, facilitando assim uma escolha informada ao fornecerem seu consentimento.

Além disso, existe a tendência natural de adotar bases legais alternativas para o tratamento de dados, reduzindo a dependência exclusiva do consentimento. Isso alinha-se à flexibilidade proposta pela LGPD, que permite outras bases legais, como o legítimo interesse, o cumprimento de obrigações legais e a execução de contratos.

Em relação às técnicas de *privacy by default*, as organizações estão começando a implementar abordagens que presumem a privacidade como configuração padrão. Isso inclui a apresentação do *opt-out* como regra em determinadas situações, onde o tratamento de dados é realizado conforme outras bases legais que não o consentimento expresso. Essa prática visa assegurar que os dados pessoais sejam protegidos desde o início, minimizando a coleta e o uso de dados ao estritamente necessário.

Essas mudanças práticas refletem um cenário de adaptação e evolução constante das organizações frente às demandas regulatórias e às expectativas dos consumidores. A busca por uma maior transparência, o respeito pela privacidade dos usuários e a adoção de práticas de tratamento de dados mais éticas são sinais de um mercado que se move em direção à conformidade legal e ao respeito pelos direitos dos indivíduos. As organizações que compreendem e se adaptam a essas mudanças demonstram não apenas um compromisso com a legalidade, mas também com a construção de uma relação de confiança duradoura com seus usuários.

CONCLUSÃO

Ao longo deste artigo, exploramos as nuances e implicações do consentimento no Marco Civil da Internet, a comparação desse com as disposições da LGPD e as mudanças práticas observadas pelo mercado diante da nova interpretação de consentimento. As reflexões aqui apresentadas evidenciam um cenário jurídico em evolução e uma sociedade cada vez mais consciente sobre a importância da proteção de dados pessoais.

A implementação de princípios de *design thinking* e *legal design*, a adoção de bases legais alternativas e as técnicas de *privacy by default* são algumas das mudanças práticas que ilustram o esforço das organizações para se adaptarem a esse novo panorama.

Olhando para o futuro, espera-se que o diálogo entre o MCI e a LGPD continue a evoluir, fomentando um ecossistema digital que respeite os direitos dos titulares de dados enquanto promove a inovação e o desenvolvimento tecnológico. A conscientização dos usuários sobre seus direitos e a capacidade das organizações de implementar práticas de proteção de dados eficazes serão cruciais para esse equilíbrio.

Finalmente, este artigo destaca a importância de uma cultura de proteção de dados robusta, que vai além da mera conformidade legal e se traduz em práticas empresariais responsáveis e sustentáveis. À medida que a sociedade avança, a proteção de dados pessoais emerge não apenas como uma questão legal, mas como um valor intrínseco à dignidade e ao respeito pela autonomia individual.

OS DESAFIOS DO COMBATE ÀS FRAUDES ELETRÔNICAS E A URGÊNCIA DE REGULAMENTAÇÃO DO TRATAMENTO DE DADOS NA ESFERA CRIMINAL

Rodrigo de Grandis
Ana Carolina de Paiva Monteiro

INTRODUÇÃO

O aumento exponencial dos casos de crimes patrimoniais cometidos no âmbito virtual no Brasil é notório, inclusive no âmbito empresarial. Todos conhecemos alguém que já sofreu ao menos uma tentativa de golpe. De acordo com o Anuário Brasileiro de Segurança Pública, publicado em 21 de julho de 2023¹, essa situação é resultado de uma reconfiguração das relações humanas no contexto virtual, especialmente após a pandemia de Covid-19. Esse fenômeno, portanto, está diretamente relacionado ao aumento do uso da internet e de redes sociais pela população, o que acabou por criar um enorme campo de oportunidade para os criminosos virtuais.

Os estudos apontaram que, entre 2018 e 2022, os registros de ocorrências pelas Polícias Cíveis relacionados a fraudes eletrônicas dispararam de 426.799 para 1.819.406 casos, representando um crescimento de mais de 325% e o equivalente a aproximadamente 207 casos por hora no país. As pesquisas realizadas indicam

1 LIMA, Renato Sérgio de; BUENO, Samira. As novas configurações dos crimes patrimoniais no Brasil. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, p. 90-97, 2023. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf>. Acesso em: 14 de mar. de 2024.

que tais agentes têm explorado fatores situacionais ao identificar vítimas mais vulneráveis, de modo a diversificar os métodos de ataque e empregar técnicas para que os usuários das redes sociais e aplicativos de mensagens sejam induzidos a compartilhar dados confidenciais com os criminosos.

Essas condutas foram recentemente objeto de maior repressão penal, com a inclusão de um tipo qualificado de estelionato previsto no artigo 171, parágrafo 2º-A, no Código Penal brasileiro, mas permanecem os desafios para a eficácia da investigação, da persecução penal e da pretendida punição dos criminosos.

De um lado, embora tenham sido criadas delegacias e órgãos internos nos Ministérios Públicos especializados em crimes virtuais, o aparato tecnológico para o deslinde das investigações ainda é bem precário e ineficiente para desvendar a prática criminosa, especialmente frente à agilidade dos fraudadores. Além de entraves técnicos, existem dificuldades decorrentes da ausência de uma regulamentação específica em âmbito criminal sobre a proteção de dados pessoais, levando as autoridades a se equilibrarem apenas no Marco Civil da Internet (MCI), Lei nº 12.965/2014, para obtenção das informações necessárias às investigações policiais. Isso porque, a esperada LGPD-Penal (Projeto de Lei, PL, nº 1.515/2020), apesar de proposta em junho de 2022, ainda aguarda a constituição de uma Comissão Especial para analisar essa matéria.

DESAFIOS NO COMBATE DA CRIMINALIDADE VIRTUAL RELACIONADA ÀS FRAUDES ELETRÔNICAS

O crescimento excepcional do volume de casos de fraudes eletrônicas nos últimos anos, conforme apontado pelo Anuário Brasileiro de Segurança Pública, constitui importante embaraço no combate às fraudes eletrônicas.

Embora, por meio da Lei nº 12.735/2012, tenha sido determinada a criação e estruturação de setores e equipes especializadas no combate aos crimes cometidos em redes de computadores, dispositivo de comunicação ou sistema informatizado, parece não ter havido, até hoje, expansão suficiente das unidades policiais de maneira a acompanhar a crescente complexidade e quantidade de delitos cibernéticos. Em outras palavras, o avanço da tecnologia e – quase que naturalmente – dos métodos de ataques criminosos colocam em xeque a estrutura e atividade tradicionais da polícia na condução da investigação e na prevenção criminal. É possível apostar, no mínimo, no investimento para o aumento do número de delegacias especializadas não só nos grandes centros, mas também em localidades

diversas, para que se crie uma efetiva rede de suporte e atendimento a esse tipo de demanda.

Além da quantidade insuficiente de unidades policiais especializadas frente ao crescimento exponencial do volume de trabalho relacionado a golpes cibernéticos – o que resulta, em muitas comarcas, no direcionamento desses casos a profissionais não capacitados – há também uma desproporcionalidade significativa entre os recursos disponíveis e a quantidade de ocorrências recebida. Isso é, as unidades policiais que apuram fraudes eletrônicas não têm aparato humano, financeiro e técnico necessário para a condução das investigações e conclusão dos casos, com a qualidade que se espera.

Ainda, o enfrentamento aos crimes cibernéticos também está diretamente relacionado à necessidade de formação de agentes capacitados por meio de cursos especializados e de rotina rígida de atualização do tema, dada a velocidade das inovações tecnológicas, o que extrapola as habilidades tradicionalmente desenvolvidas pelas academias de polícia.

De mais a mais, há também desafios decorrentes do próprio MCI a serem superados. Sabe-se que essa Lei busca disciplinar o uso da rede de computadores visando, sobretudo, o resguardo dos princípios constitucionais que estabelecem a proteção da privacidade e de dados pessoais dos seus usuários. Aliás, a exposição de motivos desse marco regulatório² já apresentava a imprescindibilidade de melhoria do diálogo entre o Direito e a Internet, ao colocar que a finalidade da nova legislação seria – e ainda é – transitar como “uma norma que reconheça a pluralidade das experiências e que considere a riqueza e a complexidade dessa nova realidade”, de forma a equilibrar, de um lado, a vida privada e sua inviolabilidade e, de outro, a garantia da guarda e disponibilização de dados e registros para o atendimento de ordens judiciais que demandem o compartilhamento de tais informações.

A intimidade, embora seja uma garantia constitucional, não é absoluta, e o MCI demonstra que o legislador não deixou essa flexibilização à margem da inovação legislativa proposta. A esse respeito, o art. 10, §3º da lei estabelece que os dados cadastrais, consistentes na qualificação pessoal, filiação e endereço, podem ser acessados pelas autoridades administrativas “que detenham competência legal para a sua requisição”, independentemente, inclusive, de ordem judicial.

Já os registros de conexão e de acesso a aplicações de internet e o conteúdo de comunicações privadas deverão ser fornecidos pelos respectivos provedores

2 Disponível em: https://www.planalto.gov.br/ccivil_03/projetos/expmotiv/emi/2011/86-mj%20mp%20mct%20mc.htm. Acesso em: 14 de mar. de 2024

às autoridades requerentes, de maneira autônoma ou associada, tão somente mediante ordem judicial suficientemente fundamentada, nos termos dos arts. 13, §5º e 15, §3º no MCI. Sem deixar de reconhecer o absoluto acerto do legislador ao condicionar a violação da privacidade e de dados pessoais dos usuários da rede a uma ordem judicial fundamentada, é certo que aqui reside um dos maiores desafios das investigações criminais: obter informações de absoluta relevância para o deslinde do caso a tempo de se conseguir combater a criminalidade das ágeis fraudes eletrônicas.

Não se desconhece que do ponto de vista da prática forense criminal, a necessidade de uma autorização judicial para obtenção de parte das informações acima mencionadas implica em uma maior delonga procedimental, que pode se tornar incompatível com a agilidade necessária para fazer cessar a conduta criminosa, por exemplo, de um agente que aplica sucessivos golpes em um único dia. Por isso, quando identificada uma linha investigativa que demanda a quebra de sigilo telemático – importante ferramenta para identificação de autoria de cibercrimes em geral –, não é incomum que a polícia fique para trás na disputa com o fraudador e a investigação perca o fôlego.

No entanto, razões dessa natureza não são suficientes para relativizar a imprescindibilidade da análise jurisdicional sobre a necessidade e proporcionalidade da comunicação privada do usuário da rede, tão bem tutelada pelo MCI e resguardada pelas empresas provedoras de conexão e de aplicação com atuação nacional.

Nesse cenário, e a despeito do esforço sistêmico para o combate da criminalidade virtual, os desafios para investigações criminais dessa natureza, sobretudo de fraudes eletrônicas, não param de crescer na mesma velocidade em que a tecnologia avança. Espera-se, ao menos, efetivo investimento de recursos por parte do Poder Público e energia da comunidade jurídica para discutir, com a seriedade e a complexidade que o tema exige, projetos legislativos já apresentados no Congresso Nacional e que podem contribuir para o avanço no enfrentamento do crime virtual.

O PL FEDERAL Nº 1.515/2022 E A URGÊNCIA NA CRIAÇÃO DE REGULAMENTAÇÃO DEFINITIVA PARA O TRATAMENTO DE DADOS PESSOAIS NA ESFERA CRIMINAL

Além do MCI, que representou o primeiro grande passo do Brasil em direção à regulamentação das atividades desenvolvidas no âmbito virtual, em maio de

2021, entrou em vigor a Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados (LGPD)³, destinada a estabelecer o tratamento de dados pessoais por pessoas físicas ou jurídicas, públicas ou privadas, garantindo-se “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º da lei).

Contudo, apesar de seu caráter complementar em relação ao MCI, a LGPD excluiu expressamente do seu escopo o tratamento de dados realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III, “a” a “d”). A Lei também estabeleceu que o tema será regido por uma legislação específica, que crie medidas proporcionais e estritamente necessárias para o atendimento ao interesse público, respeitados o devido processo legal, os princípios gerais de proteção e os direitos do titular, já previstos na LGPD (art. 4º, §1º).

Diante disso, excluída a matéria criminal do referido diploma, e considerando os diversos desafios já descritos atualmente enfrentados diante da criminalidade virtual, sobretudo nas fraudes eletrônicas, a criação de regulamentação específica para tratamento de dados na esfera criminal é medida que se impõe, em caráter de urgência.

Em novembro de 2020, foi apresentado Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, elaborado por grupo de juristas e liderado pelo ministro do Superior Tribunal de Justiça (STJ), Nefi Cordeiro⁴. Posteriormente, em junho de 2022, foi levado à Câmara dos Deputados o PL nº 1.515/2020⁵, buscando sanar lacuna legislativa deixada pela LGPD. De acordo com a exposição de motivos apresentada, o PL objetiva (i) garantir maior segurança jurídica com a regulamentação, em um único instrumento, das finalidades do tratamento de dados; (ii) atribuir, de forma proporcional e razoável, as responsabilidades aos órgãos que serão encarregados pela atividade; (iii) não impedir o fluxo de informações de dados pessoais entre os órgãos responsáveis; (iv) manter o foco no tratamento em si das informações, e não nas tecnologias utilizadas para essa atividade, tendo em vista as constantes inovações. Ainda, o texto legal destacou a importância do “dever desses agentes quanto ao inalienável respeito ao direito fundamental dos titulares de dados pessoais na proteção

3 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm. Acesso em: 14 de mar. de 2024.

4 Disponível em: <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protacao-dados-seguranca-persecucao-FINAL.pdf>. Acesso em: 14 de mar. de 2024.

5 Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274. Acesso em: 14 de mar. de 2024.

desses casos, em todas as operações de tratamento sob a responsabilidade dos citados entes estatais”⁶.

Respeitando-se os fundamentos estipulados pelo Projeto de Lei, dentre eles, o dever estatal de garantir a eficiência nas atividades de segurança por meio da instituição de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais (art. 2º, VI), nota-se um importante papel atribuído à pessoa ou ao órgão responsável pelo tratamento dos dados pessoais: o dever de distinguir os titulares dos dados em diferentes categorias – pessoas contra as quais existem indícios de que cometeram ou estão prestes a cometer uma infração ou atentado contra a segurança do Estado, pessoas processadas pela prática de ilícito penal, pessoas com condenação definitiva, vítimas ou potenciais vítimas ou, ainda, eventuais testemunhas que possam contribuir com a investigação (art. 5º, I a VI). A categorização acertadamente tenta impedir a obtenção indiscriminada de dados de pessoas que podem não ter qualquer vínculo com a investigação, tampouco possam contribuir para seu desenvolvimento.

Especificamente em relação ao acesso, tratamento e compartilhamento de dados pessoais e banco de dados controlados por pessoa jurídica de direito privado, o PL abre a possibilidade de que essas informações sejam disponibilizadas por requisição do delegado de polícia ou Ministério Público; por cooperação voluntária por parte do particular; por contrato ou acordo de cooperação; ou por canal técnico de inteligência do Estado (art. 18, I a IV). Isso quer dizer que o acesso a esses dados prescinde de autorização judicial. Contudo, como não poderia deixar de ser, demais informações pessoais que são sujeitas a sigilo legal ou constitucional seguirão dependendo de autorização judicial para seu acesso pelas autoridades competentes, nos termos do art. 19 da mesma lei e em sintonia com outros diplomas legais, como o próprio MCI ou com o art. 15 da Lei nº 12.850/2013 (Lei de Organizações Criminosas) e art. 58, § único, da Lei nº 12.037/2009 (Lei de Identificação Criminal).

A fim de garantir a implementação da LGPD-Penal à luz de garantias constitucionais, o art. 48 do PL ainda acrescenta à Agência Nacional de Proteção de Dados (ANPD), dentre outras, competências de zelar pela proteção de dados pessoais na segurança pública e do Estado, defesa nacional e na persecução penal (inciso I), além de aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação (inciso II).

Da breve análise sobre o Projeto de Lei, já é possível observar uma preocupação do legislador em fortalecer, para além do MCI, a regulamentação sobre o tratamento de dados na esfera criminal, pautada na proteção de direitos e garantias

6 *Ibidem.*

fundamentais de seus titulares, para que se possa alcançar segurança jurídica dos meios de investigação necessários frente às constantes inovações tecnológicas sem, com isso, vilipendiar o direito constitucional à privacidade dos dados e comunicações do usuário da rede.

Em que pese já proposto, o PL ainda aguarda a constituição de Comissão Especial para analisar a matéria, sendo indispensável que a comunidade jurídica e o Poder Público não percam de vista a importância do célere trâmite da medida para se combater a criminalidade virtual, que caminha a passos largos à frente das autoridades investigativas.

CONCLUSÕES

Conforme apontam os estudos desenvolvidos pelo Anuário Brasileiro de Segurança Pública, entre os anos de 2018 e 2022, os casos de fraude eletrônica (atualmente prevista no art. 171, §2º-A do Código Penal brasileiro) tiveram um crescimento vertiginoso de aproximadamente 320% no período, especialmente em razão da ampliação e intensificação do uso da internet para atividades no contexto da pandemia de Covid-19 e a constante inovação tecnológica a que estamos submetidos.

Nesse contexto, o MCI, que agora completa seu décimo aniversário, trouxe enorme avanço à identificação de autores de crimes virtuais ao contribuir para o acesso célere a dados cadastrais mais simples sem deixar, contudo, de proteger a privacidade do usuário da rede. Entretanto, é forçoso reconhecer que a persecução penal ainda enfrenta muitos desafios de ordem técnica e procedimental, que acabam por não acompanhar o volume e a velocidade dos golpes virtuais, dificultando a rápida solução dos casos.

Por esses motivos, a discussão responsável e representativa da LGPD-Penal se impõe como forma de fazer com que a investigação policial se desenrole em velocidade suficiente para alcançar os criminosos nos casos de delitos virtuais sem relativizar direitos constitucionalmente garantidos e tão bem tutelados pelo MCI.

REFERÊNCIAS

BRASIL, Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal.

BRASIL, Lei Federal nº 12.965/2014.

BRASIL, Lei Federal nº 13.709/2018.

BRASIL, Projeto de Lei nº 2.126/2011.

BRASIL, Projeto de Lei nº 1.515/2022.

LIMA, Renato Sérgio de; BUENO, Samira. As novas configurações dos crimes patrimoniais no Brasil. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública.

O COMPARTILHAMENTO DE DADOS NA DEMOCRATIZAÇÃO DO SETOR DE ENERGIA ELÉTRICA

Ana Carolina Katlauskas Calil

Luiza Sato

Desde sua criação, a eletricidade é uma das principais ferramentas para o desenvolvimento de novos processos e modelos produtivos pela humanidade. Nos últimos anos, é possível ainda observar que a eletrificação vem se tornando o principal objetivo de diversas economias mundiais (e não mais o meio para se alcançar determinados propósitos).

Com o emprego de novas tecnologias e novas aplicações em um cenário de democratização do setor elétrico, a indústria destravar-se-á, como já vem fazendo, iniciativas em matéria de serviços baseados na análise de dados, com o objetivo de apresentar soluções eficientes e sustentáveis para diferentes cadeias de produção. Em razão da quantidade de agentes envolvidos no mercado de energia elétrica, essa análise de dados pressupõe, necessariamente, uma intensificação do fluxo de informações entre diferentes participantes de mercado.

Nessa linha, o objetivo do presente artigo é compreender os movimentos de democratização sendo impostos ao mercado de energia elétrica brasileiro, com especial foco na iniciativa de “open energy”, que não poderia ser minimamente viável sem a existência de todo um arcabouço jurídico que permitisse a sua ampla e segura adoção. Considerando que, para possibilitar o “open energy”, é essencial que exista o compartilhamento de dados mediante tráfego via internet, não há dúvidas de que o Marco Civil da Internet (MCI) tenha sido absolutamente imprescindível para possibilitar o seu sucesso.

OS MOVIMENTOS REGULATÓRIOS VOLTADOS À DEMOCRATIZAÇÃO DO SETOR DE ENERGIA ELÉTRICA

No Brasil, hoje, a comercialização de energia elétrica pode ser realizada em três ambientes distintos, quais sejam: (i) o Ambiente de Contratação Regulada (ACR), no âmbito do qual concessionárias de distribuição de energia elétrica adquirem energia elétrica por meio de leilões conduzidos por autoridades governamentais para suprimento de seus consumidores cativos nos termos de contratos substancialmente regulados; (ii) o Ambiente de Contratação Livre (ACL), no qual compradores e vendedores de energia pactuam livremente os termos e condições associados à comercialização de energia elétrica entre as partes; e (iii) o Mercado de Curto Prazo (MCP), ou mercado spot, no qual são liquidadas financeiramente diferenças positivas e negativas de todas as transações de compra e venda de energia elétrica realizadas no país.

Especificamente com relação ao ACL, veja que, originalmente, a legislação estabelecia uma demanda mínima de 3 MW para que consumidores pudessem escolher livremente seus fornecedores e as condições de referido suprimento, sendo qualificados, nesse contexto, como consumidores “livres”.¹

Contudo, desde 2018, o Ministério de Minas e Energia (MME) vem estudando a possibilidade de expansão do Mercado Livre mediante a redução dos requerimentos aplicáveis à qualificação do consumidor “livre”. Isso porque, na visão do MME e observando outras experiências comparadas, a expansão de referido mercado poderia trazer algumas vantagens ao setor de energia brasileiro, como o aumento de competição em comercialização de energia e aumento de eficiência entre os consumidores, mais autonomia e melhor gestão de preferências e riscos por parte do consumidor, escolhas de provedores com base em fatores além do preço, como responsabilidade ambiental e qualidade de atendimento, incentivo à inovação etc.

Referidas análises resultaram na publicação da Portaria MME nº 50/2022, estipulando um cronograma para a abertura de mercado ou, explicando em detalhes, na escalonada redução dos requerimentos aplicáveis à qualificação de consumidores “livres”. Nos termos da Portaria MME nº 50/2022, desde o início de 2024, todo consumidor de energia elétrica atendido em alta tensão pode ser qualificado como consumidor “livre” e, nesse sentido, definir livremente seus fornecedores e os termos em que se darão os respectivos suprimentos. Uma vez analisados os resultados da expansão do Mercado Livre para alta tensão, espera-se que o mesmo caminho seja adotado para consumidores atendidos em baixa tensão.

¹ Conforme prevê o art. 15, § 2º, da Lei nº 9.074/1995.

Fato é que, após as movimentações regulatórias introduzidas pelo Governo Federal para a abertura do mercado, mais de 15.000 contratos atendidos no ACR foram denunciados para proporcionar a migração para o Mercado Livre.²

Além disso, de acordo com dados da Câmara de Comercialização de Energia Elétrica (CCEE), autoridade responsável pelo registro, contabilização e liquidação financeira de todas as operações de energia realizadas no país, hoje há mais de 10.000 consumidores livres e especiais registrados na câmara para participar em transações de compra e venda de energia³ e espera-se que referido número continue crescendo a partir da abertura integral de mercado possibilitada nesse ano de 2024, nos termos da regulamentação vigente.

E é justamente nesse cenário em que se insere o “open energy” – para viabilizar a completa liberdade da escolha do fornecedor de quem os consumidores comprarão energia, em um ambiente cada vez mais democratizado.

OPEN ENERGY E A RELAÇÃO COM O MCI

O MCI foi editado com o propósito de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, trazendo uma série de princípios e regras a respeito da economia digital e das atividades realizadas em ambiente online.

A urgência de uma norma dessa natureza ocorreu devido à extensa exploração da internet para a execução de atividades inovadoras. Para que as transações e comunicações no ambiente digital não se degradasse por conta de uma “terra sem lei”, sem respeito aos princípios democráticos e respeito à ordem jurídica, o MCI foi então promulgado, com um conteúdo fruto de contribuições da sociedade. Mediante a existência do marco legal, uma série de iniciativas puderam ser seguramente desenvolvidas e executadas pelos setores público e privado. Nesse sentido, não há dúvidas de que o MCI abriu caminhos para que hoje possamos discutir a implementação do “open energy” no país.

O “open energy” pode ser definido como o conjunto de iniciativas projetadas para possibilitar o compartilhamento de dados dos consumidores de energia entre os diferentes agentes do mercado por intermédio das chamadas *Application Programming Interfaces* (APIs). As APIs, por sua vez, correspondem a um conjunto de interfaces padronizadas, por meio das quais diferentes sistemas são integrados, permitindo, entre eles, a consulta, o compartilhamento e outras operações envolvendo dados.

2 De acordo com dados do Ministério de Minas e Energia.

3 Disponível em: <https://www.ccee.org.br/en/nossos-associados>. Acesso em: 4 de mar. de 2024

Vejam que o “open energy” em muito se assemelha ao já popularizado “open finance” implementado no setor financeiro. A partir do “open finance”, o sistema financeiro garantiu ao consumidor certo empoderamento para reger suas próprias escolhas, que é justamente o propósito do “open energy”.

Quanto ao empoderamento, o MCI já assegurava uma série de direitos aos usuários de internet, dentre eles, aquele previsto em seu art. 7º inciso VII, qual seja, o direito do usuário de internet de não fornecer a terceiros seus dados pessoais, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

A esse respeito, interessante levantar que o MCI não é mais hoje a norma a ser seguida quando abordamos o tratamento de dados pessoais, incluindo o consentimento do titular para tanto. O MCI jamais pretendeu esgotar ou ser a norma principal para regular o tratamento de dados pessoais. Em 2018, foi promulgada a Lei Geral de Proteção de Dados (LGPD), que passou a ser a norma a ser seguida para tal matéria, prevalecendo sobre as disposições contidas no MCI quanto ao tema.

Uma das questões primordiais que a LGPD tende a solucionar quando da estruturação do “open energy” diz respeito à base legal que justificará o compartilhamento dos dados entre agentes do setor elétrico. Caso seja usada a regulamentação “open finance” como inspiração, o compartilhamento apenas poderá ocorrer mediante consentimento, que inclusive conta com requisitos mais rígidos do que aqueles previstos pela própria LGPD. Caso haja uma interpretação mais ampla da LGPD, outras justificativas para o compartilhamento de dados poderão ser utilizadas, como execução de contrato, interesses legítimos ou execução de políticas públicas pela administração pública.

Outras obrigações previstas na LGPD também deverão ser observadas pelos agentes dentro do *open energy*: (i) o cumprimento do princípio da transparência, segundo o qual os consumidores deverão ser muito bem informados quanto às formas de tratamento de seus dados pessoais, incluindo as medidas de segurança e a possibilidade de compartilhamento de seus dados com terceiros; (ii) a implementação de medidas para atender titulares de dados no exercício de seus direitos; (iii) a manutenção de registro das operações de tratamento de dados pessoais que realizarem; (iv) a adoção de política de retenção e eliminação de dados pessoais; (v) a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) – órgão responsável por implementar e fiscalizar o cumprimento da LGPD – e aos titulares sobre a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares; e (vi) a indicação de encarregado pelo tratamento de dados pessoais, que será o canal com os titulares de dados e a ANPD, com a

responsabilidade de orientar os colaboradores da empresa quanto às melhores práticas para garantir a proteção de dados pessoais⁴.

Ainda, o art. 13 do regulamento do MCI, o Decreto nº 8.771/2016, estabeleceu importantes padrões de segurança da informação a serem seguidos por provedores de serviço da internet⁵. Tais diretrizes serviram de base e estão em consonância com aquelas trazidas pela Resolução Normativa nº 964 da Agência Nacional de Energia Elétrica (ANEEL), que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor. Na resolução, a ANEEL estabelece as diretrizes de cibersegurança a serem seguidas, como a transparência, a adoção de boas práticas de segurança da informação e a gestão de incidentes de segurança. É obrigatório que os agentes adotem e periodicamente revisem sua Política de Segurança Cibernética, que deve ser disponibilizada à ANEEL. Ainda, o Operador Nacional do Sistema Elétrico (ONS) publicou o Manual de Procedimentos de Operação nº RO-CB.BR.01, estabelecendo a rotina operacional envolvendo segurança cibernética no setor elétrico.

CONCLUSÕES PRELIMINARES: DESAFIOS E OPORTUNIDADES PARA OS PRÓXIMOS ANOS

Feitas as considerações, hoje, é possível verificar que o setor elétrico brasileiro caminha por um processo de democratização a partir da abertura de mercado, que, por sua vez, possibilita o aumento do número de agentes setoriais e, paralelamente, a intensificação do fluxo de informações e dados provenientes ou associados a referidos participantes/entrantes.

Observada a recém implantada abertura integral do ACL, é evidente que o “open energy” poderá trazer uma série de benefícios para a economia de energia

4 CALIL, Ana Carolina K; SATO, Luiza. A proteção de dados na era do open energy. Disponível em: <https://megawhat.energy/noticias/opiniao-da-comunidade-2/147672/ana-carolina-calil-e-luiza-sato-escrevem-protexcao-de-dados-na-era-do-open-energy>. Acesso em: 8 de mar. 2024.

5 Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e

IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como criptografia ou medidas de proteção equivalentes.

no Brasil. A título exemplificativo, os consumidores poderão receber de agentes setoriais diferentes (distribuidoras, comercializadoras/geradores e até mesmo empresas de soluções) ofertas baseadas em seu perfil de consumo, receber incentivos para reduzir o consumo em determinados períodos ou até mesmo ter acesso a produtos inovadores ainda não praticados no setor. Por um lado, os agentes setoriais se preocuparão em oferecer propostas competitivas e inovadoras aos seus clientes ao passo que a população ficará mais atenta ao seu consumo de energia e avaliará possibilidades de economia e empoderamento sobre suas ações.

Ainda, o compartilhamento e a análise de dados no setor de energia nunca foi tão relevante, possibilitando a prevenção de falhas na linha de transmissão, a previsão sobre momento da manutenção, a detecção de perdas técnicas e não técnicas (*e.g.*, furtos de energia), a melhoria na eficiência do consumo, diminuição de custos e segmentação de consumidores para melhor oferta de produtos e serviços⁶.

Contudo, um dos maiores desafios dos agentes do setor para a implementação do “open energy” em um mercado democratizado, nos termos expostos acima, diz respeito ao tratamento seguro de dados diante um fluxo intenso de informações. Desse modo, considerando a relevância da proteção de dados dentro da discussão do “open energy”, espera-se que a ANPD coordene ações com autoridades do setor elétrico para a regulamentação detalhada do tema, tal como já ocorre em outras esferas regulatórias como a concorrencial.

Além disso, outra questão a ser solucionada faz referência à base legal que justificará o compartilhamento dos dados entre agentes do setor elétrico – discussão essa que já ocorreu no contexto do mercado financeiro e do “open banking”.

De todo modo, uma vez definidas as diretrizes regulatórias envolvendo o “open energy”, a exploração de dados e informações possibilitando o protagonismo do consumidor em suas escolhas tende a tornar o mercado mais eficiente e competitivo, tal como esperado pelo Governo Federal quando do início do processo de abertura de mercado.

O MCI criou um campo digital regulado que possibilitou iniciativas baseadas no tráfego de dados via internet. A interconexão entre o “open energy” e o MCI destaca a importância de se promover um ambiente digital seguro, transparente e inovador para os consumidores que negociarão a aquisição de sua energia elétrica via internet. Tais iniciativas são grandes exemplos da positiva exploração do ambiente digital, com inúmeros benefícios para os consumidores de energia e para o desenvolvimento da infraestrutura do país.

6 SATO, Luiza. LGPD Aplicada ao Setor de Energia. In LIMA, Ana Paula M. C. de; CRESPO, Marcelo; PECK, Patricia (coord.). LGPD Aplicada. São Paulo: Ed. Atlas, 2022.

Capítulo 3

/Setores e Aplicações Específicas do Marco Civil da Internet

DIREITOS AUTORAIS E CONEXOS E O MARCO CIVIL DA INTERNET

Carla do Couto Hellu Battilana
Sofia Kilmar
Stephanie Consonni de Schryver
Marina Sayuri Kitayama

INTRODUÇÃO

Ao introduzir o tema sobre direitos autorais e sua proteção à luz do Marco Civil da Internet (MCI), o legislador foi expresso e determinou, ao dispor sobre a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, que a proteção aos direitos autorais nesse âmbito seria regulamentada por lei específica¹, a qual deverá respeitar a liberdade de expressão e a Constituição Federal.

Ainda, de forma que não restasse qualquer dúvida a este respeito, essa condição é reiterada pelo legislador na forma do artigo 31², o qual prevê que até a entrada em vigor dessa lei específica, quando se tratar de infração a direitos de autor ou a direitos conexos, a responsabilidade do provedor por danos decorrentes de conteúdos produzidos por terceiros, continuará a ser disciplinada pela legislação autoral vigente.

Anos se passaram e ainda não existe uma lei específica que verse sobre essa responsabilidade do ponto de vista de direitos autorais e conexos.

1 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. (...)

§ 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.

2 Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Quando voltamos à época em que o MCI estava sendo discutido, verificamos que o racional trazido no Projeto de Lei (PL) nº 2.616, de 2011 – de autoria do Executivo, com relatório final do deputado Alessandro Molon, em 25 de março de 2014 –, foi no sentido de que (i) o anteprojeto do MCI já representava um primeiro pontapé importante sob a perspectiva normativa quanto aos direitos e deveres para o uso da internet no Brasil, mas que alguns temas – como os direitos autorais – careceriam de proposta legislativa específica; e (ii) à época, havia um anteprojeto de lei que já estava em estudo para alteração da atual Lei de Direitos Autorais (LDA) nº 9.610, de 19 de fevereiro de 1998. Enquanto esse, ou qualquer outro projeto que tratasse sobre a regulamentação dos direitos autorais no ambiente cibernético, não fosse aprovado, tal regulamentação ficaria à cargo da LDA.

Mesmo após 10 anos da entrada em vigor do MCI, a LDA continua vigente e as discussões sobre uma possível alteração dessa lei continuam acaloradas. Afinal, a evolução da tecnologia e da internet trouxeram novos desafios e novas discussões. Por exemplo, a discussão sobre como será feita a remuneração de artistas por meio de plataformas digitais, o debate sobre se cabe remuneração a autores em decorrência do uso de suas obras intelectuais para treinamento de ferramentas de inteligência artificial (IA), bem como a discussão sobre se cabe responsabilidade civil a essas ferramentas, dentre muitas outras discussões.

Mesmo sem uma legislação específica sobre o tema até hoje, como previa o MCI, e mesmo com algumas lacunas (as quais precisam ser endereçadas pelo legislador), a LDA – aliada à outras leis – continua a ser aplicada para a proteção dos direitos autorais e conexos no Brasil³.

A LACUNA DO §2º DO ART. 19 DO MARCO CIVIL DA INTERNET

Como mencionado na seção introdutória deste artigo, desde que sancionado o Marco Civil da Internet (Lei nº 12.965/2014), aguarda-se a criação da legislação específica referente ao art. 19, parágrafo 2º, do referido diploma. Tal legislação estabeleceria diretrizes sobre a responsabilidade civil nos casos de divulgação de conteúdos que violem direitos autorais nas plataformas digitais. No entanto, transcorridos 10 anos, essa legislação ainda não foi criada, frustrando as expectativas de uma regulamentação clara do assunto. Com isso, também surgiram

3 Direitos de autor estão relacionados à proteção dos direitos dos autores de obras intelectuais expressas por qualquer meio ou fixadas em qualquer suporte, e os direitos conexos estão relacionados aos direitos dos intérpretes ou executantes, dos produtores fonográficos e das empresas de radiodifusão.

preocupações de que a ausência da lei resultaria em um ambiente digital desregulado no que concerne à disseminação de conteúdos que violam direitos autorais na internet.

Na prática, contudo, o cenário se desenvolveu de maneira diferente. Ao longo dos anos, observou-se que os titulares de direitos autorais e conexos seguem defendendo os seus direitos com base na própria LDA, nos direitos fundamentais trazidos pela Constituição Federal e em direitos previstos no Código Civil. Simultaneamente, observou-se um movimento por parte das próprias plataformas digitais para criar mecanismos de proteção dos direitos autorais e de marca em seus serviços. Assim, verificou-se uma superação da lacuna deixada pelo MCI.

Seguramente, a promulgação do MCI foi de relevância ímpar no estabelecimento de diretrizes fundamentais na internet, como a garantia da liberdade de expressão e da neutralidade de rede, representando também um avanço essencial para a segurança jurídica no ambiente online. Determinadas matérias, como visto, tiveram sua regulamentação deixada a cargo de regramentos específicos a serem criados. Exemplo que se destaca nesse sentido é a responsabilidade por conteúdos publicados nas plataformas digitais que infrinjam direitos autorais, considerando-se que o parágrafo 2º do art. 19 do MCI estipula que o regime de responsabilidade instituído pelo caput do próprio dispositivo dependerá de legislação específica⁴.

O art. 19 do MCI prevê como regra geral⁵ que os provedores de internet somente serão responsabilizados por conteúdos publicados por terceiros em suas plataformas caso descumpram ordem judicial específica de remoção do conteúdo – por ordem judicial específica, o Superior Tribunal de Justiça (STJ) entende a ordem que indique a *Uniform Resource Locator* (URL) do conteúdo específico que se determina a remoção⁶. Com isso, o objetivo da lei foi conciliar o exercício da liberdade de

4 “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. (...)”

§ 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.” (grifos nossos).

5 A exceção está prevista no art. 21 do Marco Civil da Internet, que prevê que “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”.

6 A título exemplificativo, alguns acórdãos recentes nesse sentido: AgInt no AREsp nº 2.314.086/RS, julgado pela Quarta Turma do STJ em 18 de set. de 2023, relator ministro Raul Araújo; REsp nº 1.763.517/SP, julgado pela Quarta Turma do STJ em 5 de set. de 2023, relator ministro João Otávio de Noronha; AgInt nos EDcl no AgInt no REsp nº 1.862.739/RJ, julgado pela Quarta Turma do STJ em 12 de junho de 2023, relatora ministra Maria Isabel Gallotti.

expressão com a proteção daqueles prejudicados por conteúdos lesivos, provendo mecanismos para identificar os responsáveis e remover o material ofensivo. A norma promove, assim, um

equilíbrio no exercício de direitos, na medida em que retira do provedor a pressão de remover todo e qualquer conteúdo apontado como ilícito, o que atingiria em cheio a liberdade de expressão na rede, mas não o impede de assim proceder caso entenda que o material questionado é realmente contrário aos termos de uso e demais políticas que regem o funcionamento da plataforma.⁷

Não obstante o regime geral instituído pelo art. 19, de acordo com a previsão de seu parágrafo 2º, as diretrizes aplicáveis no que concerne às violações de direitos autorais dependeriam de uma previsão legal específica. Da mesma forma, o art. 30 estipula que

até a entrada em vigor da lei específica prevista no parágrafo 2º do artigo 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, **continuará a ser disciplinada pela legislação autoral vigente** aplicável na data da entrada em vigor desta Lei (grifos nossos).

A Lei de Direitos Autorais (Lei nº 9.610/1998) em vigor não trata da responsabilidade por conteúdos veiculados nas plataformas digitais que violem os termos da referida legislação. Na época da promulgação do MCI esperava-se que esse debate ocorresse em futuro próximo, uma vez que, estava sendo discutida uma reforma na legislação de direitos autorais no Brasil. No entanto, essa reforma não aconteceu, e o país ficou sem uma previsão legal específica para a responsabilização em casos de violação de direitos autorais por terceiros. Essa lacuna legislativa poderia sugerir que o ambiente online se encontra em um cenário de desproteção dos direitos autorais. No entanto, na prática, não é isso que se verifica.

De início, sob a perspectiva dos titulares de direitos autorais e conexos, cumpre esclarecer que a LDA prevê, em seu art. 29⁸, que depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades. O MCI foi, sem dúvida, um grande e importante avanço para a regulamentação da internet,

7 SOUZA, Carlos Afonso; LEMOS, Ronaldo; BOTTINO, Celina. Marco Civil da Internet. Jurisprudência comentada. São Paulo: Thomson Reuters. Revista dos Tribunais, 2017.

8 Art. 29. *Depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades, tais como: (...)*

mas os direitos autorais nunca ficaram desamparados, ainda que o MCI não tenha tratado especificamente de sua proteção.

Nesse sentido, vale destacar que a proteção de obras autorais independe de registro, porém esse é recomendado para fins de produção de provas contra terceiros, facilitando a tomada de medidas extrajudiciais e judiciais. Hoje vemos que os titulares de direitos de autor têm inúmeros desafios para proteger suas criações na internet, porém também temos diversas ferramentas que os auxiliam neste sentido.

Assim, é importante que titulares de direitos autorais e conexos tenham uma postura proativa em relação a proteção dos seus direitos no universo cibernético e tome todas as medidas que estão em seu poder para isso, por exemplo, buscar o registro de suas obras nos órgãos competentes (como na Fundação Biblioteca Nacional, em caso de obras literárias, e na Escola da Música da Universidade Federal do Rio de Janeiro – UFRJ –, no caso de músicas); registrar seus direitos autorais em blockchain; utilizar ferramentas de IA para monitorar eventuais infrações na internet; cadastrar suas criações intelectuais em plataformas de marketplace que oferecem programas de proteção à direitos de propriedade intelectual e autoral; entre outros.

Nesse sentido, diversas plataformas de marketplace optaram por oferecer esses programas pelos quais os titulares podem denunciar eventuais infrações, como forma de tentar coibir a pirataria nesse meio digital, mostrando aos titulares que as plataformas também reprimem esse tipo de conduta e se importam com a preservação desses direitos. Também vemos provedores de aplicações de internet tomando medidas para coibir a violação de direitos autorais e intelectuais, como no caso da adoção de políticas e termos de uso que contém disposições específicas a respeito de violação de direitos de autoral, além de oferecerem ferramentas de denúncias aos próprios usuários e titulares. Os provedores de aplicações de internet trabalham de forma muito ativa na proteção tais direitos autorais e conexos.

ATUAÇÃO DAS PLATAFORMAS

Em que pese a ausência da legislação específica mencionada no art. 19, parágrafo 2º, do MCI, pudesse sugerir, à primeira vista, haver um incentivo para que conteúdos violadores de direitos autorais se propagassem pelas plataformas digitais, não foi isso que se verificou na prática. A atuação ativa de titulares, aliada à ação dos próprios provedores de aplicação, tiveram como resultado ativa proteção de direitos autorais e conexos no ambiente digital.

Nessa linha, verifica-se que todas as seis principais plataformas de rede social atuantes no Brasil segundo a revista Forbes⁹ – YouTube, Facebook, Instagram, TikTok, Kwai e X – possuem políticas específicas e oferecem canais de denúncia para violações de direitos autorais.¹⁰

Exemplificativamente, no caso do Facebook e do Instagram, serviços fornecidos pela empresa Meta, as políticas proíbem expressamente a publicação de conteúdos que violem os direitos de propriedade intelectual de terceiros, incluindo direitos autorais e de marcas comerciais. Os detentores de tais direitos têm à disposição diversas ferramentas para protegê-los, incluindo mecanismos de denúncia e tecnologias de gerenciamento de conteúdos protegidos.¹¹

As plataformas também se preocupam em garantir que os usuários tenham a oportunidade não só de denunciar como também de contestar denúncias de violação de direitos autorais. O TikTok, por exemplo, permite que os usuários entrem em contato diretamente com o titular dos direitos autorais para solicitar uma retratação, se considerarem que uma notificação de violação está equivocada. Além disso, o provedor também oferece um formulário de resposta à notificação para que os usuários possam apresentar suas defesas.¹²

Os números confirmam que as regras de proteção aos direitos autorais são efetivamente aplicadas. Segundo o Relatório de Transparência da Meta de 2022, naquele ano foram removidos 4.483.700 conteúdos das plataformas Facebook e Instagram com base em denúncias de violação de direitos autorais, além de 6.631.600 conteúdos indisponibilizados proativamente pela mesma violação. De acordo com o Relatório de Transparência do TikTok, apenas no período

9 Disponível em: <<https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>>. Acesso em: 23 de fev. de 2024.

10 Veja-se as previsões específicas constantes nas políticas de cada uma das plataformas mencionadas:

Youtube: <https://support.google.com/youtube/answer/2807622?hl=pt-BR>

Facebook: https://www.facebook.com/help/intellectual_property?ref=tos

Instagram: https://help.instagram.com/535503073130320?ref=igtos&helpref=faq_content

TikTok: <https://www.tiktok.com/legal/page/global/copyright-policy/pt-BR>

Kwai: https://www.kwai.com/legal?id=copyright_policy

X (antigo Twitter): <https://help.twitter.com/pt/rules-and-policies/copyright-policy#:~:text=O%20Twitter%20responde%20a%20den%C3%BAncias,hospedagem%20de%20m%C3%ADdia%20ou%2C%20ainda%2C>

11 Disponível em: <<https://www.meta.com/pt-br/help/policies/meta-policies/meta-copyright/>>. Acesso em: 23 de fev. de 2024.

12 Disponível em: <https://support.tiktok.com/pt_BR/safety-hc/account-and-user-safety/copyright>. Acesso em: 23 de fev. de 2024.

compreendido entre janeiro e junho de 2023¹³, foram formuladas 189.564 solicitações de remoção de conteúdos infratores de direitos autorais, sendo 113.41 bem-sucedidas.

A atuação das plataformas na defesa de um ambiente online harmônico, incluindo o que diz respeito à proteção de direitos autorais, faz todo o sentido não só do ponto de vista jurídico, mas também do ponto de vista comercial das empresas, que, com isso, oferecem um serviço melhor e mais competitivo aos usuários.

CONCLUSÃO

A matéria dos direitos autorais e conexos no contexto da internet é de suma importância. Por isso, justificou-se o temor de que a lacuna deixada pelo parágrafo 2º do art. 19 do MCI poderia levar a um cenário de desproteção dos direitos autorais no âmbito online. No entanto, o que se observou na prática foi o exato oposto. Os titulares de direitos autorais e conexos são ativos para protegê-los. Além disso, todas as principais redes sociais possuem regulamentos específicos que não apenas proíbem a veiculação de conteúdos que violem direitos autorais, mas também oferecem mecanismos de denúncia e outras ferramentas para proteger esses direitos. Funciona, assim, a atuação das próprias plataformas como meio de superação da lacuna deixada pelo MCI sobre a matéria.

13 Disponível em: <<https://www.tiktok.com/transparency/pt-br/intellectual-property-removal-requests-2023-1/>>. Acesso em: 23 de fev. de 2024.

MARCO CIVIL DA INTERNET E ELEIÇÕES: DESAFIOS E PERSPECTIVAS PARA O FUTURO

Bruna Borghi Tomé
Bruno Sá de Andrade

INTRODUÇÃO

Embora o Brasil seja considerado uma Democracia jovem e nosso país tenha passado por diversos períodos de relativização ou mesmo supressão completa do Estado Democrático de Direito, o Direito Eleitoral é um ramo tradicionalíssimo do direito brasileiro, que remonta ao período colonial.

Com o desenvolvimento de novas realidades e tipo de interação sociais naturais do passar do tempo, o Direito Eleitoral passou a se relacionar intrinsecamente com outras áreas do direito, muitas vezes fazendo intersecções com microssistemas jurídicos – é justamente o caso do Direito Digital e do microssistema trazido pelo Marco Civil da Internet (MCI).

Este trecho da presente obra pretende analisar alguns aspectos dessa dinâmica, bem como delinear brevemente os desafios e impactos que já puderam ser observados por conta dessa interação, bem como as perspectivas para o futuro no que tange a esse tema.

EVOLUÇÃO TECNOLÓGICA E DAS DISCUSSÕES SOBRE DIREITO DIGITAL NO VIÉS ELEITORAL

Como já adiantado, as raízes do Direito Eleitoral podem ser rastreadas até praticamente ao descobrimento. Ainda no período colonial ocorreram as primeiras eleições brasileiras de que se tem notícia, a saber: em 1532, para formação do Conselho Municipal da Vila de São Vicente, São Paulo; e, já no período imperial, no ano de 1822 foi positivada a primeira lei eleitoral brasileira, para formação

da Assembleia Geral Constituinte e Legislativa que elaborou a Constituição do Império de 1824.

Já na primeira metade do século XX, inaugurou-se a chamada fase moderna do Direito Eleitoral, com a promulgação do Decreto nº 21.076/1932 (Código Eleitoral de 1932), mesma oportunidade em que foi criada a Justiça Eleitoral e em que se pavimentou o caminho para a promulgação das Leis nº 4.737/1965 (Código Eleitoral) e nº 9.504/1997 (Lei das Eleições), que são dois dos principais pilares normativos do Direito Eleitoral.

Mesmo sendo um dos mais antigos ramos do direito nacional, esse foi um dos que melhor se adequou às mudanças sociais e à evolução tecnológica observadas na sociedade – muito em razão da dinamicidade do processo eleitoral (a média de duração de um processo eleitoral é de um ano e um mês) e da atuação da Justiça Eleitoral, como se verá mais à frente.

É possível definir um ponto-chave para a intersecção entre o MCI e o Direito Eleitoral: (i) a expansão do debate político – que deixou de se restringir às mesas de bar e aos círculos familiares – para um ambiente digital de alcance praticamente ilimitado; e (ii) a adaptação dos agentes políticos à essa nova realidade de modo que cada vez mais adequaram suas estratégias de campanha para esse novo ambiente (em 2022, 42% do orçamento das campanhas foi direcionado para o ambiente digital, podendo ultrapassar os 50% em 2024).

Isso pode ser demonstrado pelo aumento no número de processos na Justiça Eleitoral envolvendo provedores de aplicações de internet (especialmente aqueles responsáveis por serviços de redes sociais) a partir de 2012, com significativa intensificação entre 2016 e 2020.

Também houve diversificação dos temas tratados nesses processos: em 2012, as principais demandas resumiam-se, em maioria, à remoção de conteúdo irregular e identificação de usuários; a partir de 2018, passaram a abordar temas mais complexos, como averiguações acerca do uso de *bots* para gerar interações inautênticas nas redes sociais e do uso de inteligência artificial (IA) para disseminação de informações consideradas falsas.

A JUSTIÇA ELEITORAL COMO ENTE NORMATIZADOR: RESOLUÇÕES DO TSE QUE ACELERARAM O ALINHAMENTO ENTRE O REGRAMENTO ELEITORAL E O MCI

O Direito Eleitoral tende a acompanhar de forma mais célere as mudanças de realidade que, naturalmente, ocorrem em nossa sociedade com o passar do tempo. Muito disso se dá porque, diferentemente de outros ramos do Poder Judiciário, a Justiça Eleitoral tem maior espaço para o exercício de sua função normativo-regulamentar, exercida por meio da expedição de Resoluções, pelo Tribunal Superior Eleitoral (TSE), conforme preveem os arts. 23, IX e 105 da Lei nº 9.504/1997.

Em síntese, essas Resoluções têm três funções principais: (i) regulamentar a legislação eleitoral, traduzindo as leis eleitorais em normas práticas e aplicáveis, definindo prazos, requisitos e procedimentos específicos para cada etapa do processo eleitoral; (ii) fornecer uniformidade e previsibilidade para todos os envolvidos nas eleições, como partidos políticos, candidatos e até mesmo terceiros que, a princípio, não têm conexão direta com o processo eleitoral, como é o caso dos provedores de aplicações da internet; e (iii) adaptar as regras eleitorais à realidade social e tecnológica.

O texto dessas Resoluções é definido pelo TSE, com participação da sociedade civil por meio da apresentação de contribuições para sua redação que possam aprimorar o processo eleitoral, bem como por meio de debates em audiência pública. Trata-se de um procedimento muito mais simplificado e, portanto, célere, que o processo legislativo ordinário. Nosso escritório, TozziniFreire Advogados, tem submetido contribuições nesse sentido desde 2016, com o acolhimento de diversas sugestões relevantes do ponto de vista contencioso e até mesmo material.

É justamente por conta da conjunção desses dois fatores (participação da sociedade e procedimento simplificado para elaboração e aprovação das Resoluções) que a interação entre a matéria regulada no MCI e o microsistema jurídico eleitoral pode ser mais bem observada nas mencionadas Resoluções do que nas próprias leis eleitorais (como o Código Eleitoral e a Lei das Eleições).

A título de exemplo dessa integração, em 2017 foi expedida a Resolução TSE nº 23.551, destinada à regulação da propaganda eleitoral, e na qual foi consignado que “a ordem judicial que determinar a remoção de conteúdo divulgado na internet (...) deverá conter, sob pena de nulidade, a URL do conteúdo específico”¹. Trata-se de evidente homenagem ao texto do art. 19, §1º do MCI e à interpretação

1 Art. 33, §3º da Resolução TSE nº 23.551/2017 (revogado).

pacífica do Superior Tribunal de Justiça (STJ)² de que “a identificação clara e específica” de um conteúdo na internet deverá se dar por meio da indicação de sua URL.

Embora a Resolução TSE nº 23.551/2017 tenha sido revogada, previsão semelhante foi trazida no art. 38, §4º da Resolução TSE nº 23.610/2019, atualmente vigente e aplicável às eleições de 2024. Há, além disso, outras seis menções expressas ao MCI como fundamento de disposições na mencionada Resolução:

art. 7º, §1º – vedação ao exercício do poder de polícia pelos magistrados eleitorais quando irregularidade constatada na internet se referir ao teor da propaganda, devendo ser observado o art. 19 do MCI;

art. 32 – previsão da aplicação das penalidades previstas na Resolução ao provedor de aplicações de internet, caso não atenda à ordem judicial que determinar providências para a cessação da divulgação de propaganda irregular;

art. 39 – definição dos dados de identificação de usuários que os provedores de aplicações de internet devem fornecer;

art. 40 – previsão de que a parte interessada poderá requerer, a fim de formar conjunto probatório em processo judicial, requerer ao juízo eleitoral que ordene à(ao) responsável pela guarda o fornecimento dos dados constantes do art. 39;

art. 40, §1º – previsão dos requisitos que devem constar no requerimento mencionado pelo *caput* do artigo; e

art. 40, §1º, IV – previsão quanto à necessidade de que no requerimento mencionado pelo *caput* do artigo conste a identificação do endereço da postagem ou conta em questão (URL ou, caso inexistente, URI ou URN), observados, nos termos do art. 19 do MCI, o âmbito e os limites técnicos de cada provedor de aplicação de internet.

Na mesma linha, observa-se que o MCI é expressamente referenciado: (i) duas vezes na Resolução TSE nº 23.608/2019, dedicada à regulação de representações, reclamações e pedidos de direito de resposta previstos na Lei das Eleições para as eleições (arts. 17, §1-A e 32, §5º, que estabelecem a indicação da URL do conteúdo irregular como requisito da petição inicial que objetive a sua remoção da internet, bem como da ordem que determinar a remoção de conteúdo em sede de direito de resposta); e (ii) uma vez na Resolução TSE nº 23.650/2021, que instituiu a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral (art. 3º, parágrafo único, que referencia aos princípios da proteção da intimidade e da vida privada da pessoa natural trazidos no MCI).

2 De acordo com levantamento feito por TozziniFreire Advogados, entre 2011 e junho de 2023, foram proferidos 42 acórdãos e 144 decisões pelo STJ.

Não se observam, por outro lado, situações semelhantes no Código Eleitoral ou na Lei das Eleições, o que evidencia que o MCI se integrou de forma mais rápida – e muito bem-sucedida – ao Direito Eleitoral muito por conta da atuação do TSE e da sociedade civil, bem como do bom uso das Resoluções para os fins de adequar esse microssistema à realidade contemporânea de nossa sociedade.

O FUTURO DO DIREITO ELEITORAL DIGITAL

Em março de 2024 foi aprovada a Resolução TSE nº 23.732 que trouxe diversas alterações à Resolução TSE nº 23.610/2024. No que importa ao MCI, embora continue sendo mencionado em algumas passagens, houve alteração no tocante à atuação dos provedores de aplicações de internet. Os arts. 9º-D e 9º-E trouxeram novidades acerca do dever de cuidado e atuação imediata em determinadas hipóteses independentemente de ordem judicial.

O texto normativo foi inclusive além, trazendo disposições sobre novas tecnologias que não estão expressamente previstas no MCI, como IA, chatbots e ferramentas de lives. Entre elas:

o responsável por conteúdo produzido por IA (exceto para os casos de mera melhoria da estética do conteúdo), deverá providenciar disclaimer que exponha claramente essa circunstância (art. 9º-B). Há, entretanto, hipóteses para as quais o uso de inteligência artificial fica integralmente proibido em função de sua natureza, tais como (i) utilização da propaganda eleitoral de conteúdo que possa consistir na difusão de fatos notoriamente inverídicos ou descontextualizados, com potencial de causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral; (ii) conteúdo para favorecer ou prejudicar candidatura que se utilize de imagem ou voz de pessoa viva, falecida ou fictícia (*deep fake*) (art. 9º-C, caput, e §1º); o uso de *chatbots* se submete às regras para conteúdo produzido por meio de IA, com a observação adicional de que é vedada simulação de interlocução direta com o próprio candidato ou outra pessoa real (art. 9º-B, §3º); as lives eleitorais serão permitidas, salvo se transmitidas em site, perfil ou canal de internet pertencente à pessoa jurídica que não das pessoas políticas envolvidas (candidato, partido, coligação e federação) ou em emissora de rádio e televisão.

Parte das matérias listadas acima sequer foi ponto de discussão nas eleições municipais anteriores (vide o caso do chamado *deep fake*), mas ganharam importância significativa nesse intervalo, podendo ter consequências diretas no desfecho das eleições, tais quais as *fake news* (nesse sentido, o ex-ministro do TSE Luiz Fux, em evento realizado entre o TSE e a União Europeia, já afirmou

que Justiça Eleitoral pode eventualmente anular o resultado de uma eleição se esse resultado for decorrência da difusão massiva de *fake news*).

Nota-se que o TSE vem agindo, por meio das Resoluções para coibir práticas irregulares, especialmente em hipóteses em que ainda não há um marco legislativo próprio, como é o caso da IA e outros que, por vezes, podem acabar permeando a matéria já tratada pelo MCI.

Conclui-se que, mesmo em se tratando de tecnologias ainda não reguladas diretamente ou que sequer existam no momento, é impossível que se ignore a importância do MCI – marco pioneiro na regulação da tecnologia no Brasil – para fins de sedimentar as Resoluções eleitorais passadas e servir como elemento norteador para as vindouras.

CONCLUSÕES

Diante da já estabelecida realidade do debate político online e do dinamismo do ambiente eleitoral (que tem se mostrado cada vez mais fluído e mais inclinado a abarcar de forma rápida as mudanças tecnológicas), o TSE tem exercido importante papel regulador das normas de Direito Eleitoral, também quanto a temas afetos ao MCI – como visto, suas disposições, inclusive, serviram de base legal e mesmo de inspiração textual para diversos dispositivos constantes das resoluções eleitorais.

Embora essa atuação seja essencial para a garantia do processo eleitoral e do Estado Democrático de Direito, mostra-se imprescindível, também, que o debate sobre as matérias que situam na intersecção entre o Direito Eleitoral e o Direito Digital sejam objeto de amplo, profundo e permanente debate para que a tecnologia possa ser utilizada de forma responsável, mas sem que a respectiva regulação entre em conflito com as premissas já consagradas pela Constituição Federal e pelo MCI.

REFERÊNCIAS

BRASIL. Lei 4.737, de 15 de julho de 1965. Disponível em: <https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965>. Acesso em 08 de mar de 2024. Acesso em: 8 de mar. de 2024

Lei 9.504, de 30 de setembro de 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19504.htm. Acesso em: 8 de mar. de 2024.

CNJ. Justiça em números 2023. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2024/02/justica-em-numeros-2023-16022024.pdf>. Acesso em: 8 de mar. de 2024.

G1 Globo. Fux diz que Justiça pode anular uma eleição se resultado for influenciado por ‘fake news’ em massa. Disponível em: <https://g1.globo.com/politica/eleicoes/2018/noticia/fux-diz-que-justica-pode-anular-eleicao-se-resultado-for-fruto-de-fake-news-em-massa.ghtml>. Acesso em: 8 de mar. de 2024.

Revista Veja. O impacto da inteligência artificial nas eleições de 2024. Disponível em: <https://veja.abril.com.br/coluna/matheus-leitao/o-impacto-da-inteligencia-artificial-eleicoes-de-2024>. Acesso em: 8 de mar. de 2024.

Senado Federal. Comissão de juristas vai atualizar Código Civil para revolução digital. Disponível em: <https://www12.senado.leg.br/noticias/materias/2023/08/24/comissao-de-juristas-vai-atualizar-codigo-civil-para-revolucao-digital>. Acesso em: 8 de mar. de 2024.

TRE-SC. Histórico. Disponível em: <https://apps.tre-sc.jus.br/site/institucional/justica-eleitoral/historico/index.html>. Acesso em: 8 de mar. de 2024.

TRE-SP. Centro de Memória Eleitoral. Disponível em: <https://www.tre-sp.jus.br/institucional/centro-de-memoria-eleitoral/centro-de-memoria-eleitoral>. Acesso em: 8 de mar. de 2024.

TSE. Resolução TSE 23.610/2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em 08/03/2024. Acesso em: 8 de mar. de 2024.

Resolução TSE 23.608/2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-608-de-18-de-dezembro-de-2019>. Acesso em 08 de mar. de 2024. Acesso em: 8 de mar. de 2024.

Resolução TSE 23.551/2017. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2017/resolucao-no-23-551-de-18-de-dezembro-de-2017>. Acesso em: 8 de mar. de 2024.

Justiça Eleitoral e educação para a cidadania. Disponível em: <https://www.tse.jus.br/institucional/escola-judiciaria-eleitoral/publicacoes/revistas-da-eje/artigos/revista-eletronica-ano-ii-no-5/justica-eleitoral-e-educacao-para-a-cidadania>. Acesso em: 8 de mar. de 2024.

DIREITOS HUMANOS E INTERNET: PROMOÇÃO OU VIOLAÇÃO?

Clara Pacce P. Serva
Helena Rocha Matos

INTRODUÇÃO

Em 2023, dados do módulo de Tecnologia da Informação e Comunicação (TIC) da Pesquisa Nacional por Amostra de Domicílios (PNAD) Contínua do Instituto Brasileiro de Geografia e Estatística (IBGE)¹, revelaram que 161,6 milhões de pessoas estão conectadas.

O Brasil ocupa o segundo lugar no ranking de tempo diário utilizando a internet, atrás apenas da África do Sul². Enquanto a média mundial é de 6h40min por dia, os brasileiros passam em média 9h13min online.³ Os telefones celulares lideram: 98,9% da população com 10 anos ou mais de idade utiliza o telefone celular para acessar internet no país. Além disso, o Brasil conta com 152,4 milhões de pessoas usuárias de redes sociais⁴.

Nesse cenário, é fundamental compreender as características das interações que se estabeleceram com o acesso cada vez mais difuso⁵ da internet e de que modo

1 Pesquisa TIC Domicílios 2023 do **Instituto Brasileiro de Geografia e Estatística**. Disponível em: <https://agencia-denoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022>. Acesso em: 6 de mar. de 2024.

2 Pesquisa “We are Social”. Disponível em: <https://s3.meusitejuridico.com.br/2019/01/20de4ac8-artigo-internet-justica-dh.pdf>. Acesso em: 6 de mar. de 2024.

3 Reporte Anual 2024. Disponível em: <https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/>. Acesso em: 6 de mar. de 2024.

4 Disponível em: <https://datareportal.com/reports/digital-2023-brazil>. Acesso em: 6 de mar. de 2024.

5 Sobre sociedades hiper conectadas, ver mais em: Zambello, B. L., Ferdinandi, F., Castardo, A. P. B., Grossi-Milani, R., & Macuch, R. da S. (2021). Alpha, a Geração Hiper conectada e a Educação Emocional. *Saber E Educar*, 30(1). Disponível em: <https://revista.esepf.pt/article/view/29504>. Acesso em: 11 de mar. de 2024.

o ciberespaço pode promover ou violar direitos humanos⁶. A Lei do Marco Civil da Internet (MCI), em seu art. 2º, II, dispõe que além da liberdade de expressão, o uso da internet no Brasil também tem como fundamento os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais⁷. Não sem motivos: a Constituição Federal de 1988 consagrou⁸ os direitos humanos como um dos pilares do ordenamento jurídico brasileiro. Isso implica em dizer que, em termos de hierarquia normativa, toda legislação infraconstitucional no país deverá se pautar no respeito e na promoção aos direitos humanos⁹. Nos jargões jurídicos de direitos humanos, diz-se que serão inconventionais as leis, normas ou políticas públicas que firmam os parâmetros de direitos humanos com os quais o Brasil se comprometeu¹⁰.

CIBERESPAÇO: OPORTUNIDADE DE VIOLAÇÃO OU PROMOÇÃO DE DIREITOS HUMANOS?

No início dos anos 1990, o movimento libertarianista¹¹ defendeu que, ao novo espectro criado pelo ambiente virtual, caberia o afastamento do Estado. Passados 30 anos do *boom* da internet¹², a aplicabilidade das legislações nacionais e internacionais ao ambiente digital é consenso em países democráticos, vide os países

6 A pesquisa TIC Domicílios 2023 traz consigo recortes de classes sociais e demais indicadores sob os quais este artigo não se debruçará por inviabilidade metodológica, mas os dados indicam, por exemplo, menor nível de acesso nas classes D e E (69%) em comparação à 100% de conectividade na classe A. Além disso, entre as pessoas não alfabetizadas o acesso é de 32% em comparação a 100% para pessoas com nível superior. Disponível em: <https://cetic.br/pt/pesquisa/domicilios/indicadores/>. Acesso em: 6 de mar. de 2024.

7 Lei nº 12.965/2014, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 6 de mar. de 2024.

8 O art. 1º da Constituição Federal fixa a dignidade da pessoa humana, a cidadania e os valores sociais do trabalho como pilares do Estado Democrático de Direito. A partir da leitura conjunta do art. 5º e do art. 60, §4º, tem-se que os direitos humanos são estabelecidos como cláusulas pétreas dentre as demais normas constitucionais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 de mar. de 2024.

9 Neste artigo, a expressão “direitos humanos” será utilizada como sinônimo de “direitos fundamentais” de modo a facilitar a leitura. Ver em: de Moraes, A. (2003). Direitos humanos fundamentais. *Teoria Geral. São Paulo: Atlas*. Disponível em: <https://core.ac.uk/download/pdf/79114010.pdf>. Acesso em: 1 de mar. de 2024.

10 Para maiores reflexões sobre controle de convencionalidade, conferir: MAZZUOLI, Valerio de Oliveira. Teoria geral do controle de convencionalidade no direito brasileiro. *Revista Direito e Justiça -Reflexões Sociojurídicas -Ano IX -Nº*, v. 12, 2009.

11 ANTONIALLI, Denys; LIMA, Pedro. Aos 70, falece John Perry Barlow, um dos fundadores do movimento ciberlibertarianista e da Electronic Frontier Foundation, InternetLab, 2018. Disponível em: <https://www.internetlab.org.br/pt/noticias/aos-70-falece-john-perry-barlowum-dos-fundadores-do-movimento-ciberlibertarianista-e-da-electronic-frontier-foundation/>. Acesso em: 6 de mar. de 2024.

12 Para mais informações sobre a relação entre a década de 90 e os avanços da internet, ver em: de Quadros, C. I. (2006). Dez anos depois do boom dos diários digitais. *Revista FAMECOS*, 13(31), 65-69.

signatários da Convenção de Budapeste de combate ao cibercrime¹³. O discurso, à época marcado pela “Declaração de independência do ciberespaço”¹⁴, escrito por John Parry Barlow, em fevereiro de 1996, defendia que o conceito global da internet justificaria o afastamento completo da atividade estatal.

Houve uma segunda corrente, desenvolvida pelo professor Lawrence Lessig, de Harvard, que defendeu que a internet, seus usuários e provedores teriam condições de desenvolver uma autorregulação para o ambiente virtual. O professor desenvolveu a ideia de “mão invisível” para o controle virtual.

A teoria que prevaleceu em diversos países do ocidente¹⁵ foi a corrente tradicionalista, que projeta as leis e tratados¹⁶ internacionais à internet¹⁷. A partir do princípio da territorialidade¹⁸, cada Estado tem soberania sobre os indivíduos que se conectam ao ambiente virtual dentro do seu respectivo perímetro. Dessa forma, não há distinção entre as regras que se aplicam ao ambiente “real” e ao virtual, sobretudo no que toca à proteção de direitos humanos. Em realidade, ao contrário do entendimento adotado pela teoria libertarianista, as violações de direitos na internet¹⁹ geraram movimento reativo, de criação de legislações específicas para o ambiente virtual, normas cada vez mais atualizadas para proteger os direitos e pessoas envolvidas nas relações cibernéticas²⁰.

13 O Tratado de Budapeste é um instrumento internacional multilateral aprovado pelo Conselho Europeu em 2001 de combate ao crime cibernético. Em 2023, por meio do Decreto nº 11.491, o Brasil promulgou a Convenção, internalizando-a ao ordenamento jurídico nacional.

14 Barlow, John Perry, Declaration of the Independence of Cyberspace, 1996. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: 8 de mar. de 2024.

15 Por exemplo: [Regulamento Geral sobre a Proteção de Dados na União Europeia](#), o “Clarifying Lawful Overseas Use of Data Act” (ou Cloud Act), a Seção 230 do [Communications Decency Act](#) nos Estados Unidos da América, a [Declaração Africana sobre Direitos e Liberdades na Internet](#) e a [Proposta Legislativa de Danos On-line do Canadá](#). Acesso em: 6 de mar. de 2024.

16 Internet pode ser regulada por tratados, diz Blanco de Moraes. **Consultor Jurídico**. Disponível em: <https://www.conjur.com.br/2023-jul-04/internet-regulada-tratados-blanco-morais/>. Acesso em: 10 de mar. de 2024.

17 Está sendo discutido na ONU um novo Tratado para cibercrimes e cibersegurança. Para maiores informações: **Convenção de Cibercrimes da ONU: o que sabemos até o momento?** IRIS-BH. Disponível em: <https://irisbh.com.br/convencao-de-cibercrimes-da-onu-o-que-sabemos-ate-o-momento/>. Acesso em: 9 de mar. de 2024.

18 TIBURCIO, Carmen; ALBUQUERQUE, Felipe. Territorialidade, jurisdição e internet: alguns aspectos de direito internacional privado. **Revista Eletrônica de Direito Processual**, v. 24, n. 3, 2023.

19 Na Itália, por exemplo, a “Internet Bill of Rights” foi adotada em agosto de 2015, estabelecendo o acesso à internet como um serviço público e como um direito humano, sendo condição para o desenvolvimento individual e social. Além disso, recentemente, no campo da proteção da privacidade e dos dados pessoais, merecido destaque deve ser conferido à Lei de Proteção de Dados Pessoais, do Brasil (Lei nº 13.709), e ao Regulamento Geral sobre a Proteção de Dados 2016/679 (GDPR), na União Europeia, ambas adotadas em 2018. IN: PIOVESAN, Flavia; QUIXADÁ, Leticia. Internet, Direitos Humanos e Sistemas de Justiça. **III Congresso Mundial de Justiça Constitucional, na Universidade de Bologna**, 2017, pág. 19-21. Disponível em: <https://s3.meusitejuridico.com.br/2019/01/20de4ac8-artigo-internet-justica-dh.pdf>. Acesso em: 6 de mar. de 2024.

20 Para mais detalhes sobre os movimentos regulatórios do ciberespaço em função da violação de direitos humanos, ver em: PIOVESAN, Flavia; QUIXADÁ, Leticia. Internet, Direitos Humanos e Sistemas de Justiça. **III Congresso Mundial de Justiça Constitucional, na Universidade de Bologna**, 2017, pág. 19-21. Disponível em: <https://s3.meusitejuridico.com.br/2019/01/20de4ac8-artigo-internet-justica-dh.pdf>. Acesso em: 6 de mar. de 2024.

À luz desse cenário, somos conduzidos ao seguinte questionamento: seria o ambiente virtual um promotor de direitos humanos ou um campo de facilitação para violação de direitos? Na sociedade global marcada pela produção, distribuição e uso da informação, a internet exerce um impacto tão singular que a própria conectividade é entendida como direito humano em si²¹ e sua privação é identificada por órgãos de proteção humanitária como um risco à democracia e à liberdade de expressão²².

Na perspectiva de acesso a direitos, a internet revolucionou os mecanismos de mobilização social²³ em debates públicos, além de um maior controle de ações atentatórias a direitos humanos²⁴. O comércio online de produtos e serviços²⁵ ampliou possibilidades de geração de emprego e renda e o acesso à informação foi democratizado e estendido a regiões historicamente marginalizadas²⁶. Durante a pandemia de Covid-19, a relevância do acesso à internet no desenvolvimento de comunidades foi evidenciada, por exemplo, no acesso ao direito à educação²⁷; o resultado da suspensão das atividades presenciais atrelado à desigualdade de acesso à internet²⁸ acentuou os níveis de déficit educacional nas classes mais

21 É o entendimento de Ingo Sarlet, exprimido em “O direito humano e fundamental de acesso à internet”, no qual o autor identifica que, após a pandemia da covid-19, o direito à educação, à proteção da saúde e ao trabalho decente ficaram ainda mais atrelados ao direito ao acesso a uma internet de qualidade, segura e estável. Ver em: INGO SARLET. **Consultor Jurídico**. Disponível em: <https://www.conjur.com.br/2021-nov-12/direitos-fundamentais-direito-humano-fundamental-acesso-internet/>. Acesso em: 10 de mar. de 2024.

22 BUSSIEK, Hendrik. **Os Direitos Digitais São Direitos Humanos**. Uma introdução às circunstâncias e desafios em África. Disponível em: <https://library.fes.de/pdf-files/bueros/afrika-media/20175.pdf>. “Na África Subsaariana, 495 milhões de pessoas (46% da população) adquiriram telemóveis em 2020, no entanto, o custo do acesso à internet é muito elevado e muitos governos africanos são conhecidos por restringir o acesso à internet de modo a limitar as críticas e a oposição através de paralisações da internet, especialmente antes das eleições.” Acesso em: 10 de mar. de 2024.

23 Exemplo da história recente são as manifestações da Primavera Árabe, mobilizada em grande medida por ativismo digital. Ver em: PATRICIA, Vivian; VIEIRA, Peron. O papel da comunicação digital na primavera árabe: apropriação e mobilização social Disponível em: http://compolitica.org/novo/anais/2013_GT05-VivianPatriciaPeronVieira.pdf. Acesso em: 11 de mar. de 2024.

24 Morte de George Floyd mobiliza redes sociais e influencia manifestações. **Jornalismo PUC-SP**. Disponível em: <https://agemt.pucsp.br/noticias/morte-de-george-floyd-mobiliza-redes-sociais-e-influencia-manifestacoes#:~:text=Em%20meio%20a%20toda%20movimenta%C3%A7%C3%A3o,usado%20uma%20imagem%20completamente%20preta..> Acesso em: 11 de mar. de 2024.

25 Ver em: NO. **Comércio online cresce no Brasil e deve movimentar mais de R\$ 186 bi**. Agência Brasil. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/economia/audio/2023-07/comercio-online-cresce-no-brasil-e-deve-movimentar-mais-de-r-186-bi>. Acesso em: 12 de mar. de 2024.

26 LEMOS, Marcela. **Morador grava casa sendo revirada por policiais no RJ; PMs acabam afastados**. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/02/10/pms-sao-afastados-apos-serem-flagrados-revirando-ca-sa-em-comunidade-do-rio.htm>. Acesso em: 11 de mar. de 2024.

27 O Brasil foi o segundo país da América do Sul e o quarto do mundo que mais tempo manteve fechadas as escolas durante os dois anos e meio de pandemia de covid-19, segundo o relatório da Organização para Cooperação do Desenvolvimento Econômico (OCDE) de 2021. Ver em: **Education Policy Outlook**., 2021. Disponível em: <https://www.oecd.org/education/policy-outlook/country-profile-Brazil-2021-PT.pdf>. Acesso em: 10 de mar. de 2024.

28 Para mais, ver em: Pandemia acentua déficit educacional e exige ações do poder público. **Senado Federal**. Disponível em: <https://www12.senado.leg.br/noticias/infomaterias/2021/07/pandemia-acentua-deficit-educacional-e-exige-acoes-do-poder-publico> Acesso em 8 de mar. de 2024.

pobres²⁹, provocando perdas ainda não totalmente mensuradas³⁰. Esses são alguns dos incontáveis exemplos de como a internet atua como vetor de promoção de direitos fundamentais³¹. E, ainda que os avanços sejam incontroversos, o outro lado da realidade virtual apresenta desafios relacionados ao mau uso da ferramenta como meio de violações a direitos humanos.

O tema mobiliza diferentes setores da sociedade. No mesmo período de aprovação do Marco Civil, foi lançado pelo governo federal o programa Humaniza Redes (no bojo do Pacto Nacional de Enfrentamento das Violações de Direitos Humanos na Internet³²). O Ministério dos Direitos Humanos e Cidadania³³ apresenta o ObservaDH³⁴, plataforma direcionada ao enfrentamento de violações a direitos humanos no Brasil. Seria incauto presumir que é a internet que cria uma postura desviante – desvios existem em todos os espaços, mas o ambiente virtual é passível de utilização para práticas nefastas, as quais devem ser coibidas por ferramentas articuladas, tornando-o mais seguro para os diversos usuários.

A arquitetura das novas tecnologias depende, como todo processo complexo, da participação de múltiplos atores. O debate deve, portanto, perpassar pelo questionamento de qual será o papel daqueles envolvidos na interação social – ainda que virtual. Nesse sentido, os atores virtuais são movidos pelo mesmo propósito: de promover (i) a garantia de acesso à internet como direito humano; (ii) a redução das desigualdades para conectividade de qualidade e de segurança no Brasil e (iii) o enfrentamento a violações a direitos humanos no ciberespaço.

29 De acordo com o Relatório “Crianças negras geralmente compõem a maioria das pessoas em situação de pobreza e estão mais propensas a sofrer muito mais privações sociais e educacionais. O prolongado fechamento das escolas durante a COVID-19 provavelmente acentuou essas desigualdades. Cerca de 30% dos alunos menos favorecidos no Brasil, assim como aqueles em escolas rurais, relataram ter acesso a um computador em casa para os trabalhos escolares em 2018, contraopondo-se a quase 90% dos alunos favorecidos ou em escolas particulares.”

30 Estudo Perda de aprendizagem na pandemia. **Instituto Unibanco**. Disponível em: <https://www.institutounibanco.org.br/conteudo/estudo-perda-de-aprendizagem-na-pandemia/>. Acesso em: 10 de mar. de 2024.

31 PIOVESAN, Flavia; MUÑOZ, Lucien. **Internet e direitos humanos**. Brasil. Disponível em: <https://brasil.un.org/pt-br/74901-artigo-internet-e-direitos-humanos>. Acesso em: 1 de mar. de 2024.

32 Lançado em 2015, após a sanção do MCI, com a edição da Portaria Interministerial nº 3, de 09 de abril de 2015. Disponível em: <https://sintse.tse.jus.br/documentos/2015/Abr/9/diario-oficial-da-uniao-secao-1/portaria-interministerial-no-3-de-8-de-abril-de>. Acesso em: 10 de mar. de 2024.

33 Em fevereiro de 2024, o ministro dos Direitos Humanos, Silvio Almeida, participou [55ª sessão do Conselho de Direitos Humanos da ONU](#), onde debateu os impactos das novas tecnologias para a democracia. Segundo Almeida, “inúmeras pesquisas têm sugerido que o design algorítmico dos atuais ambientes digitais contribui para os vieses antidemocráticos explorados pela extrema direita” e seguiu pontuando que democracia não significa dar um smartphone na mão de cada cidadão mas uma estrutura para a produção de mundos comuns onde diferenças possam conviver de forma não violenta, e os recursos tangíveis e intangíveis possam ser (re)distribuídos da forma mais justa possível”. Acesso em: 6 de mar. de 2024.

34 O [ObservaDH](#) monitora violações a direitos humanos oriundos de discurso de ódio nas redes sociais. Os dados a respeito do quantitativo de crimes de ódio promovidos no ciberespaço impulsionaram a produção “Relatório de Recomendações para o Enfrentamento ao Discurso de Ódio e ao Extremismo no Brasil”, produzido pelo Grupo do Trabalho (GT) instituído pelo ministro dos Direitos Humanos e da Cidadania (MDHC).

Instrumento relevante no debate são os Princípios Orientadores da Organização das Nações Unidas (ONU) sobre Empresas e Direitos Humanos³⁵, nos quais são previstos papéis distintos para Estado e empresas na prevenção, mitigação e reparação a eventuais violações a direitos humanos relacionadas às atividades empresariais. O documento propõe que a solução não estaria em uma única medida – problemas complexos não são solucionados com medidas simplistas –, mas em um “smart mix” de providências. O desafio central que vivemos corresponde à consolidação de um sistema que fomente o acesso e uso do ambiente virtual³⁶ para acesso e exercício de direitos fundamentais, e que desestimule eventuais desvios, por meio de um esforço conjunto dos diferentes atores.

CONSIDERAÇÕES FINAIS

A internet, enquanto plataforma global, enfrenta a complexa dualidade de promover direitos fundamentais e simultaneamente ser meio para a violação desses direitos. A disseminação acelerada de informações proporciona acesso à educação, liberdade de expressão e conectividade social, fortalecendo a promoção e exercício de direitos. No entanto, a mesma rede também é passível de utilização para ameaças como violações à privacidade, disseminação de discursos de ódio e manipulação de dados, representando desafios significativos para a salvaguarda dos direitos fundamentais. Encontrar um equilíbrio entre a expansão dos benefícios da internet e a mitigação de seus impactos negativos é crucial para a construção de um ambiente digital mais ético e justo.

No Brasil, a Constituição de 1988, o Marco Civil da Internet e os tratados internacionais dos quais o país é signatário compõem parte significativa da moldura jurídica traçada em busca da prevenção a violações a direitos humanos. O desafio é, portanto, construir políticas (públicas e privadas) que viabilizem que uma ferramenta positiva como a internet, que gera acesso a direitos, não tenha seu fim desvirtuado.

Assim, conclui-se este artigo na pretensão de que o processo de consolidação de uma governança virtual em direitos humanos caminhe rumo a garantir um ciberespaço responsável, livre, seguro e ético, pautado em um *human rights approach* em que o desenvolvimento tecnológico seja, de fato, um instrumento dedicado a uma cultura de paz e à promoção de direitos e de sociedades socialmente equilibradas.

35 UNITED NATIONS. **Guiding Principles on Business and Human Rights Implementing the United Nations “Protect, Respect and Remedy” Framework**. [s.l.]: United Nations, 2011. Disponível em: <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf>. Acesso em: 10 de mar. de 2024

36 Conferir nota de rodapé nº 22.

OPEN FINANCE E O MARCO CIVIL DA INTERNET

Luiza Sato
Pedro Eroles
Júlia Viana

INTRODUÇÃO

O Brasil é o caso mais bem-sucedido de todo o mundo de operação Open Finance. No glossário fornecido pelo Banco Central do Brasil (Bacen),

o Open Finance, ou sistema financeiro aberto, é a possibilidade de clientes de produtos e serviços financeiros permitirem o compartilhamento de suas informações entre diferentes instituições autorizadas pelo Banco Central e a movimentação de suas contas bancárias a partir de diferentes plataformas e não apenas pelo aplicativo ou site do banco, de forma segura, ágil e conveniente.

Nos primeiros três anos de atividade, o Open Finance brasileiro tornou-se o maior do mundo, tanto em escopo de dados, como em volume de chamadas. Conforme números publicados, nesse período,

as instituições representadas pela Federação Brasileira de Bancos (Febraban) já investiram mais de R\$ 2 bilhões no projeto. A entidade aponta que o sistema já tem mais de 42 milhões de consentimentos e que atualmente mais de 1 bilhão de comunicações bem-sucedidas ocorrem todas as semanas.¹

A exitosa operação não poderia ser minimamente viável sem a existência de todo um arcabouço jurídico que permitisse a sua ampla e segura adoção. Considerando o cerne das atividades do Open Finance, qual seja, o compartilhamento de dados nas plataformas digitais mediante tráfego via internet, não há dúvidas de que o Marco Civil da Internet (MCI) tenha sido absolutamente imprescindível para o *case* de sucesso.

¹ CAMPOS, Álvaro. Open Finance brasileiro se torna o maior do mundo. Disponível em: <<https://valor.globo.com/financas/noticia/2024/02/05/open-finance-brasileiro-se-torna-o-maior-do-mundo.ghtml>>. Acesso em: 29 de fev. de 2024.

O OPEN FINANCE

Nos termos da Resolução Conjunta Bacen e Conselho Monetário Nacional (CMN) nº 1 de 2020, o Open Finance é caracterizado como o “compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas”. Nesse sentido, a partir da obtenção do consentimento dos clientes para fins do compartilhamento de dados de cadastro e de transações e de serviços, o Open Finance permite que as instituições financeiras se conectem diretamente às plataformas de outras instituições participantes e tenham acesso aos dados autorizados pelos clientes. Importa ressaltar que o consentimento concedido pelo cliente poderá ser revogado a qualquer momento, devendo as instituições participantes assegurar essa possibilidade por meio de procedimento seguro, ágil, preciso e conveniente.

Inicialmente, as informações disponibilizadas pelas instituições participantes no âmbito do Open Finance eram dados padronizados que abrangiam os canais de atendimento dessas instituições, bem como as características dos produtos e serviços por elas oferecidos. Posteriormente, dados sobre produtos referentes a câmbio, seguros, previdência, investimento e credenciamento passaram a integrar essa lista.

Os dados estão disponibilizados em formato aberto e permitem a construção de soluções que comparam diferentes ofertas de produtos e serviços financeiros, como tarifas bancárias, possibilitando que os clientes escolham a opção mais favorável às suas necessidades. Essa prerrogativa tanto fomentou a competitividade no sistema financeiro, uma vez que as instituições participantes podem ofertar produtos e serviços mais vantajosos aos clientes de seus concorrentes, quanto permitiu maior transparência e controle do cliente sobre os seus dados.

Com o objetivo de promover um ambiente seguro para o desenvolvimento do Open Finance, o CMN e o Bacen publicaram normativos que disciplinam as responsabilidades pelo compartilhamento de dados, abrangendo as etapas de consentimento do cliente, autenticação do cliente e das instituições participantes e confirmação. Cumpre salientar que somente instituições autorizadas participam do Open Finance, bem como há regras para responsabilização dessas instituições, de forma que todo o processo de compartilhamento ocorre em um ambiente com múltiplas camadas de segurança, considerando, ainda, que o Bacen supervisiona todo o processo.

As inovações introduzidas pelo Open Finance continuam impactando o mercado financeiro e áreas correlatas. O Bacen e a Superintendência de Seguros Privados (Susep), órgão responsável pelo controle e fiscalização dos mercados de seguro, previdência privada aberta, capitalização e resseguro, estão trabalhando de forma

conjunta para incorporar a interoperabilidade entre o Open Finance e o sistema de seguros aberto, chamado Open Insurance. Essa interoperabilidade entre os ecossistemas permitiria que as pessoas compartilhassem seus dados armazenados nas instituições autorizadas para corretoras e seguradoras supervisionadas pela Susep.

A RELAÇÃO COM O MCI

O MCI foi promulgado com o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabelecendo diversos princípios e regras a respeito da economia digital e das atividades realizadas em ambiente online.

A necessidade de uma norma dessa natureza ocorreu devido à extensa exploração da internet para a execução de atividades inovadoras, em um momento em que mal se entendia como aplicar o Direito fora das costumeiras relações analógicas. Para que o mundo conectado não se tornasse uma verdadeira “terra sem lei”, sem respeito aos princípios democráticos e respeito à ordem jurídica, o MCI surgiu após amplo debate público, tornando-se uma importante referência para a sociedade brasileira. Com a nova estrutura normativa, uma série de iniciativas puderam ser desenvolvidas e executadas pelos setores público e privado, considerando a segurança da ampla adoção pela população.

O Open Finance tem como essência o compartilhamento, no meio digital, de dados entre instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, com a finalidade de que possam fazer ofertas de produtos e serviços para clientes de seus concorrentes, com benefícios para o consumidor, que poderá obter tarifas mais baixas e condições mais vantajosas. O art. 5º, § 3º da Resolução Conjunta Bacen/CMN nº 1 de 2020 estabelece ser necessário obter consentimento do cliente, para fins do compartilhamento de dados de cadastro e de transações e de serviços, sendo o consentimento entendido como “manifestação livre, informada, prévia e inequívoca de vontade, feita por meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou de serviços para finalidades determinadas”.

Nesse sentido, o MCI já assegurava, em seu art. 7º inciso VII, o direito do usuário de internet de não fornecer a terceiros seus dados pessoais, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

A esse respeito, interessante levantar que o MCI não é mais hoje a norma a ser seguida quando abordamos o tratamento de dados pessoais, incluindo o consentimento do titular para tanto. O MCI jamais pretendeu esgotar ou ser a norma

principal para regular o tratamento de dados pessoais. Em 2018, foi promulgada a Lei Geral de Proteção de Dados (LGPD), que passou a ser a norma a ser seguida para tal matéria, prevalecendo sobre as disposições contidas no MCI quanto ao tema.

De qualquer modo, o MCI possibilitou a existência de um campo digital regulado para possibilitar iniciativas que compreendem o tráfego de dados via internet, tendo servido de base antes da vigência de lei específica sobre dados pessoais.

Ainda, o art. 13 do regulamento do MCI, o Decreto nº 8.771/2016, estabeleceu importantes padrões de segurança da informação a serem seguidas por provedores de serviço da internet². Tais diretrizes serviram de base e estão em consonância com aquelas trazidas pela Resolução Conjunta Bacen/CMN nº 1 de 2020. Dentre vários exemplos, a resolução traz a obrigação de as instituições participantes instituírem mecanismos de acompanhamento e de controle com vistas a assegurar a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo (art. 40) e de adotarem procedimentos para verificar que potenciais parceiros assegurem “a confidencialidade, a integridade, a disponibilidade e a recuperação de dados e de informações sobre serviços compartilhados” (art. 37, inciso II, alínea “c”).

CONCLUSÃO

O sucesso do Open Finance brasileiro deveu-se muito ao ambiente digital seguro e possível por conta do MCI, que trouxe as regras estruturais da segurança e compartilhamento responsável de dados na internet, fundamentais para a proteção dos usuários.

Considerando a essência do Open Finance e do Marco Civil da Internet, percebemos que ambas as iniciativas têm como objetivo principal o empoderamento dos usuários e a proteção de seus direitos digitais. Ao permitir que os usuários tenham o total controle sobre seus dados financeiros, o Open Finance está alinhado com

2 Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e

IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

os princípios da proteção de dados estabelecidos no MCI, como os da finalidade, transparência, livre acesso, qualidade e segurança.

Em conclusão, a interconexão entre o Open Finance e o MCI destaca a importância de se promover um ambiente digital seguro, transparente e inovador para os usuários. Ambas as normas ensejam uma evolução positiva da exploração do ambiente digital, com benefícios significativos para os usuários e para a sociedade como um todo.

AS NORMAS SANITÁRIAS ENQUADRADAS PELO MARCO CIVIL DA INTERNET: UM BUG REGULATÓRIO OU UMA REGULAÇÃO VIRAL?

Marco Aurélio Antas Torronteguy
Victor Hugo Callejon Avallone

INTRODUÇÃO

Passados 10 anos da entrada em vigor do Marco Civil da Internet (MCI), houve diversos impactos da norma sobre a área da saúde. Desde a criação do MCI, a internet tem sido cada vez mais utilizada para questões de saúde, ainda que as normas sanitárias nem sempre tenham sido aprimoradas para acompanharem o MCI.

Este artigo analisa como o MCI se relaciona com a regulação em saúde. Para isso, parte-se da seguinte questão: como se aplicam as normas sanitárias quando tais normas se encontram no mesmo âmbito de incidência do MCI? Não parece razoável que haja um *bug regulatório*, no qual a regulação sanitária ficaria sem dar resposta aos riscos à saúde pública derivados da internet e dos espaços digitais. Tampouco parece lógico adotar uma *regulação viral*, que viole o princípio da legalidade e da hierarquia das normas.

Diante disso, quais os principais espaços de aplicação das normas sanitárias *vis-à-vis* o MCI? A resposta a essa pergunta pode considerar três aspectos: (i) o acesso às informações e a prevenção de riscos à saúde; (ii) a proteção de dados médicos e a ampliação do acesso à saúde, bem como, (iii) a atribuição de responsabilidade na oferta e na intermediação de produtos e serviços regulados pelas autoridades sanitárias. É o que se verá a seguir, em cada sessão deste artigo.

ACESSO ÀS INFORMAÇÕES E PREVENÇÃO DE RISCOS À SAÚDE

O MCI determina que a internet no Brasil tem, como um de seus princípios, a promoção do acesso à informação e ao conhecimento (artigo 4º, II). Do ponto de vista da legislação e regulação em saúde, o acesso à informação é igualmente fundamental, uma vez que as normas sanitárias tutelam as atividades envolvendo produtos regulados, como medicamentos, alimentos, produtos médicos e cosméticos, que podem trazer riscos à saúde.

Hoje é possível facilmente acessar a bula de um medicamento ou as instruções de uso de um produto médico no site da Agência Nacional de Vigilância Sanitária (Anvisa), onde também é possível verificar a situação de regularização de produtos sujeitos à vigilância sanitária. Por exemplo, se o produto é sujeito a registro sanitário, qualquer pessoa pode livremente verificar se o registro está válido e qual é o período de sua vigência. No caso dos medicamentos, também estão disponíveis informações sobre onde o produto é fabricado, a qual categoria regulatória pertence, sua classe terapêutica e sua rotulagem. Em alguns casos, é possível até mesmo acessar o parecer público da Anvisa sobre o produto.

Especificamente sobre as bulas, a Lei nº 11.903/2009, que “dispõe sobre o rastreamento da produção e do consumo de medicamentos por meio de tecnologia de captura, armazenamento e transmissão eletrônica de dados”, foi alterada em 2022 pela Lei nº 14.338/2022 para dispor especificamente sobre as diretrizes de uma bula digital de medicamentos. A ideia é que o acesso à bula digital de determinado medicamento possa ser realizado de forma ainda mais fácil: por meio de um código de barras bidimensional de leitura rápida. Os links de hospedagem para armazenamento das bulas digitais deverão ser autorizados pela Anvisa. Trata-se de informação necessária ao acesso seguro a medicamentos que é oficialmente divulgada e publicada por meio da internet.

Como próximo passo, o tema envolvendo as bulas digitais deve ser em breve regulamentado pela Anvisa, para uma implementação das novas bulas de forma faseada, com gradual substituição das bulas impressas das embalagens dos medicamentos. O uso de bulas digitais é uma evolução não somente estética, mas também auxilia com o acesso à informação de modo digital, visando à redução de riscos à saúde e com a intenção de aperfeiçoar as ações de farmacovigilância. O novo sistema também permitirá uma atualização mais célere dessas mesmas bulas pelas empresas farmacêuticas. O formato digital permitirá, inclusive, que sejam incluídas outras informações que facilitem o entendimento, como vídeos e instruções adicionais.

Outro ponto que merece destaque sobre o acesso à informação no contexto da regulação sanitária é a possibilidade de acessar a própria regulação em vigor. A Anvisa tem competência normativa para criar normas para a proteção da saúde, normalmente editadas no formato de Resoluções da Diretoria Colegiada (RDCs). Novas RDCs muitas vezes revogam RDCs anteriores, recentes e antigas, e de forma parcial ou integral. Com a internet e com a biblioteca temática de normas da Anvisa, hoje é possível acessar as normas da Anvisa de forma muito mais fácil, o que também facilita a atuação e adequação da indústria.

PROTEÇÃO DE DADOS MÉDICOS E AMPLIAÇÃO DE ACESSO À SAÚDE

O MCI também trouxe princípios muito importantes sobre a proteção dos dados pessoais e das comunicações privadas. A garantia da proteção às informações de saúde e ao prontuário antecede à criação do MCI (e, conseqüentemente, da Lei Geral de Proteção de Dados – LGPD), mas o MCI pavimentou a aplicação dos princípios envolvendo o sigilo também nas relações via internet.

Hoje é inquestionável que uma consulta médica realizada pela internet estará sujeita aos mesmos cuidados, proteções e sigilo de uma consulta médica realizada de forma presencial. No entanto, desde a criação do MCI, a prestação de serviços de saúde pela internet precisou ser reconhecida como segura e permitida pela legislação.

Em que pese já existirem discussões anteriores sobre a possível prestação de serviços online por meio do atendimento entre médico e paciente nos anos anteriores, o tema ganhou força e foi endereçado pelas normas sanitárias durante a pandemia de Covid-19. Primeiramente, a prática da telemedicina diretamente entre médico e paciente foi condicionada à situação de Emergência em Saúde Pública de Importância Nacional (ESPIN).

Após o fim da ESPIN, diante dos resultados positivos observados da prática da telessaúde, houve a alteração da Lei nº 8.080/1990, que “dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências”. Atualmente, a prática da telemedicina não mais possui caráter excepcional e temporário, mas abrange todas as profissões da área da saúde regulamentadas pelos órgãos do Poder Executivo federal, nos termos do art. 26-A – trata-se do conceito de *telessaúde*.

Dentre os princípios da telessaúde previstos na Lei nº 8.080/1990, destacam-se a confidencialidade dos dados e a universalização do acesso às ações e serviços

de saúde à população brasileira. Nesse sentido, a prática da telemedicina (bem como da prestação de outros serviços de saúde pela internet) está intimamente ligada ao MCI, dado o alinhamento de suas disposições aos seus princípios.

Quanto à universalização de acesso às ações e serviços de saúde, nota-se sintonia com o MCI à medida em que esse reconhece a importância da internet para promoção do desenvolvimento humano e do exercício da cidadania. Tal promoção é exatamente o que ocorre com a utilização da telemedicina, dadas as possibilidades de expansão do acesso a consultas por pacientes junto a profissionais de saúde de forma remota, sendo tal ferramenta fundamental para a difusão do acesso à saúde.

Já no que diz respeito ao princípio da telemedicina quanto à confidencialidade de dados, as disposições do MCI sobre privacidade de informações fortalecem a prática da prestação remota de serviços de saúde, uma vez que o MCI ressalta a inviolabilidade da privacidade dos agentes.

A importância da privacidade no âmbito da saúde, é, ainda, corroborada pela LGPD, que classifica dados referentes à saúde como “dados sensíveis”, cujo tratamento deve observar uma série de requisitos previstos na norma, dentre os quais a proibição da comunicação ou uso compartilhado de informações relacionadas à saúde entre controladores para fins de obtenção de vantagem econômica, salvo para fins de prestação de assistência à saúde, nos termos do art. 11, § 4º da LGPD.

RESPONSABILIDADE SOBRE CONTEÚDOS NA OFERTA E INTERMEDIÇÃO DE PRODUTOS E SERVIÇOS REGULADOS

Com o objetivo de assegurar a liberdade de expressão, o art. 19 do MCI estabelece que provedores de aplicações de internet somente podem ser responsabilizados civilmente por conteúdos disponibilizados por terceiros, se não tomarem providências para retirar o conteúdo do ar após ordem judicial específica, considerando os limites técnicos do provedor e do prazo assinalado.

Desde a edição do MCI, surgiram diversos novos modelos de negócios envolvendo serviços e produtos que podem se relacionar com atividades reguladas, como a criação de diversas novas empresas conhecidas como *Healthtechs*, plataformas de intermediação, *marketplaces*, dentre outros modelos inovadores.

Nesse ponto, a legislação e regulação sanitária ainda não acompanharam as novas tendências do mercado e, sobretudo, a evolução da tecnologia. Por exemplo,

as normas envolvendo prestação de serviços médicos ainda não endereçam claramente o papel das empresas que prestam serviços de intermediação.

Em igual medida, tampouco foram regulamentadas as plataformas que prestam serviços integrados. Ainda hoje, as normas sobre saúde e sobre atuação ético-profissional em saúde distinguem as noções de comercialização de produto e de prestação de serviço. Assim, de um modo geral, as autoridades ainda têm a tendência a interpretar que é proibido a uma empresa atuar na cadeia de comercialização de produtos relacionados à saúde (como a venda de medicamentos) e, ao mesmo tempo, atuar na prestação de serviços relacionados a esses mesmos produtos (como um atendimento médico).

Outro ponto diz respeito à venda de produtos. Por exemplo, o controle sanitário exercido pela Anvisa também abrange a oferta de medicamentos pela internet. A RDC Anvisa nº 44/2009 prevê uma série de requisitos a serem observados na prática de dispensação remota de medicamentos. Ocorre que a norma foi criada até mesmo antes da popularização dos smartphones (sem modificações relevantes até agora) e, ao tratar da venda remota de medicamentos, menciona somente a venda por sites (<http://>) próprios de farmácias, sem qualquer previsão regulatória da venda por aplicativos ou mesmo do uso de plataformas de *marketplaces* pelas próprias farmácias. Trata-se de norma obsoleta que há de ser atualizada pela Anvisa.

Hoje é possível incorporar muitos dos novos negócios digitais ao ecossistema da economia da saúde, de forma segura e inovadora, mas é preciso que as normas sanitárias evoluam para acompanhar as novas tendências. Portanto, deve haver atribuições claras para as entidades corretas, evitando-se responsabilização de plataformas de intermediação ou de *marketplaces* como se fossem prestadores de serviços de saúde ou ofertantes de produtos regulados, quando claramente não o são.

CONSIDERAÇÕES FINAIS

A internet tornou-se ferramenta ligada intrinsecamente à vida do ser humano e sua utilização oferece aplicações importantes também no campo da saúde. Nesse sentido, o MCI segue exercendo papel fundamental ao trazer diretrizes relacionadas à segurança da informação, à promoção do desenvolvimento humano e da difusão do conhecimento e de informações, que permeiam cada vez mais os produtos e serviços sujeitos à vigilância sanitária.

O desenvolvimento em ritmo excepcional de utilidades derivadas da tecnologia da informação contribuiu para as origens do MCI, assim como novos cenários tecnológicos relacionados à saúde têm surgido exponencialmente. Todos os elementos desse caldeirão de inovações desafiam as normas existentes, exigindo novas regulamentações e interpretações para proteger a privacidade, definir responsabilidades e garantir o uso ético dessas inovações.

Com a incorporação cada vez maior de novas tecnologias, como a inteligência artificial (IA), ou mesmo com relação às aplicações do metaverso no setor da saúde, é esperado que a regulação infralegal da Anvisa seja constantemente aprimorada, bem como seja corretamente interpretada à luz do MCI. Para tanto, serão necessários, por exemplo, maior alinhamento e coordenação entre órgãos reguladores, avaliação de impacto regulatório para a atualização normativa, como também a participação do setor regulado e sociedade civil.

Em suma, quando se pergunta qual é o desafio de aplicar as normas sanitárias no mesmo contexto de incidência do MCI, a resposta pode ser a seguinte: não se trata de um *bug regulatório*, no qual a regulação sanitária ficaria sem dar resposta aos riscos à saúde pública. Tampouco se trata de uma regulação viral, que se impusesse a qualquer custo e violasse a legalidade da norma hierarquicamente superior. Trata-se de uma interpretação conforme o Direito, a saber: as normas infralegais da Anvisa devem ser interpretadas de modo a respeitar o MCI.

REFERÊNCIAS

BRASIL. Lei nº 8.080, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Diário Oficial da União. Brasília, DF, 20 set. 1990.

BRASIL. Lei nº 9.782, de 26 de janeiro de 1999. Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária, e dá outras providências. Diário Oficial da União. Brasília, DF, 27, jan. 1999.

BRASIL. Lei nº 11.903, de 14 de janeiro de 2009. Dispõe sobre o rastreamento da produção e do consumo de medicamentos por meio de tecnologia de captura, armazenamento e transmissão eletrônica de dados. Diário Oficial da União. Brasília, DF, 15, jan. 2009.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União. Brasília, DF, 24, abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília, DF, 15, ago. 2018.

BRASIL. Ministério da Saúde. Agência Nacional de Vigilância Sanitária (Anvisa). Resolução da Diretoria Colegiada – RDC 44, de 17 de agosto de 2009. Dispõe sobre Boas Práticas Farmacêuticas para o controle sanitário do funcionamento, da dispensação e da comercialização de produtos e da prestação de serviços farmacêuticos em farmácias e drogarias e dá outras providências. Diário Oficial da União, Poder Executivo, Brasília, DF, 18 ago. 2009.

BRASIL. Ministério da Saúde. Portaria 467, de 20 de março de 2020. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. Diário Oficial da União, Poder Executivo, Brasília, DF, 23 mar. 2020.

BRASIL. Ministério da Saúde. Agência Nacional de Vigilância Sanitária (Anvisa). Resolução da Diretoria Colegiada – RDC 585, de 10 de dezembro de 2021. Aprova e promulga o Regimento Interno da Agência Nacional de Vigilância Sanitária – Anvisa e dá outras providências. Diário Oficial da União, Poder Executivo, Brasília, DF, 15 dez. 2021.

TORRONTÉGUY, M.A.A.; AVALLONE, V.H.C. Direito da saúde hackeado: metahealth. In: MARTINS, P.H.M. et al. Metaverso: Aspectos Jurídicos. São Paulo: Almedina, 2022, p. 115-126.

TORRONTÉGUY, M.A.A. et. alli. Brazil. In : BOGAERT, Peter. The Life Sciences Law Review. 11ª. Edição. Londres: Law Business Research, 2023, p. 53-68.

SEGUROS: DISTRIBUIÇÃO PELA INTERNET

Bárbara Bassani de Souza

INTRODUÇÃO

Quando da publicação da Lei nº 12.965, de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (o Marco Civil da Internet, MCI), os produtos de seguros já eram distribuídos em larga escala por meios remotos.

Nos últimos 10 anos, o setor de seguros vem crescendo e, com isso, naturalmente, há um aumento dos mais diversos canais de distribuição desses produtos com a utilização ampla da internet.

O regulador de seguros, a Superintendência de Seguros Privados (Susep), atento a esse movimento, consolidou inovações normativas, propiciando mais liberdade, flexibilidade e transparência, ao mesmo tempo em que há uma preocupação maior com segurança cibernética.

CONTRATAÇÃO DE SEGUROS POR MEIOS REMOTOS

A partir da publicação do MCI, iniciou vigia a Resolução do Conselho Nacional de Seguros Privados (CNSP) nº 294/2013, que dispunha sobre a utilização de meios remotos nas operações relacionadas a planos de seguro e de previdência complementar aberta, considerada um passo importante para esse tipo de contratação.

Com o passar dos anos, a contratação de seguros por meios remotos foi intensificada, não apenas impulsionada pela pandemia, como também por todos os novos canais de distribuição, que foram surgindo e a utilização de novas tecnologias. Naturalmente, o regramento referente a esse tema também sofreu modificações importantes para a compatibilização com a nova realidade.

Nesse sentido, vige a Resolução CNSP nº 408/2021, segundo a qual meios remotos são aqueles que permitem a troca de e/ou o acesso a informações e/ou

todo tipo de transferência de dados por meio de redes de comunicação envolvendo o uso de tecnologias tais como rede mundial de computadores, telefonia, televisão a cabo ou digital, sistemas de comunicação por satélite, entre outras.

Dada a amplitude do conceito de meios remotos atribuído pelo regulador, a distribuição de seguros nesses canais tem aumentado cada vez mais, especialmente, pela internet¹. Para tanto, segundo a referida norma, devem ser garantidas: (i) a integridade, a autenticidade, o não-repúdio e a confidencialidade das informações e dos documentos eletrônicos; (ii) a confirmação do recebimento de documentos e mensagens enviadas pela seguradora ao cliente ou, quando couber, ao intermediário; e (iii) o fornecimento de protocolo² ao cliente ou, quando couber, ao intermediário, para as solicitações e procedimentos relativos ao produto contratado, conforme requisitos previstos na referida norma.

O conceito de meio remoto atribuído no âmbito regulatório de seguros é permitido não apenas para a oferta de seguros como também para emissão, envio e disponibilização de documentos relativos à contratação do seguro, tais como propostas, documentos contratuais, documentos de cobrança, notificações, extratos, condições contratuais, regulamentos, materiais informativos e comunicados.

As propostas de seguro podem ser preenchidas e formalizadas por meio do ambiente remoto, desde que passível de comprovação da autoria e integridade, devendo o cliente receber instruções detalhadas para acesso seguro aos documentos contratuais dos produtos contratados. Do mesmo modo, o ambiente remoto deverá garantir que as solicitações e os procedimentos necessários ao encerramento da relação contratual possam ser efetuados pelo meio que foi utilizado na contratação, sem prejuízo da disponibilização de outros meios.

Por força normativa, a utilização de meios remotos na emissão de documentos contratuais deverá garantir a possibilidade de impressão ou *download* do

1 Nesse sentido, a Susep, quando da exposição de motivos da referida norma, fundamentou: “Sob essa perspectiva, o consumidor brasileiro está pronto para a disrupção digital [1]: dois em cada três brasileiros têm acesso a smartphones e à internet; os brasileiros passam mais de nove horas por dia conectados (uma das maiores taxas do mundo); estão em 2º ou 3º lugar entre os que mais usam as principais plataformas de mídia social, incluindo Facebook, Instagram, YouTube, Netflix, WhatsApp e Pinterest; a publicidade digital continua crescendo a taxas de dois dígitos e o mesmo acontece com o e-commerce, a economia compartilhada e os serviços de entrega domiciliar. 13. Assim, é importante que seja revisada a regulamentação sobre a utilização de meios remotos nas operações de seguro, previdência complementar aberta e capitalização, com uma estrutura mais simples e objetiva do que o normativo vigente, e focada em: i) apresentação dos requisitos técnicos necessários para uso de meios remotos; e ii) tratamento sobre o uso de meios remotos para emissão e envio de documentos, contratação e demais procedimentos. A minuta não restringe os procedimentos e solicitações relativos ao produto contratado (que podem ser efetivados por uso de meios remotos), possibilitando uma operação 100% digital.” (Disponível em: < <https://www.gov.br/susep/pt-br/arquivos/arquivos-dos-documentos-e-publicacoes/arquivos-normas-em-consulta-publica/consultas-publicas-passadas-de-2021/ExposioMotivosMeiosRemotos.pdf> >. Acesso em: 10 de mar. de 2024).

2 O simples acesso ou consulta a documentos e informações disponibilizados pelo ente supervisionado dispensam a necessidade de fornecimento de protocolo.

documento pelo cliente e os documentos contratuais emitidos por meios remotos devem conter informação de data e hora de sua emissão, tudo para garantir que o cliente tenha provas efetivas da contratação, caso, por exemplo, precise se valer de meios judiciais para questioná-la ou mesmo para evitar problemas com a regulação de sinistros e com a próprio recebimento da indenização securitária.

Outro aspecto importante é que a utilização dos meios remotos não isenta as seguradoras ou seus parceiros comerciais do cumprimento de suas obrigações para com os segurados, especialmente no que se refere às regras de boas práticas de conduta³, as quais incluem a garantia de transparência e clareza ao quanto contratado e à necessária observância da legislação de proteção de dados.

CANAIS DE DISTRIBUIÇÃO

A parceria entre empresas e seguradoras para a oferta de seguros em meios remotos é comum. Instituições financeiras, organizações varejistas, agências de turismo, empresas de assistência, *marketplaces* têm sido importantes canais de distribuição de seguros. Referidas parcerias, geralmente, são estabelecidas por meio de estipulação⁴ ou de representação de seguros⁵, as quais não se confundem com a corretagem de seguros.

O corretor de seguros é considerado um *player* diferente, ou seja, não é estipulante e nem representante, sendo vedada (i) a atuação do estipulante e do representante de seguros como corretor de seguros; e (ii) a atuação de corretor de seguros e seus prepostos como representante de seguros.

O estipulante de seguros representa o grupo segurado e apenas pode comercializar apólice coletiva. A atuação do estipulante deve estar pautada pela preservação prioritária dos interesses do grupo segurado. Já, o representante de seguros atua como um distribuidor da seguradora, atuando em nome e no interesse da seguradora.

Com as recentes alterações normativas, o representante de seguros passou a ter uma atuação mais ampla, na medida em que a limitação de ramos de seguros

3 Vide Resolução CNSP nº 382, de 4 de março de 2020, que dispõe sobre princípios a serem observados nas práticas de conduta adotadas pelas sociedades seguradoras, sociedades de capitalização, entidades abertas de previdência complementar e intermediários, no que se refere ao relacionamento com o cliente, e sobre o uso do cliente oculto na atividade de supervisão da Susep, na forma definida por esta Resolução, e dá outras providências.

4 A estipulação de seguros está, atualmente, prevista na Resolução CNSP nº 434/2021, que revogou a Resolução CNSP nº 107/2004.

5 A representação de seguros está, atualmente, prevista na Resolução CNSP nº 431/2021, que revogou a Resolução CNSP nº 297/2013.

foi suprimida pela Susep⁶, o que, certamente, contribui para o aumento das operações de representação e consequente diminuição nas operações de estipulação, ao longo do tempo.

Além do modelo tradicional de representação de seguros, a regulamentação passou a permitir, de forma expressa, o modelo de representação ampliada, consubstanciado na figura do *Managing General Agent* (MGA), definido pela Susep como a entidade empresarial que recebe autorização de uma seguradora para administrar programas de seguro, negociar contratos em seu nome e atuar como intermediário entre seguradoras e corretores e/ou segurados. O MGA pode subscrever riscos, coletar prêmios, auxiliar na regulação de sinistros, ofertar seguros e administrar a carteira. A parceria com um MGA pode ser considerada como uma filial que fornece programas de seguros especializados dentro de classes específicas.

Basicamente, o MGA é uma entidade empresarial que recebe autorização de uma seguradora para administrar programas de seguro e negociar contratos em seu nome. O MGA pode atuar como intermediário entre seguradoras e corretores e/ou segurados.

A despeito da atuação como um parceiro comercial de uma seguradora ser regulada, o parceiro (com exceção do corretor) não é um ente regulado, por si. Nesse sentido, as regras do MCI são fundamentais para nortear as principais diretrizes que devem ser observadas quanto aos direitos do segurado, enquanto usuário da internet, quando o parceiro atuar também como um provedor, sem prejuízo, obviamente, da necessária observância das regras regulatórias referentes à distribuição de seguros.

6 Nos termos da Resolução CNSP nº 297/2013, revogada desde 1º de dezembro de 2021, a oferta de seguros por parte do representante estava limitada aos seguintes ramos: riscos diversos, garantia estendida, funeral, viagem, auto, prestamista, desemprego/perda de renda, eventos aleatórios, animais, microsseguros de danos, pessoas e previdência, assistência em geral. Referida limitação era excepcionada apenas em algumas situações específicas.

Por fim, o *Open Insurance*⁷, Sistema de Seguros Aberto, que permite o compartilhamento de dados dos segurados, e que vem sendo desenvolvido nos últimos anos, também será um ambiente de distribuição de seguros, no qual o olhar para a proteção dos interesses do segurado e a contratação pela internet ganhará ainda mais evidência.

SEGURANÇA CIBERNÉTICA

A Susep está atenta à segurança cibernética, tanto que publicou a Circular nº 638, em 3 de agosto de 2021, dispondo sobre os requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, Entidades Abertas de Previdência Complementar (EAPCs), sociedades de capitalização e resseguradores locais.

A publicação da referida regra está condizente com a necessária preocupação e adoção de medidas para minimização de vulnerabilidades dos sistemas das seguradoras e de seus parceiros, propiciando maior segurança aos segurados e englobando diretrizes contemplando a promoção de ações voltadas à disseminação da cultura de segurança cibernética, política de segurança cibernética, prevenção e tratamento de incidentes, além de regras para a terceirização de serviços de processamento e armazenamento de dados.

7 Recentemente introduzido pelo regulador, o *Open Insurance* é um ecossistema que permitirá aos consumidores o compartilhamento de informações e dados a respeito de produtos e serviços de seguros, previdência e capitalização, entre empresas do sistema de seguros e diferentes empresas autorizadas e credenciadas pela Susep para oferecer o serviço de agregação de dados e representação do cliente. O objetivo é melhorar a experiência do cliente e facilitar o processo de tomada de decisão frente a produtos e serviços das seguradoras e, do ponto de vista das empresas, tornar mais competitiva a oferta de seguros, incentivando a inovação no setor segurador, com a incorporação de novas tecnologias. (...) O ecossistema de informações compartilhadas tem como base dois tipos de dados, pessoais e públicos. Os dados pessoais são compostos pelas informações cadastrais dos consumidores, dados de apólices, contratos, títulos de capitalização, histórico de utilização, as transações dos clientes frente às seguradoras e entre outros. Já os dados públicos abrangem desde dados dos canais de atendimento, telefone ou canais digitais, corretores e representantes das empresas até informações de produtos disponíveis para comercialização, como seguros, previdência aberta e capitalização. (...) De acordo com o cronograma de implementação da Susep, o *Open Insurance* será realizado em três fases. A primeira fase – open data - teve início em dezembro de 2021 e se estende até 30 de junho de 2022, com o compartilhamento de dados públicos das empresas participantes, serviços e produtos disponíveis e canais de atendimento. A segunda fase tem previsão para iniciar em setembro de 2022, se estendendo até junho de 2023, e consiste no compartilhamento pelos participantes, dos dados pessoais e das movimentações dos clientes relacionadas aos produtos de seguros, previdência complementar aberta e capitalização, quando autorizado por eles. Por fim, a terceira fase terá início em dezembro de 2022 e será finalizada em junho de 2023, quando serão efetivados os serviços do *Open Insurance*, tais como: resgate, portabilidade e aviso de sinistro, entre outros, com foco na melhor experiência do consumidor. (Disponível em: <<https://cnseg.org.br/open-insurance-novo.html>>. Acesso em: 10 de mar. de 2024).

CONCLUSÃO

A cada dia, as seguradoras são mais desafiadas a desenvolver novos modelos de negócios, interagindo com os mais diversos canais de distribuição para ofertar os produtos de seguros, no ambiente que a internet propicia.

A simplificação regulatória vista nos últimos anos cria um ambiente saudável para o desenvolvimento de um setor mais inovador, mas, ao mesmo tempo, atento para diretrizes mínimas de segurança e proteção ao cliente, em linha com as principais diretrizes do MCI.

De todo modo, em razão das especificidades do mercado regulado, a distribuição de seguros pela internet deve, necessariamente, observar as regras emanadas pela Susep, sob pena da aplicação de penalidades cabíveis por parte da autarquia, inclusive.

REFERÊNCIAS

Fontes Legislativas

BRASIL. Lei nº 4.594, de 29 de dezembro de 1964. *Lei do Corretor de Seguros*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4594.htm>. Acesso em: 10 de mar. de 2024.

BRASIL. Decreto-Lei nº 73, de 21 de novembro de 1966. *Sistema Nacional de Seguros Privados*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del0073.htm>. Acesso em: 10 de mar. de 2024.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm>. Acesso em: 10 de mar. de 2024.

Sítios eletrônicos

<https://cnseg.org.br/>

<http://novosite.susep.gov.br/>

A GESTÃO E AUTENTICIDADE DOS LIVROS SOCIETÁRIOS DIGITAIS FRENTE AO MARCO CIVIL DA INTERNET

João Ribeiro da Costa
Oswaldo Noce Dalla Torre
Ana Carolina Gaspar
Isabella Fontoura D'Angelo
Maria Fernanda Seba Rahe

As características, direitos e deveres das sociedades por ações, sejam de capital aberto ou fechado, são previstos pela Lei nº 6.404/1976, a Lei das Sociedades Anônimas (S/A), segundo a qual é obrigatória a manutenção dos Livros Societários (ou Livros Sociais), no qual são formalizados e registrados todos os eventos societários de uma companhia. Seguindo os ditames do artigo 100 da referida lei, a companhia deve ter, além dos livros obrigatórios para qualquer comerciante:

I – o livro de “Registro de Ações Nominativas”, para inscrição, anotação ou averbação: (a) do nome do acionista e do número das suas ações; (b) das entradas ou prestações de capital realizado; (c) das conversões de ações, de uma em outra espécie ou classe; (d) do resgate, reembolso e amortização das ações, ou de sua aquisição pela companhia; (e) das mutações operadas pela alienação ou transferência de ações; e (f) do penhor, usufruto, fideicomisso, da alienação fiduciária em garantia ou de qualquer ônus que grave as ações ou obste sua negociação.

II – o livro de “Transferência de Ações Nominativas”, para lançamento dos termos de transferência, que deverão ser assinados pelo cedente e pelo cessionário ou seus legítimos representantes;

III – o livro de “Registro de Partes Beneficiárias Nominativas” e o de “Transferência de Partes Beneficiárias Nominativas”, se tiverem sido emitidas;

IV – o livro de Atas das Assembleias Gerais;

- V – o livro de Presença dos Acionistas;
- VI – os livros de Atas das Reuniões do Conselho de Administração, se houver, e de Atas das Reuniões de Diretoria;
- VII – o livro de Atas e Pareceres do Conselho Fiscal.

Até pouco tempo, o gerenciamento dos livros societários era feito de forma física, com a compra de brochuras em papelarias, escrituração manual e autenticação presencial na Junta Comercial. É custoso imaginar que, não obstante a profusão tecnológica observada na atualidade, o registro dos livros que garantem aos acionistas o direito sobre suas ações ainda fosse feito em papel e caneta. Evidente que o abandono desse formato era mais do que ansiado pela comunidade jurídica.

Além de vagaroso, o processo de elaboração manual dos livros acionários físicos favorecia erros de difícil correção e perfeitamente evitáveis no ambiente digital: perda de livros, rasgo de páginas, rasuras no preenchimento, textos ilegíveis ou assinaturas pendentes. Como resultado, a segurança da informação física se tornou inevitavelmente reduzida, quando comparada à modalidade digital, onde não existe a possibilidade de perda ou de estrago do material. Some-se a isso a ineficiência em operações societárias e de fusão e aquisição de empresas, que dependiam de assinaturas presenciais e manuscritas para serem concluídas.

Esse formato físico era obrigatório para todos os livros acionários de companhias, até que, em 2013, com a Instrução Normativa nº 11, do Departamento Nacional de Registro Empresarial e Integração (DREI), as sociedades por ações de capital fechado foram autorizadas a digitalizar seus livros. A normativa, no entanto, teve baixíssima adesão e os problemas se mantiveram.

Em 2014, o Marco Civil da Internet (MCI) reformou a mentalidade de todos os setores, de forma que a transição dos livros societários para o formato digital tornou-se indispensável. Os princípios e objetivos delineados pelo MCI, especialmente no que tange à liberdade dos modelos de negócios promovidos na internet, e à promoção da inovação e da acessibilidade coadunaram-se com essa inovação, que passou a ser cada vez mais desejada.

Foi somente em 2021 que a sinergia entre a Instrução Normativa (IN) do nº 82 do DREI e a IN DREI nº 79 impulsionou transformações substanciais na esfera da governança corporativa. Publicada em 19 de fevereiro de 2021, a IN DREI nº 82 buscou modernizar, simplificar e uniformizar os registros públicos empresariais, destacando-se pela introdução dos livros societários digitais obrigatórios, que tornam integralmente digital o processo de abertura e encerramento desses registros.

A normativa determinou que os livros societários fossem exclusiva e obrigatoriamente digitais, gerados ou acessados por plataformas eletrônicas e armazenados

nos servidores das Juntas Comerciais, com a expressa vedação na apresentação de novos registros em papel, preenchidos ou em branco, para autenticação (ressalvando-se a utilização dos registros já abertos na Junta Comercial até sua conclusão).

E não é só, tendo em vista a valorização da privacidade e proteção de dados que permeiam a era digital, a segurança da informação torna-se uma prioridade para as Instruções Normativas do DREI, que passaram a exigir a garantia de integridade e inviolabilidade dos dados hospedados nas plataformas eletrônicas de livros societários.

Essas mudanças aprimoram a gestão e a transparência das organizações e atenderam às demandas contemporâneas por mobilidade e agilidade, especialmente em um contexto pós-Covid-19, onde a acessibilidade digital e a assinatura eletrônica emergem como recursos indispensáveis para a adaptação e o progresso empresarial.

É dizer, portanto, que a IN DREI n° 82, aliada à IN DREI n° 79, representou uma revolução na governança das organizações ao introduzir os Livros Societários Digitais, modernizando e simplificando os processos de registro empresarial e fortalecendo a segurança da informação.

A regulamentação contemplou, ainda, a ampliação de acessibilidade e facilidade de atualização por meio da assinatura eletrônica, o que demonstra um avanço significativo em direção a uma gestão mais eficiente e transparente das companhias brasileiras. Com a adoção de registros corporativos digitais, os dados e informações empresariais podem ser armazenados em sistemas de segurança mais avançados, com emprego de criptografia de ponta, controle de acesso estrito e autenticação robusta de usuários. Essa proteção se revela essencial para garantir a confidencialidade e a integridade das informações e segredos empresariais.

Ademais, a certificação digital, medida utilizada como meio de garantir a autenticidade e integridade das transações eletrônicas, também deve ser utilizada para fortalecer a segurança e validade dos registros nos livros societários digitais, bem como proporcionar uma camada adicional de proteção aos dados dos acionistas, garantindo a confiança e legitimidade das operações corporativas.

A segurança dos dados torna-se ainda mais emblemática ao tratar das informações sensíveis dos acionistas que constam nos livros societários, como o registro da participação acionária, da distribuição de dividendos e de dados financeiros pessoais. Em relação a esses dados, deve-se observar, em linha com o artigo 10 do MCI, o dever das empresas de se atentarem à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, sendo de fundamental importância que estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Em relação à forma de coleta, armazenamento e utilização dos dados pessoais dos acionistas, mostra-se de extrema relevância a adoção de práticas transparentes de gerenciamento de informações, sendo dever do responsável pela provisão de serviços comunicar aos acionistas, bem como a qualquer outra parte direta ou indiretamente envolvida, de forma clara e transparente, as medidas e os procedimentos de segurança e de sigilo adotadas, na forma do art. 10, § 4º, do MCI, de modo que a digitalização dos livros societários não comprometa a privacidade e os direitos dos acionistas.

Em conclusão, a implementação dos Livros Societários Digitais não apenas atende às demandas por modernização e eficiência nos registros empresariais, mas também responde aos desafios contemporâneos de necessidade de adaptação a novas formas de trabalho e comunicação. Ao proporcionar acessibilidade e segurança aprimoradas, essa medida facilita a conformidade regulatória e promove uma cultura de transparência e responsabilidade dentro das organizações. Além disso, trata-se de relevante ferramenta de otimização do tempo no ambiente corporativo, apta a contribuir para o aprimoramento dos padrões de governança de sociedades anônimas, alinhando-as com a mentalidade trazida pelo Marco Civil da Internet e remodelando a maneira como as empresas operam e se relacionam com seus acionistas.

PROTEGENDO SEU INVESTIMENTO: CONSIDERAÇÕES LEGAIS PARA POTENCIAIS COMPRADORES EM OPERAÇÕES DE M&A ENVOLVENDO PROVEDORES DE APLICAÇÕES DE INTERNET À LUZ DO MARCO CIVIL DA INTERNET

Luiz Renato Okumura
Pedro Vecci Biancardini
João Vitor de Almeida Ramos

INTRODUÇÃO

Operações de fusões e aquisições (M&A, na sigla em inglês) são permeadas por uma miríade de questões legais que demandam meticulosa atenção das partes envolvidas. Quando a sociedade-alvo objeto da operação (*target*, no jargão do setor) é um provedor de aplicações de internet, um relevante fator a ser levado em consideração pelo potencial comprador ou investidor é a responsabilidade civil do provedor por conteúdos gerados por terceiros dentro do ambiente virtual.

O artigo 19 do Marco Civil da Internet (MCI) estabelece que a responsabilidade dos provedores de aplicações de internet por danos decorrentes de conteúdos criados por terceiros somente resta configurada quando o provedor descumpre ordem judicial que determina a retirada de tal conteúdo do meio virtual.

À parte do regime legal, o MCI permite que os provedores de aplicações de internet desenvolvam suas próprias políticas de termos de uso, as quais podem, a título ilustrativo, regular o conteúdo que pode ser exibido na plataforma e criar mecanismos de denúncia para averiguar supostos conteúdos ilícitos. Nessa hipótese, caso os provedores de aplicações entendam que determinado conteúdo de terceiros está em desacordo com os termos de uso da plataforma e façam sua remoção (observada a vedação ao abuso de direito), não estarão, em princípio, contrariando o MCI.

Em um contexto de operações de M&A, a compreensão do regime legal de responsabilidade civil do provedor de aplicações de internet – e do modo como os provedores lidam com os deveres que lhes são impostos pela lei – é fundamental, uma vez que tais aspectos impactam não somente o *valuation* da sociedade, como também a sua atratividade perante o mercado. Por essa razão, os potenciais compradores ou investidores devem ter uma visão clara das peculiaridades desse ramo de atividade, para reconhecer contingências passadas, evitar passivos futuros e garantir que a transação seja levada a cabo.

Nesse cenário, o presente artigo propõe-se a examinar as principais cautelas que o potencial comprador ou investidor deve guardar durante a operação de fusão e aquisição de provedores de aplicações de internet, com especial destaque para o processo de auditoria legal (ou *legal due diligence*) e a elaboração do contrato de compra e venda de participações societárias (notadamente, das cláusulas de condições precedentes, obrigações pós-fechamento, declarações e garantias e indenização).

A AUDITORIA LEGAL

Durante o processo de auditoria legal, é recomendável que potenciais compradores ou investidores realizem uma análise cuidadosa da sociedade-alvo provedora de aplicações de internet, para avaliar sua conformidade com o MCI. O escopo da *legal due diligence* deve incluir a revisão de eventuais processos e reclamações extrajudiciais envolvendo a remoção de conteúdos de terceiros, uma vez que tais questões podem evidenciar possíveis contingências e responsabilidades legais substanciais correntes ou futuras para a *target*.

Da mesma maneira, a existência e a eficácia de políticas internas de termos de uso relacionadas à moderação de conteúdo devem ser objeto de escrutínio durante a auditoria legal. Uma política robusta de moderação de conteúdo é crucial para garantir a conformidade dos provedores de aplicação com as disposições legais

e mitigar os riscos associados à própria responsabilidade civil, principalmente se o provedor almeja demonstrar atratividade comercial perante os demais *players* do mercado.

Os potenciais compradores ou investidores devem, desse modo, verificar se tais políticas estão alinhadas com os padrões mais rigorosos exigidos pelo MCI e, ainda, se são implementadas de maneira eficaz pela sociedade-alvo. Afinal, discrepâncias entre as políticas e a prática da sociedade-alvo podem revelar vulnerabilidades significativas em termos de conformidade legal e, por conseguinte, podem suscitar a necessidade de o possível comprador ou investidor tomar certas precauções no momento da negociação dos documentos definitivos da operação.

DOCUMENTOS DEFINITIVOS

Concluída a auditoria legal e iniciada a fase de negociação, é fundamental que o potencial comprador ou investidor considere a inclusão de cláusulas específicas que enderecem aspectos relacionados à responsabilidade civil do provedor de aplicações e à sua conformidade legal com o MCI. Ilustrativamente, o potencial investidor, por intermédio de condições precedentes¹, pode exigir que a consumação da operação esteja subordinada à estruturação ou aprimoramento das políticas próprias de moderação de conteúdo pela *target* provedora e/ou à resolução de conflitos com terceiros prejudicados pelo conteúdo veiculado nas plataformas digitais.

Alternativamente, caso não seja de interesse do potencial comprador ou investidor postergar o fechamento da operação e o condicionar à verificação de determinados fatos ou à prática de algum ato pelo provedor de aplicação – haja vista que a função precípua das condições precedentes está relacionada ao diferimento da eficácia do negócio para o fechamento da operação –, podem-se avençar, no contrato de compra e venda de participações societárias, obrigações pós-fechamento. Trata-se de outro mecanismo eficaz de proteção do comprador ou investidor, utilizado, notadamente em aquisições parciais, para estabelecer compromissos claros a serem cumpridos pela *target* após o fechamento da transação, dentro de um prazo, comumente, acordado entre as partes.

Nessa perspectiva, o potencial comprador ou investidor pode exigir que o provedor elabore e implemente de forma eficaz tais políticas em um prazo que o

¹ As condições precedentes correspondem a “determinadas exigências próprias do contrato de alienação de ações/quotas que determinados deveres ou ‘condições’ (em sentido lato) sejam previamente cumpridos por uma das partes, antes da chamada ‘data do fechamento’” (MARTINS-COSTA, Fernanda Mynarski. Condição suspensiva: função, estrutura e regime. São Paulo: Almedina, 2017, p. 93).

incentive a adequar-se às necessidades identificadas na auditoria legal, sob pena de a *target* ou os sócios-vendedores incorrerem, por exemplo, em multas em caso de inadimplemento de tais obrigações. Igualmente, é possível endereçar, contratualmente, a obrigatoriedade de criação ou aperfeiçoamento de canais internos de gestão de denúncias ou de ordens judiciais, ou mesmo o aprimoramento das práticas e da organização internas no que concerne ao gerenciamento da remoção de conteúdos de terceiros. Tais medidas almejam garantir que a sociedade-alvo tenha mecanismos eficazes para lidar com conteúdos inadequados e, assim, mitigar o risco de futuras responsabilizações ou sanções legais.

Destacam-se, ademais, as cláusulas de declarações e garantias e de indenização como um dos principais mecanismos de alocação de riscos posto à disposição das partes.

A cláusula de declarações e garantias constitui “uma técnica contratual por meio da qual as partes fazem afirmações positivas ou negativas sobre diversos aspectos do bem objeto do negócio, cuja veracidade e exatidão são garantidas pela parte que presta tais afirmações”². No mais das vezes, tais disposições são estipuladas em conjunto com uma cláusula de indenização, por meio da qual o contratante que presta as declarações e garantias obriga-se a indenizar e a manter a outra parte indene de perdas por ela eventualmente sofridas em virtude de qualquer violação, falsidade, omissão, erro, inadequação ou inexatidão das declarações e garantias.

No contexto de uma operação de M&A envolvendo provedores de aplicações de internet, o comprador ou investidor pode exigir, por exemplo, que a *target* ou os sócios-vendedores prestem declarações e garantias específicas relacionadas à existência de políticas de moderação de conteúdo, bem como a ausência de

2 GREZZANA, Giacomo. A cláusula de declarações e garantias em alienação de participação societária. São Paulo: Quartier Latin, 2019, p. 19. Segundo o autor, as “principais declarações e garantias abrangem (i) existência e regular constituição da sociedade e suas subsidiárias, (ii) titularidade plena das ações ou quotas da sociedade-alvo, (iii) inexistência de restrições ao direito de voto, dividendos e demais direitos da relação societária, (iv) inexistência de efeitos adversos e não violação de contratos ou leis pela transferência da participação, (v) exatidão das demonstrações financeiras da sociedade e contabilização de acordo com princípios geralmente aceitos, (vi) cumprimento de normas tributárias e previdenciárias pela sociedade-alvo, (vii) cumprimento de normas trabalhistas, (viii) cumprimento de normas ambientais e detenção de todas as licenças ambientais necessárias ao funcionamento da sociedade, bem como o correto cumprimento de suas condicionantes, (ix) cumprimento dos contratos da sociedade com clientes, fornecedores e prestadores de serviço, (x) titularidade de todos os ativos de propriedade intelectual necessários ao desempenho das atividades sociais ou detenção de licenças sobre os mesmos, (xi) situação da sociedade com relação a litígios em curso, (xii) detenção de autorizações regulatórias e governamentais para exercer as atividades da sociedade-alvo, (xiii) contratação de apólices de seguro suficientes para conduzir os negócios sociais e quitação em dia dos respectivos prêmios, (xiv) propriedade sobre bens móveis e imóveis da sociedade e, cada vez mais, tem-se incluído também declarações sobre (xv) observância da legislação anticorrupção” (GREZZANA, Giacomo. A cláusula de declarações e garantias em alienação de participação societária. São Paulo: Quartier Latin, 2019, p. 63).

processos judiciais ou reclamações extrajudiciais relacionadas a violações de direitos autorais ou intimidade.

É essencial, ainda, que o comprador ou investidor considere a inclusão de disposições que estabeleçam a obrigação dos sócios alienantes das participações societárias de indenizá-lo por eventuais perdas sofridas por aquele, resultantes da violação das declarações e garantias. As cláusulas de indenização, em conjunto com as declarações e garantias, colaboram para a equânime divisão dos riscos entre as partes envolvidas na operação, garantindo que o comprador ou investidor não seja responsabilizado por questões que já existiam antes de seu ingresso no quadro societário e lhe proporcionando uma maior segurança e proteção contra eventuais contingências legais após o fechamento da operação.

CONCLUSÃO

O regime legal de responsabilidade civil do provedor de aplicações de internet, previsto no MCI, deve ser um ponto de atenção especial para potenciais compradores ou investidores em operações de M&A envolvendo sociedades desse segmento de mercado. Nesse contexto, a análise meticulosa da *target* durante a auditoria legal e a inclusão de cláusulas específicas no contrato de compra e venda de participação societária são medidas fundamentais para mitigar os riscos inerentes à atividade da sociedade-alvo e garantir que a transação seja exitosa.

Conforme exposto acima, a relevância da auditoria legal aprofundada está em identificar e avaliar os riscos e contingências relacionados à atividade e às operações da *target* e propor soluções. Como visto, a análise deve abranger a verificação de processos e reclamações extrajudiciais, com o fim de identificar possíveis responsabilidades futuras, a investigação de reclamações relacionadas à violação de direitos autorais, intimidade e outros conteúdos sensíveis, e a avaliação de eventuais políticas internas de moderação de conteúdo existentes, para verificar sua conformidade com o MCI e as melhores práticas do mercado.

Já no que tange à estruturação do contrato de compra e venda de participação societária, é recomendável a inclusão de previsões que resguardem o comprador ou investidor, tais como: (i) condições precedentes, as quais podem subordinar o fechamento da operação à implementação de medidas de conformidade com o MCI ou ao aprimoramento das políticas internas relevantes, por exemplo; (ii) obrigações pós-fechamento que determinem a implantação de políticas efetivas de moderação de conteúdo publicados por terceiros e outros mecanismos de proteção dentro de um prazo pré-estipulado no contrato; (iii) declarações e garantias

relacionadas à existência de políticas de moderação de conteúdo e à ausência de processos judiciais ou reclamações extrajudiciais; e (iv) obrigação de indenizar, estabelecendo a responsabilidade do vendedor por perdas decorrentes de violações das declarações e garantias prestadas.

A observância das cautelas mencionadas neste artigo é, em suma, fundamental para que o potencial comprador de uma sociedade provedora de aplicações de internet possa realizar uma transação segura e bem-sucedida. Atentar-se à responsabilidade civil do provedor, no contexto do MCI, e às cláusulas e condições necessárias para a correspondente proteção permitirá ao comprador salvaguardar seus interesses e minimizar os riscos inerentes à aquisição da *target*.

REFERÊNCIAS

GREZZANA, Giacomo. A cláusula de declarações e garantias em alienação de participação societária. São Paulo: Quartier Latin, 2019.

MARTINS-COSTA, Fernanda Mynarski. Condição suspensiva: função, estrutura e regime. São Paulo: Almedina, 2017.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda., 2016.

COMPLIANCE E TRANSPARÊNCIA: A IMPORTÂNCIA HISTÓRICA E FUTURA DO MCI DIANTE DO DESENVOLVIMENTO TECNOLÓGICO

Giovanni Paolo Falcetta
Laís Cury Rezende

Em 2024 completa 10 anos desde a entrada em vigor do Marco Civil da Internet (MCI) – a Lei nº 12.965/2014. O nome “Marco” condiz substancialmente com o que a lei foi capaz de alcançar, pois funcionou como uma ferramenta que permitiu (e promoveu) o desenvolvimento regulatório no âmbito tecnológico. Hoje, mais do que nunca, a legislação deve acompanhar os avanços de tecnologia, e o MCI foi um ponto-chave nesse sentido.

Do ponto de vista de compliance, o MCI promoveu transparência e governança no âmbito governamental, bem como estabeleceu esses dois princípios como diretrizes básicas do gerenciamento da *internet* no Brasil.

Com esse foco, este artigo mostrará como o MCI foi um importante paradigma regulatório, como ele amparou e segue auxiliando no desenvolvimento da transparência e da governança (pública e privada) no Brasil. Por fim, irá provocar e discutir a importância de esses marcos regulatórios continuarem avançando em linha com o avanço tecnológico mundial.

MCI COMO IMPORTANTE PARADIGMA REGULATÓRIO

A *internet* para fins comerciais passou a ser utilizada no Brasil por volta de 1995. Com ela, surgiram questionamentos e preocupações quanto à utilização de dados no mundo virtual, prevenção de ilícitos cibernéticos (que infelizmente continuam até hoje) e como tornar a *internet* segura e democrática.

Nesse âmbito, o MCI teve como objetivo regular direitos, deveres e garantias no uso da *internet*, visando a mitigação dos riscos gerados por essa. Para isso, o MCI estabeleceu normas sobre como deve se dar o uso dos dados na *internet*, as obrigações dos provedores de *internet* no tratamento de conteúdo, o estabelecimento da liberdade de expressão e do acesso à informação como princípio do uso da *internet*, dentre diversas outras previsões essenciais. Isso trouxe benefícios que tornam o MCI um marco.

Ao regulamentar o universo virtual, o MCI trouxe segurança e permitiu que essa ferramenta fosse explorada para alcançar fins públicos que ajudam cidadãos e empresas no Brasil. A utilização da *internet* para esse fim não seria possível sem que o virtual estivesse regulado e sob o escrutínio legal. Esse ponto será mais explorado em outro tópico, porém ele é relevante neste momento para o estabelecimento do MCI como marco. Isso porque, um desses fins públicos, é a divulgação e acesso à informação e transparência. Muitos podem pensar que a Lei de Acesso à Informação (LAI) seria o verdadeiro marco nesse ponto da transparência, pois foi a lei que estabeleceu o direito de acesso à informação. Não obstante, apesar de a LAI ter sido, sem sombra de dúvida, uma das mais relevantes nesse âmbito, o ponto crucial é que o MCI permitiu, ao regular a *internet*, que essa fosse tratada como uma fonte de informações públicas, ao torná-la um recurso (um pouco mais) seguro. Isso ampliou o espectro do direito de acesso à informação, que a *internet* provê uma gama maior e de forma mais rápida. Sem a *internet* (regulada), o acesso à informação ficaria dificultado e limitado.

Em segundo lugar, ao endereçar as questões basilares da gestão da *internet*, o MCI permitiu o aprofundamento da discussão regulatória nesse âmbito. Um exemplo disso é a proteção de dados. Esse ponto da segurança de dados havia sido endereçado no MCI, mas de forma incipiente. A Lei Geral de Proteção de Dados (LGPD) veio e então aprofundou a regulamentação do uso de dados no Brasil. Mas, esse aprofundamento pela LGPD só pôde ser alcançado uma vez que as questões basilares já tivessem sido endereçadas – e isso havia sido feito pelo MCI.

Em resumo, esses dois exemplos mostram como o MCI viabilizou conquistas que não teriam sido possíveis sem ele, e ajudou no desenvolvimento da regulamentação da internet no Brasil. O Brasil é hoje visto como referência pela qualidade e confiabilidade das informações públicas, e pelo fato de permitir acesso fácil à informação. E isso – apesar das diversas empreitadas e tentativas de órgãos reguladores, desde 2003, de desenvolver e promover transparência – foi possível com a ajuda do MCI, em 2014. Vamos explorar esse ponto da transparência mais a fundo.

COMPLIANCE, TRANSPARÊNCIA E GOVERNANÇA AGRADECEM

Uma vez estabelecida a relevância do MCI como marco, fundamental aprofundar a sua importância no ponto da transparência e compliance.

O fato de o MCI ter estabelecido essa primeira regulamentação da internet significou um avanço por si só no que tange a transparência. Isso porque, o MCI, ao estabelecer direitos e garantias no âmbito virtual, trouxe segurança e permitiu que essa ferramenta fosse explorada para alcançar alguns fins públicos que ajudam cidadãos e empresas no Brasil.

Nessa linha, o MCI indicou a promoção do acesso à informação como objetivo da norma. Além disso, o estabelecimento da transparência e de mecanismos de governança são também indicados como diretrizes para o desenvolvimento da internet no Brasil:

Art. 4º A disciplina do uso da internet no Brasil tem por **objetivo a promoção**: (...) II - **do acesso à informação**, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos
(...)

Art. 24. **Constituem diretrizes** para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil: I - **estabelecimento de mecanismos de governança multiparticipativa, transparente**, colaborativa e democrática, com a **participação do governo, do setor empresarial**, da sociedade civil e da comunidade acadêmica (...)¹

O que isso significou foi que a internet passou a ser um local virtual (*website*, no inglês) que condensa informações de diversas fontes. Isso permitiu que a internet passasse a ser um mecanismo de comunicação e acesso à informação em uma escala sem precedentes. Do ponto de vista de compliance e transparência,

1 Lei 12.965/2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm

isso foi relevantíssimo e contribuiu para o desenvolvimento de mecanismos de compliance nas empresas.

Um exemplo é a facilidade de pesquisar, online, as informações societárias e corporativas de empresas, via os sites das juntas comerciais. Isso permite que procedimentos de *know your client* sejam executados de forma eficiente e rápida. Em um ‘clique’, pode-se saber quem é a cliente, sua Classificação Nacional das Atividades Econômicas (CNAE) – podendo já fazer uma verificação cruzada com o produto/serviço que oferece –, seu Cadastro Nacional da Pessoa Jurídica (CNPJ) – compreendendo se está ativo ou tem alguma restrição –, seus sócios e administradores.

Diretamente relacionado a isso – porém de forma mais ampla – está o acesso a informações de mídia. É estabelecida a recomendação, do ponto de vista de compliance, que empresas identifiquem quem são seus terceiros, e façam as devidas diligências e *background checks* nos possíveis e futuros parceiros de negócio. Isso, com a internet, se tornou fácil e significativamente instantâneo. Anteriormente, só era possível verificar ou ter acesso a mídia em cópia física de jornais. Hoje, com um *enter* no teclado, e com diversas ferramentas que compilam e organizam as informações da internet em um só lugar, as empresas obtêm informações quanto àquele terceiro instantaneamente, permitindo uma parcela da avaliação de risco de forma rápida e eficiente.

Outro exemplo é o acesso a informações perante órgãos públicos. Esse acesso, tradicionalmente, só era possível por meio de protocolo físico perante os órgãos. Hoje em dia uma ampla gama dessas informações pode ser solicitada ou obtida online (com exceção, naturalmente, de informações mais antigas que podem não estar disponíveis em razão do tempo decorrido). A pesquisa de processos judiciais é um exemplo claro disso. Graças ao trabalho do Conselho Nacional de Justiça (CNJ) que disponibilizou o sistema “PJe” a todos os estados no Brasil, os processos judiciais atualmente correm de forma eletrônica. A qualquer momento as partes podem verificar o status ou protocolar uma petição online. Também, empresas que estão realizando investigações internas, ou negociando acordos de leniência, e precisam, por exemplo, de informações de contratos públicos, ou licitações específicas, podem obter muitas informações no site do órgão responsável pela licitação, ou do órgão com o qual o contrato foi firmado. Claro, esse banco de dados não é infalível ou inteiramente completo, mas o avanço, e o benefício às empresas decorrente disso, é visível.

A internet regulada também permite que empresas conduzam as chamadas “*open source investigations*”, que nada mais são do que verificações feitas puramente com base em informações públicas ou sites abertos. Hoje em dia, a gama

de informações disponíveis online faz com que essas investigações possam trazer as informações essenciais para tomada de determinadas decisões comerciais (tais como, contratar um terceiro, seguir com uma parceria etc.).

Assim, todas essas conquistas, e o alcance da internet atualmente, foi possível graças à regulamentação desse meio de comunicação e meio de garantia de transparência.

Um comentário aqui é relevante. Não se está propondo aqui que a regulamentação da internet no Brasil tornou confiável toda e qualquer informação na internet – porque sabemos que isso não é verdade. A conquista do MCI não foi – nem seria – essa confiabilidade máxima, mas sim o fato de que a internet passou a estar sob o escrutínio legal. Isso permite que qualquer um exija – mesmo que judicialmente, se necessário – o cumprimento de normas ali previstas, o que contribui para a confiabilidade.

O MCI também contribuiu para um outro ganho nesse âmbito de transparência e governança. Isso porque ele foi uma ferramenta para promoção da transparência e boa governança públicas. Ao fazer isso, o poder público se colocou sob o escrutínio da população, e estabeleceu um padrão alto nesse âmbito de transparência e compliance. Indiretamente, o que isso traz é a legitimidade para o governo exigir que empresas sejam também transparentes.

AVANÇOS TECNOLÓGICOS E REGULAMENTAÇÃO

Para concluirmos, um apelo é importante. Vimos nos demais tópicos porque o MCI foi tão importante para a história de compliance e transparência no Brasil, e isso é visto até hoje, inclusive internacionalmente. A conquista obtida pelo MCI, porém, não pode ser vista como estanque, nem ser interpretada como atestado de que regulamentações adicionais não são necessárias. Muito pelo contrário. A legislação sempre precisou acompanhar os avanços tecnológicos e, conforme tratado anteriormente, isso é um dos motivos pelos quais o MCI foi um marco.

Contudo, a internet se desenvolve cada vez mais, e de forma cada vez mais rápida. Em menos de 30 anos, fomos de internet discada a internet na ponta dos dedos e metaverso. O metaverso e o uso de inteligência artificial demandarão uma regulamentação e controle muito rígidos, pois implicam em um novo âmbito de interações sociais, comerciais e corporativas². Assim, quaisquer condutas que se deem nessas searas precisam estar sob o escrutínio legal e dos órgãos de controle.

2 Para uma análise mais detalhada do tema: KIM, Shin Jae; FACETTA, Giovanni Paolo; MIKULETIC NETO, Franco. Qual o valor do NFT? Riscos e possibilidades no metaverso – NFTs e a relativização do valor. In: SEREC, Fernando Eduardo. Metaverso: Aspectos Jurídicos. São Paulo: Grupo Almedina (Portugal), 2022.

Porém, os avanços tecnológicos são tão rápidos, que as oportunidades para irregularidades são enormes, já que a regulamentação não consegue ser tão rápida quanto o avanço tecnológico. Em 2017, a revista americana “*The Atlantic*” anunciou o aumento de fraudes no âmbito de criptomoedas, principalmente naquele momento em que criptomoedas estavam ainda em fase embrionária e, portanto, pessoas não sabiam lidar com elas³. Acelerando para quatro anos depois, isso seguia sendo um problema aqui no Brasil, a exemplo da Operação Kryptos, que envolveu suspeita de fraude bilionária com criptomoedas, por meio de uma pirâmide financeira (o famoso “*Ponzi scheme*”).⁴

Esses são alguns poucos exemplos do porquê a atualização constante da legislação é essencial, para coibir abusos e mitigar riscos. E esse é um risco que afeta a todos, pessoas físicas, empresas, governo – todos estão expostos aos riscos pela ausência de controle do que ocorre no mundo virtual. Até que isso ocorra, precisamos todos usufruir dos benefícios e conquistas obtidas até o momento, mas, ao mesmo tempo, pensar em formas de nos proteger e mitigar esses riscos.

REFERÊNCIAS

ABDALA, Victor. Polícia Federal faz operação contra fraudes com criptomoedas. Ago 2021. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-08/policia-federal-faz-operacao-contrafraudes-com-criptomoedas>. Acessado em: 7 de mar. de 2024.

De MIRANDA, Wallace Vieira, e ZAGANELLI, Juliana Costa. Marco Civil da Internet. Marco Civil da Internet e Política Pública de Transparência: uma Análise da E-Democracia e do Compliance Público. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/4921>. Acessado em: 7 de mar. de 2024.

KIM, Shin Jae; FACETTA, Giovanni Paolo; MIKULETIC NETO, Franco. Qual o valor do NFT? Riscos e possibilidades no metaverso – NFTs e a relativização do valor. In: SEREC, Fernando Eduardo. Metaverso: Aspectos Jurídicos. São Paulo: Grupo Almedina (Portugal), 2022.

3 Disponível em: <https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/>. Acessado em 7 de mar. de 2024.

4 Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-08/policia-federal-faz-operacao-contrafraudes-com-criptomoedas>. Acessado em 7 de mar. de 2024.

MORRIS, David Z. The Rise of Cryptocurrency Ponzi Schemes. Mai 2017. Disponível em: <https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/>. Acessado em: 7 de mar. de 2024.

SULLIVAN, Kevin. Anti-money laundering in a nutshell – awareness and compliance for financial personnel and business managers. Apress, Nova Iorque, 2015, p. 34.

O POTENCIAL DA INTELIGÊNCIA ARTIFICIAL PARA MOLDAR O FUTURO DO COMÉRCIO INTERNACIONAL BRASILEIRO

Shin Jae Kim
Isabelle Ruiz Guero

INTRODUÇÃO

Seria impensável, até uns anos atrás, imaginar receber, na nossa casa, um produto do outro lado do globo, a um clique de botão em plataformas online e *marketplaces* internacionais. O avanço tecnológico certamente impulsionou a criação de um novo mercado gigantesco, que acabou por beneficiar os consumidores que passaram a ter acesso ao mercado global. A Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI), que completou 10 anos, representou uma evolução importante para a garantia da segurança jurídica desse mercado. Isso porque, apesar de não tratar da matéria em sentido estrito e direto, o MCI disciplina princípios aplicáveis a tudo o que ocorre na internet em âmbito nacional, inclusive no e-commerce, incidindo também sobre operações que circundam a cadeia de fornecimento desses serviços no âmbito online – como disposições sobre proteção à privacidade, responsabilidade civil por conteúdo de terceiros etc.

Foi com esse cenário de maior segurança jurídica que o comércio eletrônico passou a ser um mercado cada vez maior e mais presente na vida dos brasileiros. Isso impõe crescente demanda por maior celeridade e redução de burocracia e o papel da inteligência artificial (IA) no comércio internacional torna-se cada vez mais crucial.

Assim, a IA é considerada um dos pilares da quarta revolução industrial, que engloba também um amplo sistema de tecnologias avançadas como robótica, internet das coisas e computação em nuvem, redefinindo as formas de produção e os modelos de negócios no Brasil e no mundo.

Embora a IA seja uma tecnologia de uso geral com grande potencial para estimular a inovação, seu impacto no comércio internacional é especialmente marcante, revelando um poder de revolucionar a forma com que os negócios internacionais são conduzidos e impulsionar a transformação econômica, especialmente em países em desenvolvimento, como o Brasil¹.

A *Internacional Trade Administration*, agência do Departamento de Comércio americano, projeta um aumento significativo – cerca de 15 trilhões de dólares – no comércio global até 2030, impulsionado pelo uso de IA². Esse prognóstico reflete não apenas o impacto esperado, mas também a necessidade de explorar e entender profundamente as contribuições da IA para o comércio internacional, principalmente em contextos nacionais específicos, como o Brasil.

Tendo em vista os 10 anos do MCI, um dos maiores marcos legais da regulação de uma nova tecnologia no país, e que serviu como importante instrumento para a garantia da segurança jurídica no e-commerce, este artigo visa contribuir para esse debate com um olhar para o futuro, explorando os benefícios da aplicação da IA no comércio exterior, além de examinar como essa tecnologia pode ajudar países em desenvolvimento a diversificar suas economias, e analisar como a Receita Federal do Brasil a tem aplicado em seus processos aduaneiros para maximizar sua eficiência.

OS BENEFÍCIOS DA APLICAÇÃO DE IA NO COMÉRCIO EXTERIOR

A aplicação da IA no comércio exterior oferece uma ampla variedade de benefícios. A IA pode otimizar processos aduaneiros rotineiros, ao analisar dados e documentos, detectando anomalias e riscos potenciais, resultando em um desembaraço aduaneiro mais eficiente e preciso, e melhorando também a observância às medidas de segurança e conformidade.

Na esfera privada, a IA é uma grande aliada para interpretar informações de mercado, tendências de consumo e regulamentações internacionais, fornecendo insights valiosos para a tomada de decisões estratégicas, garantindo competitividade no mercado global. Esses dados podem versar sobre automação de processos envolvendo cadeia de suprimentos e equipamentos utilizados, prevendo, por exemplo, quando máquinas precisam de manutenção, monitoramento da

1 MISHRA, S.; KOOPMAN, R.; DE PRATO, G. et al. AI specialization for pathways of economic diversification. *Scientific Reports* volume 13, Article number: 19475. Nature, 2023. DOI <https://doi.org/10.1038/s41598-023-45723-x>.

2 ADMINISTRATION, Internacional Trade. Artificial Intelligence. Disponível em: <https://www.trade.gov/artificial-intelligence>.

temperatura de cargas sensíveis, rastreamento de carga e análise de dados de estoque, transporte e demanda, ajudando a otimizar operações de logística³.

Além disso, pode ser um grande recurso para identificar oportunidades comerciais. Ao analisar bases de dados de diversas fontes, incluindo relatórios de mercado e redes sociais, os algoritmos de IA podem identificar tendências emergentes, preferências dos consumidores e exigências do mercado. Isso permite que as empresas desenvolvam estratégias de marketing direcionadas, identifiquem novos mercados de exportação e adaptem as suas ofertas de produtos para atender às necessidades específicas dos clientes.

Em relação ao comércio internacional de serviços, instituições financeiras utilizam a tecnologia para auxiliar na análise de risco de pagamentos internacionais, prevendo taxas de câmbio, possíveis atividades fraudulentas, reduzindo tempo de processamento de transações, entre outros⁴.

Em suma, as soluções envolvendo IA podem ser implementadas em todas as fases produtivas, desde pesquisa e desenvolvimento, até produção, distribuição, reparação e reciclagem⁵, resultando em operações mais céleres, mitigação de riscos em toda a cadeia de suprimentos e custos operacionais, e maximização do crescimento econômico, em última instância⁶.

COMO A IA PODE AJUDAR A DIVERSIFICAR BENS E SERVIÇOS EM PAÍSES EM DESENVOLVIMENTO

A utilização estratégica da IA pode fortalecer indústrias tradicionais, especialmente nos setores exportadores, e identificar novas oportunidades de crescimento em mercados emergentes⁷.

Por exemplo, na agricultura brasileira, a IA pode auxiliar na análise de dados agrícolas em tempo real, prevendo consequências condições climáticas, uso da

3 EXTERIOR, Portal do Comércio. O uso de inteligência artificial no comércio exterior. Disponível em: <https://portaldocomercioexterior.com.br/o-uso-de-inteligencia-artificial-no-comercio-exterior/>.

4 Ferencz, J., J. López González and I. Oliván García (2022), “Artificial Intelligence and international trade: Some preliminary implications”, OECD Trade Policy Papers, No. 260, OECD Publishing, Paris, <https://doi.org/10.1787/13212d3e-en>.

5 MISHRA, Saurabh; ZACCARIA, Andrea; RODARTE, Israel Osorio. Artificial intelligence (AI) can help developing economies diversify. The Trade Post, World Bank, 2024. Disponível em: <https://blogs.worldbank.org/trade/artificial-intelligence-ai-can-help-developing-economies-diversify?deliveryName=DM209753>.

6 EMIX. Inteligência artificial no comércio exterior: o que é e onde está presente?. 2023. Disponível em: <https://emix.com.br/inteligencia-artificial-comercio-exterior/#:~:text=Segmentos-,Intelig%C3%AAncia%20artificial%20no%20com%C3%A9rcio%20exterior%3A%20o%20que%20%C3%A9%20e%20onde,e%20monitorando%20cadeias%20de%20suprimentos>.

7 MISHRA, Saurabh; ZACCARIA, Andrea; RODARTE, Israel Osorio. *loc. cit.*

água, saúde do solo e outros fatores variáveis. Isso pode ajudar os agricultores a aumentar o rendimento e a qualidade da safra e identificar o que plantar, como, onde e quando⁸.

O setor médico-hospitalar, de grande importância estratégica para o Brasil, também pode se beneficiar com a IA, por meio da aplicação em diagnósticos médicos, prevenção de surtos de doenças e desenvolvimento de novos medicamentos, entre outros⁹.

Além disso, a IA pode ser um importante aliada para a descoberta de oportunidades de diversificação de bens e serviços, bem como destinos, auxiliando a diversificar as receitas de exportação a longo prazo.

A IA também pode ser um ativo importante para além das empresas, auxiliando governos a projetar políticas comerciais melhores. Diante de choques às cadeiras globais de valor por eventos inesperados, como desastres naturais, ataques cibernéticos ou até mesmo crises sanitárias, a IA é útil para analisar dados em tempo real e fornecer informações mais oportunas e granulares aos agentes econômicos e aos formuladores de políticas públicas, bem como ajudar a entender o impacto da incerteza ou de choques específicos. Ao utilizar a IA para debruçar sobre essas preocupações, tem-se subsídios para a criação de estratégias industriais e de desenvolvimento econômico.

O DESENVOLVIMENTO DE SOLUÇÕES DE IA PARA A OTIMIZAÇÃO DOS PROCESSOS ADUANEIROS BRASILEIROS

A Receita Federal Brasileira (RFB), enquanto autoridade aduaneira, ciente dos benefícios decorrentes das ferramentas de IA, desenvolveu, em 2014, a primeira inteligência artificial de uso generalizado em suas unidades aduaneiras: o Sistema de Seleção Aduaneira por Aprendizado de Máquina (Sisam)¹⁰.

O Sisam monitora e “aprende” com o histórico de Declarações de Importação (DIs) do Sistema Integrado de Comércio Exterior (Siscomex) e aumenta a eficiência

8 Ferencz, J., J. López González and I. Oliván García (2022), “Artificial Intelligence and international trade: Some preliminary implications”, OECD Trade Policy Papers, No. 260, OECD Publishing, Paris, <https://doi.org/10.1787/13212d3e-en>.

9 FERENCZ, J.; GONZÁLEZ, J. LÓPEZ; e GARCÍA, I. OLIVÁN. Artificial Intelligence and international trade: Some preliminary implications. OECD Trade Policy Papers, No. 260, 2022. OECD Publishing, Paris. Disponível em <https://doi.org/10.1787/13212d3e-en>.

10 FILHO, Jorge Eduardo de Schoucair Jambeiro. Inteligência Artificial no Sistema de Seleção Aduaneira por Aprendizado de Máquina. Prêmio de Criatividade e Inovação da RFB 2015. Receita Federal do Brasil, 2016. Disponível em: <http://bibliotecadigital.economia.gov.br/handle/123456789/522897>.

do despacho aduaneiro, na medida em que há redução do percentual de mercadorias verificadas no despacho aduaneiro de importação e, concomitantemente, redução de evasão fiscal na importação e o descumprimento de exigências administrativas¹¹.

O Sisam tanto aumenta a precisão da seleção de DIs para canais de conferência quanto ajuda a escolha de mercadorias individuais para verificação. Ele analisa os itens de cada adição dos DIs e, para todos eles, calcula a probabilidade da presença de vários tipos de erros, como referentes a classificação fiscal, erros de origem, em regimes tributários, em acordos tarifários, de falta de licenciamento e nas alíquotas dos tributos incidentes sobre a importação, além de direitos antidumping. Ele também indica quanto, em valor, esses erros podem representar de perda para o Fisco, detalhando as consequências tributárias e não tributárias de cada dos valores envolvidos. Com isso, o Sisam atua na otimização da fiscalização, tanto decidindo automaticamente quais verificações devem ser realizadas quanto apoiando fiscais¹².

Há também outros programas desenvolvidos pela RFB que utilizam IA, como o Analisador Inteligente e Integrado de Transações Aduaneiras (Aniita) e o Programa de Acompanhamento em Tempo Real das Operações Aduaneiras (PATROA).

O Aniita, cujo desenvolvimento iniciou-se em 2011, consiste em um sistema para gerenciamento de riscos aduaneiros, em que a alimentação de dados desse sistema é baseada em outros sistemas e na alimentação pela própria fiscalização aduaneira¹³.

Por sua vez, o PATROA, lançado em 2017, é um sistema adicional que também tem como objetivo a gestão de riscos aduaneiros. Com base nas informações aduaneiras, o próprio sistema analisa e decide sobre o acionamento da fiscalização ou não. O PATROA pode invocar a Aniita e o Sisam para obter a análise detalhada de uma transação e, em seguida, decidir se um agente deve receber um e-mail ou uma mensagem instantânea em seu telefone celular¹⁴.

Assim, é possível notar que os sistemas aduaneiros desenvolvidos pela RFB, mediante o uso de IA, visam buscar solução de gerenciamento de risco e eficiência operacional. Essa estratégia abre o caminho para uma rede de administração alfandegária global mais integrada e conectada, e posiciona o Brasil como um participante proativo no futuro das operações aduaneiras¹⁵.

11 *Ibid.*

12 *Ibid.*

13 COUTINHO, Gustavo Lacerda. Aniita – uma abordagem pragmática para o gerenciamento de risco aduaneiro baseada em software. Receita Federal do Brasil, 2012. Disponível em: <http://repositorio.enap.gov.br/handle/1/4607>.

14 COUTINHO, Gustavo Lacerda; e FILHO, Jorge Eduardo de Schoucair Jambeiro. Brazil's new integrated risk management solutions. WCO, 2018. Disponível em: <https://mag.wcoomd.org/magazine/wco-news-86/brazils-new-integrated-risk-management-solutions/>.

15 JUNQUEIRA, Carla Amaral de Andrade. Recent Customs Reforms in Brazil. Global Trade and Customs Journal Volume 18, Issue 11/12 (2023) pp. 450 – 453. Disponível em: <https://doi.org/10.54648/gtcj2023055>.

CONCLUSÃO

É evidente a atmosfera de transformação econômica e tecnológica sem precedentes. O aniversário de 10 anos do MCI é uma importante data para lembrarmos os avanços tecnológicos significativos vividos desde então, e nos convida a pensar em um comércio eletrônico para o futuro. À medida que governos e empresas reconhecem o potencial da IA, testemunhamos sua utilização como instrumento para moldar o futuro do comércio exterior, prometendo não apenas otimizar os processos existentes, mas também criar novas possibilidades de abordagem mais ágeis e eficientes para enfrentar desafios globais. Além disso, a iminência da IA tem o poder de reconfigurar os padrões do comércio mundial.

Para países em desenvolvimento, como o Brasil, o pleno aproveitamento do potencial da IA é crucial para impulsionar a competitividade e diversificar a economia, fortalecendo sua posição no mercado global.

A iniciativa da Receita Federal do Brasil em desenvolver sistemas baseados em IA para otimizar processos aduaneiros é um exemplo relevante de como governos podem liderar a transformação digital do comércio internacional. Esses esforços não apenas aumentam a eficiência operacional, como também fortalecem a segurança e conformidade das transações comerciais, beneficiando tanto as empresas quanto o desenvolvimento econômico, em seu sentido mais amplo.

No âmbito aduaneiro, há desafios que podem utilizar a IA como ferramenta de combate, visando melhorar a detecção de erros de classificação fiscal de mercadorias importadas e quantidades de mercadorias usando imagens de raios-x de containers, por exemplo, reduzindo consideravelmente o risco de contrabando, fraude e evasão fiscal. Soluções pensadas para prevenir a falsificação de documentos e investimentos nos agentes fiscais para capacitação são também fundamentais para garantir o bom funcionamento e simplificação dos procedimentos aduaneiros.

É essencial continuar investindo nesse formato de tecnologia para enfrentar os desafios emergentes no comércio internacional e colaborar, em escala global, para construir um sistema de comércio internacional mais resiliente, inclusivo e sustentável.

Capítulo 4

/Marco Civil da Internet e Resolução de Disputas

DIÁLOGOS ENTRE O CÓDIGO DE PROCESSO CIVIL DE 2015 E A INTERNET

Elias Marques de Medeiros Neto

Eugen Ehrlich sabiamente proclamou que o Direito é um mero lago em um Oceano de fatos. Nesse contexto, tanto o processualista como o legislador possuem a difícil missão de sempre adaptar e/ou transformar o sistema normativo diante das intermináveis mutações fáticas.

É nesse cenário que este artigo apresentará alguns pontos de diálogo entre o universo da internet e a legislação processual, tendo-se como objetivo demonstrar que possivelmente estamos no início de uma longa caminhada para adaptar os veículos do processo civil às infinitas evoluções da tecnologia.

O clássico processo civil, tido como ciência social prática voltada a instrumentalizar a satisfação do direito material a ser tutelado, precisa naturalmente conviver, nos tempos modernos, com uma realidade tecnológica avançada. O que exige, portanto, não só a adaptação profissional daqueles que militam nos pretórios, como também um olhar cauteloso sobre como zelar pela segurança jurídica e pelas garantias constitucionais em uma era cada vez mais regida por ferramentas virtuais.

O Código de Processo Civil de 2015 (CPC/2015), de certa forma, já entrou em vigor com previsões contemporâneas a esse inevitável movimento tecnológico. Mas, por certo, mesmo após a vigência do diploma processual, ocorreram inserções no Código inspiradas nas novas tecnologias; tudo de modo a se demonstrar que as adaptações normativas, com esse vetor de diálogo entre direito e novas tecnologias, vieram para ficar.

Um primeiro exemplo se encontra logo no artigo 193 do CPC/2015, que estipula que: “Os atos processuais podem ser total ou parcialmente digitais, de forma a permitir que sejam produzidos, comunicados, armazenados e validados por meio eletrônico, na forma da lei”.

E, em sintonia com os pilares fundamentais da publicidade e do contraditório, o art. 194 do CPC/2015 prescreve que:

Os sistemas de automação processual respeitarão a publicidade dos atos, o acesso e a participação das partes e de seus procuradores, inclusive nas audiências e sessões de julgamento, observadas as garantias da disponibilidade, independência da plataforma computacional, acessibilidade e interoperabilidade dos sistemas, serviços, dados e informações que o Poder Judiciário administre no exercício de suas funções.

Cada vez mais, na rotina do nosso contencioso, ocorrem comunicações e práticas de atos processuais através de plataformas virtuais, sendo que esses importantes arts. 193 e 194 se mostram bem frequentes no cotidiano forense.

Com preocupação quanto à segurança jurídica, o art. 195 do CPC/2015 orienta que:

O registro de ato processual eletrônico deverá ser feito em padrões abertos, que atenderão aos requisitos de autenticidade, integridade, temporalidade, não repúdio, conservação e, nos casos que tramitem em segredo de justiça, confidencialidade, observada a infraestrutura de chaves públicas unificada nacionalmente, nos termos da lei.

E, com a mesma diretriz, é a previsão do art. 197 do CPC/2015: “Os tribunais divulgarão as informações constantes de seu sistema de automação em página própria na rede mundial de computadores, gozando a divulgação de presunção de veracidade e confiabilidade”.

Para comprovar que a era da tecnologia já é um fator dominante para o modelo processual, o art. 246 do CPC/2015 prescreve que a citação deve ser feita preferencialmente por meio eletrônico:

A citação será feita preferencialmente por meio eletrônico, no prazo de até 2 (dois) dias úteis, contado da decisão que a determinar, por meio dos endereços eletrônicos indicados pelo citando no banco de dados do Poder Judiciário, conforme regulamento do Conselho Nacional de Justiça.

Aliás, o art. 246 do CPC/2015 tem forte ligação com a Portaria do Conselho Nacional de Justiça (CNJ) nº 46, a qual dita que, desde 1º de março de 2024, grandes e médias empresas devem se cadastrar no Domicílio Judicial Eletrônico, integrante do Programa Justiça 4.0 do CNJ, que tem como finalidade centralizar as comunicações de processos em uma única plataforma digital.

O art. 270 do CPC/2015, na mesma direção, estabelece que: “As intimações realizam-se, sempre que possível, por meio eletrônico, na forma da lei”.

Em aplaudido prestígio ao princípio da imediatidade do julgador com a prova oral produzida em audiência, o parágrafo terceiro do art. 385 do CPC/2015 possibilita a realização, por vídeo conferência, do depoimento pessoal de parte que reside em comarca diferente da que está tramitando o feito:

§ 3º O depoimento pessoal da parte que residir em comarca, seção ou subseção judiciária diversa daquela onde tramita o processo poderá ser colhido por meio de videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real, o que poderá ocorrer, inclusive, durante a realização da audiência de instrução e julgamento.

Com idêntica finalidade, para fins da prova testemunhal, é a previsão do parágrafo primeiro do art. 453:

§ 1º A oitiva de testemunha que residir em comarca, seção ou subseção judiciária diversa daquela onde tramita o processo poderá ser realizada por meio de videoconferência ou outro recurso tecnológico de transmissão e recepção de sons e imagens em tempo real, o que poderá ocorrer, inclusive, durante a audiência de instrução e julgamento.

Pode-se afirmar, aliás, que a prática de audiências e julgamentos virtuais tornaram-se muito frequentes na era pós pandemia relativa à Covid-19, razão pela qual o CNJ proferiu o Ato Normativo nº 0003090-74.2022.2.00.0000, de 21 de junho de 2022, para melhor reger a realização das videochamadas.

Ainda no ambiente das provas, o art. 441 do CPC/2015 expressamente admite o documento eletrônico: “Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica”.

Inegável que cada vez mais a produção de documentos ocorre nos ambientes virtuais, sendo certo que, não raro, importantes negociações acabam sendo realizadas e documentadas através de plataformas digitais.

Atento a isso, o art. 784 do CPC/2015 reconhece o documento eletrônico como título executivo, salientando, em seu parágrafo 4º, que: “Nos títulos executivos constituídos ou atestados por meio eletrônico, é admitida qualquer modalidade de assinatura eletrônica prevista em lei, dispensada a assinatura de testemunhas quando sua integridade for conferida por provedor de assinatura”.

Nunca é demais frisar que a segurança jurídica no manejo dos atos e negócios eletrônicos é estrutura fundamental para a higidez do procedimento executivo, de tal modo que se recomenda sempre o uso de plataformas digitais que possam conferir garantia de autenticidade das assinaturas a serem inseridas nos documentos.

Em aliança com a busca de efetividade e eficiência nos atos executivos, conforme previsões dos artigos 4º e 8º do CPC/2015, as técnicas de investigação patrimonial e de penhora, na era da internet, ganharam velocidade por meio dos famosos sistemas da família “Jud”, implementados pelo CNJ: Sisbajud, CCS-Bacen, Infojud, Infoseg, Renajud, SerasaJud, Sniper, SREI e Sistema Nacional de Gestão de Bens (SNGB).

A notória penhora online tem minuciosa previsão no art. 854 do CPC/2015 e é, sem dúvida, uma grande ferramenta para a célere busca de patrimônio do devedor no procedimento executivo:

Para possibilitar a penhora de dinheiro em depósito ou em aplicação financeira, o juiz, a requerimento do exequente, sem dar ciência prévia do ato ao executado, determinará às instituições financeiras, por meio de sistema eletrônico gerido pela autoridade supervisora do sistema financeiro nacional, que torne indisponíveis ativos financeiros existentes em nome do executado, limitando-se a indisponibilidade ao valor indicado na execução.

Os breves pontos de diálogo acima elencados entre o CPC/2015 e o mundo da internet não são exaustivos, tanto que as noticiadas recentes formas de as Cortes nacionais se organizarem para otimizar e realizar os seus trabalhos estão fortemente influenciadas pelos movimentos de automação e de aplicação de inteligência artificial (IA).

A busca de um Poder Judiciário 4.0 é regida por iniciativas de gestão de dados, categorização de atos processuais e otimização de atividades.

Segundo pesquisa do CNJ, houve um grande aumento no volume de projetos de IA no Poder Judiciário. Sendo que, em 2022, foram apontadas 111 iniciativas, com 53 Tribunais no país já aplicando formas avançadas de tecnologia para a prática de atos processuais.

O Janus, como exemplo, é uma solução que automatiza tarefas repetitivas e utiliza a IA para apoiar o julgamento de pedidos de candidatura e tentar agilizar na prestação de contas eleitorais.

Outro projeto é o Gemini, que agrupa processos por similaridade de tema nas unidades de primeiro e segundo grau da Justiça do Trabalho, podendo ajudar a acelerar os julgamentos.

Por sua vez, a Sofia, assistente virtual de atendimento (*chatbot*) nos juizados especiais do Tribunal de Justiça da Bahia, utiliza IA na triagem automática de processos.

O Amon, ainda em fase de teste, permite reconhecimento facial a partir de imagens e vídeos atendendo algumas necessidades da segurança interna do Tribunal.

Já o Toth, em fase de estudos, permitirá análise da petição inicial do advogado buscando recomendar a classe e os assuntos processuais a serem cadastrados no Processo Judicial eletrônico (PJe) durante a autuação.

A maioria das iniciativas do Poder Judiciário está voltada para o levantamento, a classificação e gestão de dados. Mas, não há dúvidas de que existem estudos para implementação de IA para auxiliar na elaboração de textos jurídicos, para reconhecer visualmente detentos, para identificar classe e assunto de processo a partir dos termos da petição inicial, para identificar e categorizar processos com semelhanças e para fins de identificação de relevância e/ou repercussão geral e para otimizar movimentos processuais.

Destaca-se, ainda, o Projeto Victor, fruto de uma parceria entre o Supremo Tribunal Federal (STF) e a Universidade de Brasília, o qual foi idealizado para auxiliar a Corte Suprema na análise dos recursos extraordinários, especialmente quanto à sua classificação em temas de repercussão geral de maior incidência.

No Superior Tribunal de Justiça (STJ), destaca-se o projeto Sócrates 2.0, concebido como uma plataforma composta por: (i) Sistema de Gerenciamento de Normas, (ii) Sistema de Gerenciamento de Controvérsias, (iii) Sistema de Gerenciamento de Modelos, (iv) Pesquisa Automática de Jurisprudência, (v) Pesquisa Automática de Doutrina; e (vi) Sistema de Gerenciamento de Acervo por Controvérsias.

Como visto, a era da tecnologia veio para transformar a rotina das atividades forenses, sendo que pontos de conexão entre o CPC/2015 e o universo da internet naturalmente não se limitam aos breves exemplos elencados nesse artigo.

E em um momento de celebração de aniversário do Marco Civil da Internet (MCI), sem prejuízo da importância magistral da Lei nº 12.965/2014 como um todo, destaca-se, para fins da instrumentalização dos atos processuais, a fundamental observância do artigo 3º, V, dessa norma: “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”.

Naturalmente, por fim, a evolução normativa do sistema processual prosseguirá, ainda que com atrasos, sempre buscando-se se adaptar às velozes mutações da tecnologia; em mais uma demonstração de que o direito, claro, é um mero lago em um oceano de fatos.

O VALOR PROBATÓRIO DE MENSAGENS ELETRÔNICAS NO PROCESSO DO TRABALHO

Maurício de Carvalho Góes
Marina Silveira Frank

INTRODUÇÃO

Todos sabem que o Marco Civil da Internet (MCI) representa um marco em termos de normatização das relações desenvolvidas e abrangidas, talvez, por uma das ferramentas mais utilizadas na vida das pessoas: a internet.

Nesse sentido, a internet acaba se configurando como um fato social e, por conseguinte, um fato jurídico (também, fato jurídico trabalhista).

Em se tratando especificamente de Direito do Trabalho, indubitavelmente, a internet produz efeitos significativos nas relações materiais de trabalho e, por consequência, no âmbito processual, na medida em que será a reclamação trabalhista a forma de instrumentalização da lide laboral.

Por isso, o presente artigo tem por objetivo principal abordar o tema, delimitando-o quanto ao valor probatório das mensagens eletrônicas no processo do trabalho, mormente a sua admissão, o cotejo com outras provas e o entendimento da atual jurisprudência sobre a utilização de provas dessa natureza.

A FASE PROBATÓRIA NO PROCESSO DO TRABALHO

Para a abordagem do valor probatório de mensagens eletrônicas no Processo do Trabalho, é necessário transitar entre os aspectos gerais envolvendo o tema da prova no processo judicial trabalhista, como também a sua utilização na forma digital.

No processo do trabalho, os meios de prova estão previstos na Consolidação das Leis do Trabalho (CLT), basicamente, nos artigos 818 a 830, indo ao encontro da concepção de que o processo do trabalho está calcado nos princípios da

celeridade e da simplicidade. Porém, considerando os poucos artigos destinados à fase instrutória do processo laboral, é necessário que seja utilizada a lei processual civil como fonte subsidiária, observados os requisitos exigidos no artigo 769 da CLT. Além disso, especificamente quanto à prova documental, a legislação trabalhista não possui item exclusivo envolvendo a matéria. O que ocorre é que a CLT faz referência a documentos, de maneira não organizada, em alguns artigos (777, 780, 787 e 830).

Quanto à fase de instrução processual, a CLT estabelece em seu art. 765 que os julgadores possuem ampla liberdade na direção do processo, podendo determinar qualquer diligência que seja necessária para o esclarecimento delas. Já no Código de Processo Civil (CPC), os arts. 369 e 370 regulamentam em mesmo sentido. O primeiro dispositivo refere que as partes possuem o direito de se utilizar de todos os meios legais, como também moralmente legítimos, ainda que não previstos no CPC, para provar a verdade dos fatos em que são fundados o pedido ou a defesa, a fim de influir na convicção do juiz. Já o segundo artigo estabelece que caberá ao julgador, de ofício ou em razão de requerimento de alguma das partes, determinar as provas necessárias ao julgamento do mérito da ação. São nesses dispositivos, portanto, que se encontra o fundamento para o uso de provas digitais.

O MCI, Lei nº 12.965/2014, ainda exige a obrigatoriedade de guarda dos registros de conexão, por um ano, e dos registros de acesso a aplicações de internet, por seis meses, conforme arts. 13 e 15.

De forma resumida, são esses os dispositivos leis que permeiam a utilização de provas digitais no processo do trabalho. Dito isso, cabe agora analisar especificamente o que são, e de que forma as mensagens eletrônicas são aceitas pela Justiça do Trabalho na fase de instrução.

AS MENSAGENS ELETRÔNICAS COMO ESPÉCIE DE PROVA DIGITAL

Por prova digital, entende-se: “O instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato, suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para a sua determinação”¹. Possível compreender, portanto, que a prova digital ou demonstra a ocorrência de um fato ocorrido no mundo digital ou é um

1 THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital** – Conceito de prova digital, procedimentos e provas digitais em espécie. São Paulo: Revista dos Tribunais, 2020. p. 33.

meio digital para comprovar determinado fato. Logo, as mensagens eletrônicas produzidas em redes sociais são consideradas provas eletrônicas.

De acordo com Luciane Cardoso Barzotto, a prova digital é uma prova atípica, visto que não está taxativamente prevista nos códigos processuais, sendo importantes, porém, para o julgador atingir ao máximo o juízo de verossimilhança. Seriam, até então, por exemplo, as máximas de experiência, fatos notórios, indícios, entre outros. Entretanto, com o surgimento da digitalização processual, nasce uma nova prova atípica, que é a prova eletrônica, digital ou virtual².

Importante referir que, no entanto, ainda que não prevista nos códigos processuais, a prova digital passou a estar autorizada a partir da publicação da Lei nº 11.419/2006, a qual dispõe sobre a informatização do processo judicial (processo eletrônico), ao prever em seu art. 13 que: “O magistrado poderá determinar que sejam realizados por meio eletrônico a exibição e o envio de dados e de documentos necessários à instrução do processo”. Há, portanto, uma autorização legal para que o magistrado determine a realização de provas digitais, tais como vídeos, textos e todos as postagens existentes nas redes sociais, postados publicamente na rede mundial de computadores, em perfis abertos, acessados pelo magistrado ou pelas partes³.

Para ser válida, a prova digital precisa cumprir os requisitos da integridade, da autenticidade, bem como a cadeia de custódia. A autenticidade seria “a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital”⁴. Já a integridade deve ser compreendida como “a qualidade da prova digital que permite a certeza com relação à sua completude e não adulteração”⁵. Por fim, a cadeia de custódia, THAMAY e TAMER esclarecem que:

[...] é preciso preservar a autenticidade e a integridade em todo processo de produção da prova digital, desde sua identificação, coleta, extração de resultados, até a apresentação no processo ou procedimento de destino. A ideia é construir verdadeiro registro histórico da evidência, de toda vida da prova. A ideia é que se alguém seguir os mesmos passos já dados na produção da prova, o resultado será exatamente o mesmo.

2 BARZOTTO, Luciane Cardoso. A Prova Digital como Meio de Prova Atípica: Aspectos teóricos e um Caso Prático. In.: BERTACHINI, Danielle.; MISKULIN, Ana Paula Silva Campos.; NETO, Planton Teixeira de Azevedo (Coords). **Provas digitais no processo do trabalho**: realidade e futuro. Campinas: Lacier Editora, 2022. p. 99-101.

3 BARZOTTO, Luciane Cardoso. A Prova Digital como Meio de Prova Atípica: Aspectos teóricos e um Caso Prático. In.: BERTACHINI, Danielle.; MISKULIN, Ana Paula Silva Campos.; NETO, Planton Teixeira de Azevedo (Coords). **Provas digitais no processo do trabalho**: realidade e futuro. Campinas: Lacier Editora, 2022. p.40.

4 THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital** – Conceito de prova digital, procedimentos e provas digitais em espécie. São Paulo: Revista dos Tribunais, 2020. p. 40.

5 THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital** – Conceito de prova digital, procedimentos e provas digitais em espécie. São Paulo: Revista dos Tribunais, 2020. p. 45.

Nesse ponto, é importante sinalizar datas, horários, quem teve acesso, onde o acesso foi feito e até quaisquer alterações inevitáveis relacionadas⁶

Por essa razão, simples *printscreen* de e-mails, conversas de WhatsApp, ou outras redes sociais, no corpo de petições acabam não servindo como documento, mas simples ilustração. Os advogados devem buscar identificar (i) a data em que feito o acesso à prova; (ii) a data de extração da prova digital; (iii) os horários de acesso e da extração; (iv) quais as pessoas que tiveram acesso e/ou acessaram a referida prova; (v) em que lugar se deu o acesso e a extração das informações; (vi) se, na extração dos dados, ocorreram alterações inevitáveis. Assim, será possível demonstrar ao juízo a lisura na obtenção os dados, buscando assegurar a confiabilidade na prova digital⁷.

A melhor opção para assegurar a validade da prova digital é a realização de ata notarial (art. 384 c/c art. 405, do CPC). O referido documento é um instrumento pelo qual o tabelião concede autenticação a algum fato, inserindo-o em seus livros, tendo com a finalidade principal de tornar-se prova em processo judicial. Difere-se da escritura pública, já que essa contém a manifestação de vontade das partes interessadas, podendo conter elementos acidentais como condição, termo e encargo. Já a ata notarial contém a narração de fatos que o tabelião presenciou e transcreveu, sem emitir juízo de valor, para um documento com fé e conteúdo probatório de uma escritura pública⁸.

Na utilização da ata notarial para troca de mensagens eletrônicas ou *sites* de internet, por exemplo, deve ser apresentado o conteúdo ao notário. A partir do que é visto e constatado, o tabelião redige a correspondente descrição em seus livros, lavrando a ata notarial respectiva. Sendo assim, o documento serve uma importante função de declarar as informações e fatos contidos nas provas digitais. Importante referir que, de acordo com o parágrafo único do art. 193 do CPC, são aplicáveis às atas notariais, no que houver compatibilidade, as regras contidas nos arts. 193 a 199, que regulamentam os atos processuais total ou parcialmente digitais.

Quanto ao ônus probatório, como não há regra específica sobre o tema, aplica-se o disposto no art. 429 do CPC, o qual dispõe que “Incumbe o ônus da prova

6 THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital** – Conceito de prova digital, procedimentos e provas digitais em espécie. São Paulo: Revista dos Tribunais, 2020. p. 114.

7 SILVA, José Antônio Ribeiro de Oliveira. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova correlatas. In.: In.: BERTACHINI, Danielle.; MISKULIN, Ana Paula Silva Campos.; NETO, Planton Teixeira de Azevedo (Coords). **Provas digitais no processo do trabalho: realidade e futuro**. Campinas: Lacier Editora, 2022. p. 86.

8 TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática**. São Paulo: Saraiva, 2015. p. 157-158.

quando: I – se tratar de falsidade de documento ou de preenchimento abusivo, à parte que a arguir; II – se tratar de impugnação da autenticidade, à parte que produziu o documento”. Sendo assim, se a parte contra a qual se produziu a prova documental não impugna sua assinatura, mas somente o seu conteúdo, é dela o ônus da prova. A parte, nesse caso, deverá provar, por exemplo, que houve alguma adulteração. Poderá fazer isso por meio da juntada da prova original (sem as alegadas alterações), a realização de perícia técnica, ou até mesmo a expedição de ofícios para os locais em que se guardam os dados extraídos, como os provedores de internet. Entretanto, se a impugnação do documento for quanto à assinatura, o ônus da prova será de quem a arguiu.

Importante referir, contudo, que assim como as demais espécies típicas de provas, a prova digital não reduz, nem elimina, a prova oral, conhecida como a rainha dentre as espécies utilizadas no processo do trabalho. Isso se dá ao fato de que as relações de trabalho estão protegidas pelo princípio da primazia da realidade sobre a forma. Dessa forma, ainda que exista uma prova digital no processo que embase a tese da parte autora, ou da parte ré, ainda assim, através de testemunhas, poderá seu teor ser relativizado.

O ENTENDIMENTO DA JUSTIÇA DO TRABALHO QUANTO AO VALOR PROBATÓRIO DE MENSAGENS ELETRÔNICAS NO PROCESSO DO TRABALHO

Considerando o até aqui exposto, não restam dúvidas de que mensagens eletrônicas podem ser consideradas válidas na fase instrutória do processo judicial. Cabe, no entanto, analisar de que forma essa espécie de prova é valorada especificamente na Justiça do Trabalho.

A respeito da utilização de mensagens de áudio e escritas produzidas no aplicativo WhatsApp, o Tribunal Superior do Trabalho (TST) já se posicionou⁹ no sentido de que a sua validade deve ser relacionada com o Tema Repercussão Geral 237, do Supremo Tribunal Federal (STF), o qual estabelece que: “É lícita a prova consistente em gravação ambiental realizada por um dos interlocutores sem o conhecimento do outro”. Ou seja, não há ilicitude na gravação de conversação em áudio ou escrita por um dos interlocutores, não sendo necessário o conhecimento prévio da gravação pela outra pessoa. Cabe, no entanto, à parte contrária fazer

9 **Agravo em Agravo de Instrumento em Recurso de Revista nº 10290-35.2020.5.18.0103**, julgado pela 2ª Turma do Tribunal Superior do Trabalho em 24/06/2022, Rel. Margareth Rodrigues Costa. Disponível em: <<https://consultaprocessual.tst.jus.br/consultaProcessual/consultaTstNumUnica.do?consulta=Consultar&conscsjt=&numeroTst=10290&digitoTst=35&anoTst=2020&orgaoTst=5&tribunalTst=18&varaTst=0103&submit=Consultar>>. Acesso em: 1 de mar. de 2024

prova do fato impeditivo, extintivo ou modificativo alegado, o qual possa invalidar as mensagens trazidas aos autos.

De acordo com a ministra Margareth Rodrigues Costa:

[...] É certo que o áudio e o texto enviados pelas partes por meio do aplicativo de mensagens *WhatsApp* podem ser exibidos em juízo como meio de prova por um dos interlocutores, sem a necessidade de comunicação prévia da outra parte acerca da gravação, até porque a comunicação fica registrada no aplicativo mensageiro e está disponível para ambos interlocutores. Não há ilicitude na demonstração em juízo de fatos a partir de correspondência eletrônica recebida pelo destinatário, que pode fazer qualquer uso não vedado pelo ordenamento jurídico vigente. Ressalta-se que não houve apreensão do telefone, acesso indevido ou interceptação por terceiros das comunicações enviadas pelas partes por meio do aplicativo de mensagens, mas apenas utilização da comunicação por um dos interlocutores, legítimo detentor do conteúdo da mensagem. [...] No presente caso, o Tribunal Regional considerou válida como prova as gravações de áudio e as mensagens de aplicativo (*WhatsApp*) recebidas pelo reclamante em conversa com a Sra. Ivonice, integrante do setor de recursos humanos dos reclamados. Logo, é imperioso reconhecer a licitude e validade da prova apresentada pelo reclamante. No mais, os reclamados não comprovaram as suas alegações com relação ao conteúdo da prova (não era a Sra. Ivonice nas gravações e adulteração ou edição do áudio). Nos termos do art. 373, II, do CPC/2015, compete ao réu o ônus da prova em relação ao fato impeditivo, extintivo ou modificativo do diretor do autor, o que não ocorreu [...] ¹⁰.

Nesse mesmo sentido, o Tribunal Regional do Trabalho (TRT) da 10ª Região ¹¹ reconheceu a licitude de áudios de *WhatsApp* apresentados em reclamação trabalhista, com base no que dispõe o art. 5º, LVI, da Constituição Federal, bem como os arts. 369 e 422, do CPC. A Constituição Federal reconhece como direito fundamental de primeira dimensão a proibição de utilização de provas obtidas por meios ilícitos, ao passo que o CPC estabelece que as partes possuem o direito de empregar todos os meios legais, assim como os moralmente legítimos, mesmo que não previstos no Código, para provar os fatos que fundamentam o pedido ou a defesa, influndo de forma eficaz na convicção do julgador. Sendo assim, se as mensagens utilizadas como prova observam o entendimento firmado pelo STF, não há que se considerar ilícita.

10 **Agravo em Agravo de Instrumento em Recurso de Revista nº 10290-35.2020.5.18.0103**, julgado pela 2ª Turma do Tribunal Superior do Trabalho em 24/06/2022, Rel. Margareth Rodrigues Costa. Disponível em: <<https://consultaprocessual.tst.jus.br/consultaProcessual/consultaTstNumUnica.do?consulta=Consultar&conscsjt=&numeroTst=10290&digitoTst=35&anoTst=2020&orgaoTst=5&tribunalTst=18&varaTst=0103&submit=Consultar>>. Acesso em: 1 de mar. de 2024.

11 **Recurso ordinário nº 000009-86.2021.5.10.00015**, julgado pela 3ª Turma do Tribunal Regional do Trabalho da 10ª Região em 23/04/2022, Rel. Cilene Ferreira Amaro Santos. Disponível em: <<https://pje.trt10.jus.br/consultaprocessual/detalhe-processo/0000099-86.2021.5.10.0015/2#1dae52c>>. Acesso em: 1 de mar. de 2024.

Em outra ação, comprovando o fato de que simples *prints* podem ser desconsiderados em juízo, em uma ação julgada improcedente, o juiz da 2ª Vara do Trabalho de Campina Grande/PB¹², ao analisar o pedido de acúmulo de função, entendeu que a captura de tela, desacompanhado de ata notarial ou laudo emitido por entidades terceiras, e impugnada pela parte contrária, não poderia ser aceita como prova. Por essa razão, julgou improcedente o pedido que buscava-se provar por meio da prova eletrônica, em razão da parte autora não ter se desincumbido do seu ônus probatório.

Portanto, ainda que a jurisprudência aceite, em princípio, a utilização da prova digital, cabe ao juiz a análise do caso concreto, levando em consideração, não só a licitude da prova, mas sua conexão com as demais provas produzidas no processo.

CONSIDERAÇÕES FINAIS

Encerrada a argumentação do presente trabalho, conclui-se que o tema tem relevância atual, na medida em que não há uma norma específica que discipline a produção e o valor probatório das mensagens eletrônicas. Essa lacuna acarreta a aplicação dos dispositivos celetistas acerca do ônus da prova, a aplicação subsidiária/supletiva do Código de Processo Civil e adoção da hermenêutica do caso concreto, tudo, equilibrado pelo cotejo de todas as provas produzidas nos autos, baseado no princípio da primazia da realidade (decorrência lógica do Princípio da Proteção que, por essência, também informa o direito processual do trabalho).

Destarte, não se pode permitir a banalização dessa espécie de prova, entendendo-se que, em qualquer caso, a mera apresentação de mensagens eletrônicas pode servir de prova absoluta, mas, minimamente, como início de prova. Por outro lado, a análise do caso concreto, a natureza do fato e do direito em debate, e a regra de ônus da prova poderão, em determinados casos, impor mais valor às mensagens eletrônicas, sempre pretendendo-se a entrega da tutela jurisdicional a partir de um devido (e almejado) processo legal.

REFERÊNCIAS

BARZOTTO, Luciane Cardoso. A Prova Digital como Meio de Prova Atípica: Aspectos teóricos e um Caso Prático. In.: BERTACHINI, Danielle.; MISKULIN, Ana

12 ATSum 0001002-27.2022.5.13.0008, sentença publicada 10/03/2023, Juiz Carlos Hinderburg de Figueiredo. Disponível em: <<https://pje.trt13.jus.br/consultaprocessual/detalhe-processo/0001002-27.2022.5.13.0008/1#cb42bc0>>. Acesso em: 8 de mar. de 2024

Paula Silva Campos.; NETO, Planton Teixeira de Azevedo (Coords). **Provas digitais no processo do trabalho**: realidade e futuro. Campinas: Lacier Editora, 2022.

SILVA, José Antônio Ribeiro de Oliveira. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova correlatas. In.: In.: BERTACHINI, Danielle.; MISKULIN, Ana Paula Silva Campos.; NETO, Planton Teixeira de Azevedo (Coords). **Provas digitais no processo do trabalho**: realidade e futuro. Campinas: Lacier Editora, 2022.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. São Paulo: Saraiva, 2015.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital** – Conceito de prova digital, procedimentos e provas digitais em espécie. São Paulo: Revista dos Tribunais, 2020.

Agravo em Agravo de Instrumento em Recurso de Revista nº 10290-35.2020.5.18.0103, julgado pela 2ª Turma do Tribunal Superior do Trabalho em 24/06/2022, Rel. Margareth Rodrigues Costa. Disponível em: <<https://consultaprocessual.tst.jus.br/consultaProcessual/consultaTstNumUnica.do?consulta=Consultar&conscsjt=&numeroTst=10290&digitoTst=35&anoTst=2020&orgaoTst=5&tribunalTst=18&varaTst=0103&submit=Consultar>>. Acesso em: 8 de mar. de 2024

Recurso ordinário nº 000009-86.2021.5.10.00015, julgado pela 3ª Turma do Tribunal Regional do Trabalho da 10ª Região em 23/04/2022, Rel. Cilene Ferreira Amaro Santos. Disponível em: <<https://pje.trt10.jus.br/consultaprocessual/detalhe-processo/0000099-86.2021.5.10.0015/2#1dae52c>>. Acesso em: 1 de mar. de 2024.

ATSum 0001002-27.2022.5.13.0008, sentença publicada 10/03/2023, Juiz Carlos Hinderburg de Figueiredo. Disponível em: <<https://pje.trt13.jus.br/consultaprocessual/detalhe-processo/0001002-27.2022.5.13.0008/1#cb42bc0>>. Acesso em: 8 de mar. de 2024.

/Nossos autores

ANA CAROLINA DE PAIVA MONTEIRO

Os desafios do combate às fraudes eletrônicas e a urgência de regulamentação do tratamento de dados na esfera criminal

Advogada da área de Penal Empresarial. Graduada pela Pontifícia Universidade Católica de São Paulo (PUC-SP), pós-graduada em Penal Empresarial pela Fundação Getulio Vargas (FGV), possui experiência Direito Penal econômico, envolvendo crimes financeiros, tributários, licitatórios e lavagem de capitais, além de delitos contra a vida e cometidos no âmbito da violência doméstica.

ANA CAROLINA GASPAR

A gestão e autenticidade dos livros societários digitais frente ao Marco Civil da Internet

Assistente Jurídica das áreas de Direito Societário e M&A em TozziniFreire Advogados. Graduada da Pontifícia Universidade Católica de São Paulo (PUC-SP). Possui experiência em Direito Societário e M&A.

ANA CAROLINA KATLAUSKAS CALIL

O compartilhamento de dados na democratização do setor de Energia Elétrica

Advogada da área de Infraestrutura e Energia. Graduada pela Escola de Direito de São Paulo da Fundação Getúlio Vargas (FGV), especialista em Aspectos Físicos e Regulamentares do Setor de Energia pela Associação Brasileira de Companhias de Energia Elétrica (ABCE) e em Mercado Financeiro e de Capitais pelo INSPER. Integrante do Instituto Brasileiro de Direito de Energia (IBDE) e da Comissão de Energia do Instituto dos Advogados de São Paulo (IASP). Ana Carolina Calil é especializada em energia elétrica e assessora clientes dos diversos segmentos da indústria (geração, distribuição, transmissão, comercialização e consumo) em questões tanto regulatórias como transacionais. Sua atuação inclui assessoria jurídica em operações societárias envolvendo empresas atuantes no setor de energia elétrica, assim como no desenvolvimento de projetos. Possui ampla experiência na elaboração, revisão e negociação de contratos relacionados ao setor de energia, bem como na representação de clientes em processos judiciais e administrativos e em consultas regulatórias. Ana é reconhecida por relevantes guias jurídicos, como Chambers Global, Chambers Brazil, Latin Lawyer 250, Leaders League e The Legal 500 (como next generation partner).

BÁRBARA BASSANI DE SOUZA

Seguros: distribuição pela internet

Sócia na área de Seguros e Resseguros de TozziniFreire Advogados, com atuação em consultoria regulatória e contencioso. Doutora e Mestre em Direito Civil pela Universidade de São Paulo. Especializada em Direito Civil e Graduada em Direito pela Universidade Presbiteriana Mackenzie. Professora em instituições de ensino superior. Autora de diversos livros e artigos. Diretora da AIDA Brasil – Associação Internacional de Direito de Seguro e Acadêmica da Academia Nacional de Seguros e Previdência.

BRUNA BORGHI TOMÉ

Marco Civil da Internet e eleições: desafios e perspectivas para o futuro

Bruna possui mais de 10 anos de experiência na área de Tech Litigation, tendo assessorado algumas das empresas mais relevantes do setor, com foco em questões contenciosas relacionadas à tecnologia e privacidade de dados, incluindo temas judiciais e administrativos decorrentes da promulgação do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Sua atuação abrange todo o contencioso estratégico, desde inquéritos civis e ações civis públicas até os leading cases nos tribunais superiores. No âmbito do Direito Eleitoral Digital, é responsável pelas questões contenciosas e regulatórias. Graduada pela Faculdade de Direito, especializada em Direito Processual Civil e mestre em Direito Processual Civil pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Bruna foi finalista do Euromoney Women in Business Law Awards 2022 - Americas e destaque como Leading Individual na primeira e segunda edição do guia Global Data Review - GDR 100. Em 2021, foi mencionada pelo guia jurídico Leaders League como uma das líderes das práticas de Tecnologia e Proteção de Dados. É também recomendada pelos guias The Legal 500 e Latin Lawyer 250 em Contencioso. Bruna é LACCA Approved em Data, Technology and Privacy Law.

BRUNO SÁ DE ANDRADE

Marco Civil da Internet e eleições: desafios e perspectivas para o futuro

Advogado na área de Direito Eleitoral Empresarial e Digital em TozziniFreire Advogados. Graduado e especialista em Proteção de Dados pela Universidade Presbiteriana Mackenzie.

CARLA DO COUTO HELLU BATTILANA

Marco Civil e Proteção de Dados: consentimento e o caminho para regulação de proteção de dados no Brasil

Direitos autorais e conexos e o Marco Civil da Internet

Sócia das áreas de CyberSecurity & DataPrivacy, e Corporate M&A de TozziniFreire. Graduada em Direito pela Pontifícia Universidade Católica, com L.LM na University of Chicago. Detentora dos certificados CIPP/E, CIPM, e CDPO/BR pela IAPP (International Association of Privacy Professionals). Carla é reconhecida pelos importantes guias jurídicos The Legal 500, Latin Lawyer 250, Global Data Review, Análise Advocacia 500 e Análise Advocacia Mulher.

CLARA PACCE P. SERVA

Direitos Humanos e internet: promoção ou violação?

Sócia e head na área de Empresas e Direitos Humanos e coordenadora da advocacia Pro Bono em TozziniFreire Advogados. Mestre em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Membro do Comitê de Empresas e Direitos Humanos da International Bar Association (IBA) e colíder da Câmara Temática de Impacto Social do Conselho Empresarial Brasileiro para o Desenvolvimento Sustentável (CEBDS), entre outros.

ELIAS MARQUES DE MEDEIROS NETO

Diálogos entre o Código de Processo Civil de 2015 e a internet

Pós-Doutorado em Direito Processual Civil pelas Universidades de Lisboa, Coimbra e Salamanca. Pesquisador Visitante em Direito Processual Civil no Instituto Max Planck. Doutor e mestre em Direito Processual Civil pela Pontifícia Universidade Católica de São Paulo (PUC-SP) e graduado em Direito pela Universidade de São Paulo (USP). Sócio de Resolução de Disputas de TozziniFreire Advogados. Vice-presidente da Comissão de Processo Civil da Ordem dos Advogados do Brasil de São Paulo (OAB SP) e presidente da Comissão de Processo Civil da OAB SP de Pinheiros. Professor universitário.

GABRIELA VITIELLO WINK

Regulação da internet e o futuro da rede

Graduada pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), especialista em Processo Civil pela Universidade Federal do Rio Grande do Sul (UFRGS) e em Direito Civil pela UniRitter. Sócia de TozziniFreire Advogados nas áreas de Contencioso, Arbitragem e Direito do Consumidor.

GIOVANNI PAOLO FALCETTA

Compliance e transparência: a importância histórica e futura do MCI diante do desenvolvimento tecnológico

Sócio na área de Compliance e Investigação de TozziniFreire Advogados, Giovanni assessora conselhos de administração, companhias e comitês independentes na prevenção, detecção, resposta e remediação de questões de alta complexidade relacionadas a compliance, anticorrupção e crises corporativas. Ademais, coordena investigações internas para clientes nacionais e estrangeiros, auxiliando-os a enfrentar assuntos complexos que envolvem interação simultânea em múltiplas frentes, envolvendo reguladores, terceiros, litígios e mercado. Giovanni é professor convidado em instituições nacionais e internacionais, além de palestrar em eventos internacionais sobre compliance, investigações internas e gerenciamento de crises. Giovanni é graduado pela Pontifícia Universidade Católica de São Paulo (PUC-SP), e mestre em Direito Privado Europeu pela Sapienza – Università di Roma.

HELENA ROCHA MATOS

Direitos Humanos e internet: promoção ou violação?

Advogada na área de Empresas e Direitos Humanos em TozziniFreire Advogados. Mestre em Direito Constitucional pela Universidade Federal Fluminense. Especialista em Políticas Públicas e Economia pela Universidade de Oxford. Pesquisadora Ad Doc e membro do Conselho Consultivo do Instituto de Defensores dos Direitos Humanos.

ISABELLA FONTOURA D'ANGELO

A gestão e autenticidade dos livros societários digitais frente ao Marco Civil da Internet

Advogada das áreas de Direito Societário e M&A em TozziniFreire Advogados. Graduada pela Universidade Presbiteriana Mackenzie. Possui experiência em Direito Societário e M&A.

ISABELLE RUIZ GUERO

O potencial da inteligência artificial para moldar o futuro do comércio internacional brasileiro ..

Advogada, atuando na área de Comércio Internacional de TozziniFreire Advogados. É pós-graduanda em Direito Internacional, com ênfase em Comércio Internacional, pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (USP) e bacharel em Direito pela Universidade Presbiteriana Mackenzie.

JOÃO VITOR DE ALMEIDA RAMOS

Protegendo seu investimento: considerações legais para potenciais compradores em operações de M&A envolvendo provedores de aplicações de internet à luz do Marco Civil da Internet

Advogado da área de M&A, Societário e Investimento Estrangeiro. Graduado pela Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC-SP).

JÚLIA VIANA

Open Finance e o Marco Civil da Internet.....

Advogada das áreas de Mercado de Capitais e Direito Bancário de TozziniFreire Advogados. É graduada na Universidade São Judas Tadeu e possui vasta experiência voltada à estruturação de operações financeiras, financiamentos, emissão e oferta pública de títulos e valores mobiliários representativos de dívida, coordenação e participação em procedimentos de due diligence, bem como securitização de créditos, além de atuar em atividades relacionadas a regulação de serviços financeiros, como o cumprimento de regras e regulamentos relevantes por instituições financeiras.

LAÍS CURY REZENDE

Compliance e transparência: a importância histórica e Futura do MCI diante do desenvolvimento tecnológico

Advogada sênior na área de Compliance e Investigação de TozziniFreire Advogados. Laís possui ampla experiência profissional, tanto no Brasil como no Reino Unido, em due diligences de compliance e anticorrupção, investigações internas de compliance e anticorrupção, negociação de acordos de leniência, consultoria de compliance e jurídica anticorrupção, treinamentos de compliance e anticorrupção, bem como em outros assuntos relacionados a compliance e governança corporativa. Atuou em diversas, e nas principais, investigações de corrupção e questões de compliance no Brasil. Graduada pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Mestre pela London School of Economics and Political Science, com foco em Direito Corporativo e Direito Público. Integrante do Comitê de Compliance do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (IBRAC) e membro do Women's White Collar Defense Association.

LUCIANA BAZAN MARTINS BISETTI

Regulação da internet e o futuro da rede

Sócia de TozziniFreire Advogados na área de Contencioso, Luciana atua em casos estratégicos de diversas naturezas, com especial experiência em matérias atinentes a relações de consumo de alta complexidade e responsabilidade civil. Especialista em Direito do Consumidor, atua perante as autoridades de consumo em todos os níveis, tanto em sede de procedimentos administrativos quanto em negociações de acordos. Em disputas judiciais, Luciana possui vasta experiência em demandas coletivas, com atuação em centenas de ações civis públicas em todo o país, e em demandas individuais estratégicas. Sua atuação abrange os mais diversos setores da economia, com especial ênfase em clientes do setor de telecomunicações, tecnologia, varejo, soluções de pagamentos, automotivo e prestadoras de serviços públicos. Graduada em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP), pós-graduada em Processo Civil pela Fundação Getulio Vargas (FGV), cursou a Academy of American and International Law, organizada pelo Center for American and International Law, EUA, e especialista em Direito do Consumidor pela Faculdade de Direito de Coimbra, Portugal. É reconhecida pelo The Legal 500, relevante guia jurídico.

LUIZ RENATO OKUMURA

Protegendo seu investimento: considerações legais para potenciais compradores em operações de M&A envolvendo provedores de aplicações de internet à luz do Marco Civil da Internet

Sócio da área de M&A, Societário e Investimento Estrangeiro e do grupo setorial de Agronegócios. Mestre (LL.M.) com ênfase em Direito Societário pela University of Chicago, Illinois, EUA. Especializado em Gestão Empresarial pela Business School São Paulo. Graduado pela Faculdade de Direito da Universidade de São Paulo (USP).

LUIZA SATO

O compartilhamento de dados na democratização do setor de Energia Elétrica

Open Finance e o Marco Civil da Internet.....

Sócia do escritório TozziniFreire Advogados em São Paulo, com reconhecida experiência nas áreas de Proteção de Dados, Direito Digital e Propriedade Intelectual. É graduada na Faculdade de Direito do Largo São Francisco da Universidade de São Paulo (USP), com pós-graduação em Propriedade Intelectual na GVLaw e possui LL.M em Direito e Tecnologia pela Universidade da Califórnia – UC Berkeley. Em 2023, Luiza foi eleita pela Legal500 como next generation partner, pela WWL Global, como uma das 500 advogadas recomendadas no mundo na área de Proteção de Dados. Luiza também é reconhecida pelo diretório Chambers & Partners na área de Proteção de Dados. Atua hoje principalmente em consultoria, projetos de adequação, prevenção e resolução de incidentes de segurança da informação e transações envolvendo proteção de dados, segurança da informação, direito digital e direitos de propriedade intelectual.

MARCELA WAKSMAN EJNISMAN

Marco Civil e Proteção de Dados: consentimento e o caminho para regulação de proteção de dados no Brasil

Sócia das áreas de CyberSecurity & DataPrivacy, e Corporate M&A de TozziniFreire. Graduada em Direito pela Pontifícia Universidade Católica, com L.LM na Cornell Law School. Marcela é membro do International Technology Law Association, e recomendada em relevantes guias jurídicos, tais como Chambers Brazil, The Legal 500, Latin Lawyer 250, Who's Who Legal e Análise Advocacia

500. Marcela é reconhecida como LACCA Thought Leader: Intellectual Property, e é LACCA Approved.

MARCO AURÉLIO ANTAS TORRONTÉGUY

As normas sanitárias enquadradas pelo Marco Civil da Internet: um bug regulatório ou uma regulação viral?

Sócio de TozziniFreire Advogados na área de Ciências da Vida e Saúde. Doutor pela Faculdade de Direito da Universidade de São Paulo (FD-USP) e especialista em Direito Sanitário pela Faculdade de Saúde Pública da USP (FSP-USP).

MARIA EUGÊNIA GEVE M. LACERDA

Marco Civil e Proteção de Dados: consentimento e o caminho para regulação de proteção de dados no Brasil.

Advogada na área de Cybersecurity & Data Privacy de TozziniFreire. Graduada pela Escola de Direito de São Paulo da Fundação Getúlio Vargas, mestre em Filosofia e Teoria Geral do Direito pela Faculdade de Direito da Universidade de São Paulo. Certificada pelo CIPM/IAPP. Reconhecida como Associate do Watch no guia Chambers&Partners nos anos de 2021, 2022 e 2023.

MARIA FERNANDA SEBA RAHE

A gestão e autenticidade dos livros societários digitais frente ao Marco Civil da Internet

Advogada das áreas de Direito Societário e M&A em TozziniFreire Advogados. Graduada pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Possui ampla experiência em Direito Societário e M&A.

MARINA SAYURI KITAYAMA

Direitos autorais e conexos e o Marco Civil da Internet

Advogada das áreas de Tecnologia e Inovação. Graduada em Direito e mestranda em Filosofia e Teoria Geral do Direito pela Universidade de São Paulo

MARINA SILVEIRA FRANK

O valor probatório de mensagens eletrônicas no processo do trabalho

Advogada da área Trabalhista do escritório TozziniFreire Advogados. Graduada pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), especialista em Direito e Processo do Trabalho e mestre em Teoria da Jurisdição e Processo pela na mesma universidade

MAURÍCIO DE CARVALHO GÓES

O valor probatório de mensagens eletrônicas no processo do trabalho

Advogado da área Trabalhista. Sócio do escritório TozziniFreire Advogados. Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Mestre em Direitos Fundamentais pela Universidade Luterana do Brasil (ULBRA). Especialista em Direito do Trabalho pela UNISINOS. Professor do mestrado profissional do Programa de Pós-Graduação em Direito e Negócios da UNISINOS. Professor de Direito do Trabalho, de Direito Coletivo do Trabalho e de Direito Processual do Trabalho da Graduação (*Law School*) e da pós-graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Professor do curso de pós-graduação na Universidade Federal do Rio Grande Sul (UFRGS). Membro titular da Cadeira 33 da Academia Sul-rio-grandense de Direito do Trabalho.

NICOLAS ERIC MATOSO MEDEIROS DE SOUZA

Regulação da internet e o futuro da rede

Advogado sênior de TozziniFreire Advogados na área de Contencioso, Nicolas possui vasta experiência nas áreas de direito do consumidor e direito digital, atuando na representação de empresas nacionais e internacionais em processos administrativos e judiciais de alta complexidade, bem como em consultoria em defesa do consumidor, relações governamentais e planejamento estratégico. Atuou na Secretaria Nacional do Consumidor por mais de três anos, coordenando a Coordenação de Saúde e Segurança, responsável pela avaliação de recalls, condução de investigações e processos administrativos, inclusive sendo um dos autores dos normativos referente ao tema.

OSWALDO NOCE DALLA TORRE

A gestão e autenticidade dos livros societários digitais frente ao Marco Civil da Internet

Sócio das áreas de Direito Societário e M&A em TozziniFreire Advogados. Graduado pela Universidade Presbiteriana Mackenzie. Possui ampla experiência em Direito Societário e M&A e Mineração.

PATRÍCIA HELENA MARTA MARTINS

Regulação da internet e o futuro da rede

Sócia nos grupos de prática de Tecnologia e Inovação e Cybersecurity & Data Privacy de TozziniFreire Advogados, Patrícia também possui ampla experiência nas áreas de Contencioso e Direito do Consumidor, assessorando clientes em questões contenciosas relacionadas a essas áreas, na prevenção de responsabilidade, discussão sobre responsabilidades de intermediários e defesa em ações coletivas. Também atua na coordenação de processos em tribunais superiores, bem como em contencioso cível de proteção de dados e interação com autoridades administrativas. Como especialista em Direito Digital, conduz casos envolvendo direito eleitoral digital, estruturando e gerenciando as atividades de monitoramento da posição das autoridades brasileiras em relação às Fake News, além de contribuir com sugestões ao Tribunal Superior Eleitoral sobre a regulamentação eleitoral da publicidade eleitoral na internet. Graduada pela Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC-SP), pós-graduada em Direito das Relações de Consumo pela PUC-SP e especializada em Gestão Empresarial pela Business School São Paulo. Recomendada por Chambers Brazil, The Legal 500, Análise Advocacia 500 e Who's Who Legal, relevantes guias jurídicos.

PEDRO EROLES

Open Finance e o Marco Civil da Internet.

Sócio de TozziniFreire Advogados nas áreas de Direito Bancário e Inovação Financeira. É graduado, mestre e doutor em Direito pela Universidade de São Paulo (USP) e pós-doutorando em Direito Internacional pela USP. Pedro tem grande experiência com atividades voltadas para regulação de serviços financeiros, regulação de pagamentos, transações financeiras, mercado de capitais, fintechs, criptomoedas, derivativos, blockchain, transações envolvendo entidades reguladas (como M&As, IPOs e financiamentos) e processos administrativos perante

o Banco Central e a Comissão de Valores Mobiliários (CVM). Atua desde 2018 como consultor da Procuradoria-Geral do Banco Central do Brasil.

PEDRO VECCI BIANCARDINI

Protegendo seu investimento: considerações legais para potenciais compradores em operações de M&A envolvendo provedores de aplicações de internet à luz do Marco Civil da Internet

Advogado da área de M&A, Planejamento Patrimonial e Sucessório e Societário e Investimento Estrangeiro. Graduado pela Faculdade de Direito da Universidade do Estado do Rio de Janeiro.

RODRIGO DE GRANDIS

Os desafios do combate às fraudes eletrônicas e a urgência de regulamentação do tratamento de dados na esfera criminal

Sócio na área de Penal Empresarial, com 20 anos de experiência no serviço público, tendo atuado como Promotor de Justiça em São Paulo em 2003 e Procurador da República de 2004 a 2023, com prática preponderante em crimes contra o sistema financeiro nacional e lavagem de ativos ilícitos.

SHIN JAE KIM

O potencial da inteligência artificial para moldar o futuro do comércio internacional brasileiro ..

Sócia responsável pela área de Compliance & Investigação de TozziniFreire Advogados e co-head do grupo Regulatório. Coursou a Academy of American and International Law, organizada pelo Center for American and International Law, EUA; é mestre em Direito Internacional e Comparado pela Vrije Universiteit Brussel, Bélgica; especializada em Direito Tributário e graduada pela Faculdade de Direito da Universidade de São Paulo (USP).

SOFIA KILMAR

Direitos autorais e conexos e o Marco Civil da Internet

Sócia das áreas de Tecnologia e Inovação. Graduada, Mestre e Doutora pela Universidade de São Paulo. Integrante do International Institute for Conflict Prevention & Resolution (CPR). Especializada em direito processual civil e de

tecnologia, perante a Universidade de Harvard, a Fundação Getulio Vargas e o Instituto de Tecnologia e Sociedade do Rio de Janeiro.

STEPHANIE CONSONNI DE SCHRYVER

Direitos autorais e conexos e o Marco Civil da Internet

Sócia da área de Propriedade Intelectual. Graduada pela Pontifícia Universidade Católica de São Paulo (PUC-SP), possui ampla experiência em assuntos relacionados à propriedade intelectual, direitos autorais, entretenimento, fusões e aquisições envolvendo ativos de propriedade intelectual, concorrência desleal, ambush marketing, disputas de nomes de domínio, contratos de tecnologia, entre outros.

VICTOR HUGO CALLEJON AVALLONE

As normas sanitárias enquadradas pelo Marco Civil da Internet: um bug regulatório ou uma regulação viral?

Advogado Sênior da área de Ciências da Vida e Saúde de TozziniFreire. Mestre em Direito do Comércio Internacional pela Faculdade de Direito da Universidade de São Paulo (FD-USP) e especialista em Direito Sanitário pela Faculdade de Saúde Pública da USP (FSP-USP).



Tozzini Freire.

ADVOGADOS



tozzinifreire.com.br