

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Inteligência Artificial e Big Data

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
outubro/2022

CEPED



DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Inteligência Artificial e Big Data

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
outubro/2022

CEPED



ITS

COORDENAÇÃO:

Sérgio Branco e Chiara de Teffé

PROJETO GRÁFICO, DIAGRAMAÇÃO E CAPA:

Mariana Bertoluci

PRODUÇÃO EDITORIAL:

Instituto de Tecnologia e Sociedade - ITS

REVISÃO:

Chiara de Teffé

**Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)**

Inteligência artificial e Big Data [livro eletrônico] / coordenação Sérgio Branco, Chiara de Teffé. -- Rio de Janeiro, RJ : ITS - Instituto de Tecnologia e Sociedade, 2023. -- (Diálogos da pós-graduação em direito digital ; 1)
PDF

Vários autores.

Bibliografia.

ISBN 978-85-5596-004-8

1. Big Data 2. Direito digital 3. Direito e tecnologia 4. Inteligência artificial 5. Proteção de dados - Direito - Brasil I. Branco, Sérgio. II. Teffé, Chiara de. III. Série.

23-147239

CDU-34:004

Índices para catálogo sistemático:

1. Direito digital 34:004

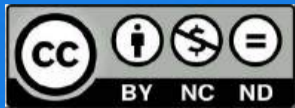
Tábata Alves da Silva - Bibliotecária - CRB-8/9253-0

COMO CITAR:

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Inteligência Artificial e Big Data: diálogos da pós-graduação em Direito Digital*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2022. 327p.

INSTITUTO DE TECNOLOGIA E SOCIEDADE:

itsrio.org | @itsriodejaneiro | midias@itsrio.org



A obra Inteligência Artificial e Big Data: diálogos da pós-graduação em Direito Digital está protegida com a seguinte licença:

Creative Commons Atribuição-NãoComercial-Sem Derivações 4.0 Internacional



Você tem o direito de:

Compartilhar — copiar e redistribuir o material em qualquer suporte ou formato

O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.



De acordo com os seguintes termos:

Atribuição — Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso.



Não Comercial — Você não pode usar o material para fins comerciais.



Sem Derivações — Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

Sem restrições adicionais — Você não pode aplicar termos jurídicos ou medidas de caráter tecnológico que restrinjam legalmente outros de fazerem algo que a licença permita.

https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt_BR

Lista de Autores

Bárbara Milanese Pimentel

Daniela Cenci Lima

Davi Brito de Almeida

Denise de Souza Luiz Francoski

Fábio Pimentel de Carvalho

Gabriela Brum Davoli

Gabriel Maciel de Lima

Larissa Fernanda de Mesquita Baraldo

Larissa Sad Coelho

Marcelo Batista Gomes da Cruz

Maria Luiza Correia Fernandes

Rafael Lucas Borba

Rafael Rocha Pessoa

Rafaella Fernandes dos Santos

Sabrina Wervloet

Tamara da Silva

Viviane de Souza Ramos Pereira

APRESENTAÇÃO

A **Pós-Graduação em Direito Digital**, conduzida pelo Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ), por meio de seus professores, assistentes acadêmicos e alunos, vem produzindo conteúdos e diálogos de grande relevância para os cenários jurídico e tecnológico.

Com grande satisfação, gostaríamos de realçar que o projeto vem sendo ampliado semestralmente, o que nos provoca de forma constante a incrementar e trazer novos recursos e vozes para a nossa especialização *lato sensu*.

A diversidade de pessoas envolvidas nos projetos, a pluralidade de perspectivas e a reflexão crítica sobre a proteção dos direitos humanos e a aplicação da tecnologia em nossa sociedade são bases do ITS Rio, centro de pesquisa multidisciplinar totalmente independente, que atua há quase 10 anos nos ambientes carioca, nacional e internacional.

Para esta publicação foram selecionados 17 artigos de integrantes do programa de Pós-Graduação em Direito Digital, os quais exploram relevantes temas acerca de aplicações da inteligência artificial, big data e inovação.

Novos modelos de negócios; aplicações com inteligência artificial no Judiciário, na medicina e na música; atendimento dos direitos dos titulares dos dados pessoais; riscos à privacidade; *dark patterns* nas contratações pela internet; proteção às informações do consumidor no ambiente virtual; gamificação nas interfaces de trabalho; moderação e ordens de remoção de conteúdo na internet; criptomoedas e inovação; open banking; e tributação de software são alguns dos interessantes temas tratados na coletânea.

O conteúdo aqui exposto não reflete necessariamente a opinião institucional do ITS Rio, ou de seus membros, representando reflexão acadêmica de responsabilidade de seu autor.

Acreditamos na importância da difusão e do acesso ao conhecimento, por essa razão o presente livro encontra-se disponível de forma gratuita e sob a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Para os próximos anos, esperamos ampliar parcerias e desenvolver mais ações voltadas à educação e à pesquisa que impactem positivamente a sociedade e promovam o Direito Digital.

Agradecemos a todos que contribuíram e se interessaram por esse projeto.

Rio de Janeiro, 19 de julho de 2022.
Os coordenadores

Os coordenadores

Sérgio Branco é Cofundador e Diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Especialista em propriedade intelectual pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Pós-graduado em cinema documentário pela FGV Rio. Graduado em Direito UERJ. Sócio de Rennó Penteado Sampaio Advogados.

Chiara de Teffé é Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Graduada em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Atualmente, é coordenadora de pesquisa e publicações da pós-graduação em Direito Digital do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a UERJ, e professora de Direito Civil e Direito Digital na faculdade de Direito do IBMEC Rio. Leciona em cursos específicos de pós-graduação e extensão do CEPED-UERJ, da PUC-Rio, da EMERJ e do ITS Rio. Membro da Comissão de Proteção de Dados e Privacidade da OABRJ. Membro do Fórum Permanente de Liberdade de Expressão, Liberdades Fundamentais e Democracia da EMERJ. Foi professora substituta de Direito Civil na UFRJ. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Atua como advogada em áreas do Direito Civil e do Direito Digital e como consultora em proteção de dados pessoais.

Sumário

- 1 Orientações normativas para o uso de inteligência artificial no sistema de justiça brasileiro**
DANIELA CENCI LIMA _____ PÁGINA 10
- 2 Medicina de precisão e IA: implicações jurídicas**
DAVI BRITO DE ALMEIDA _____ PÁGINA 29
- 3 A questão da titularidade dos direitos autorais de música produzida por Inteligência Artificial no ordenamento jurídico europeu**
RAFAEL LUCAS BORBA _____ PÁGINA 50
- 4 Tracking Pixels: riscos invisíveis à privacidade**
MARIA LUIZA CORREIA FERNANDES _____ PÁGINA 71
- 5 O atendimento dos direitos dos titulares dos dados pessoais: o case do TJSC com o aplicativo LGPDjus**
DENISE DE SOUZA LUIZ FRANCOSKI _____ PÁGINA 87
- 6 *Dark patterns* nas contratações pela internet e o direito do consumidor**
VIVIANE DE SOUZA RAMOS PEREIRA _____ PÁGINA 124
- 7 Riscos a direitos e liberdades fundamentais como baliza da proteção de dados pessoais**
RAFAEL ROCHA PESSOA _____ PÁGINA 141
- 8 O consumidor e a publicidade direcionada *on-line*: uma análise segundo a Lei Geral de Proteção de Dados Pessoais**
GABRIELA BRUM DAVOLI _____
- 9 Aplicação da Gamificação nas Interfaces de Trabalho e seus Reflexos no Direito ao Não-Trabalho**
TAMARA DA SILVA _____ PÁGINA 173

Sumário

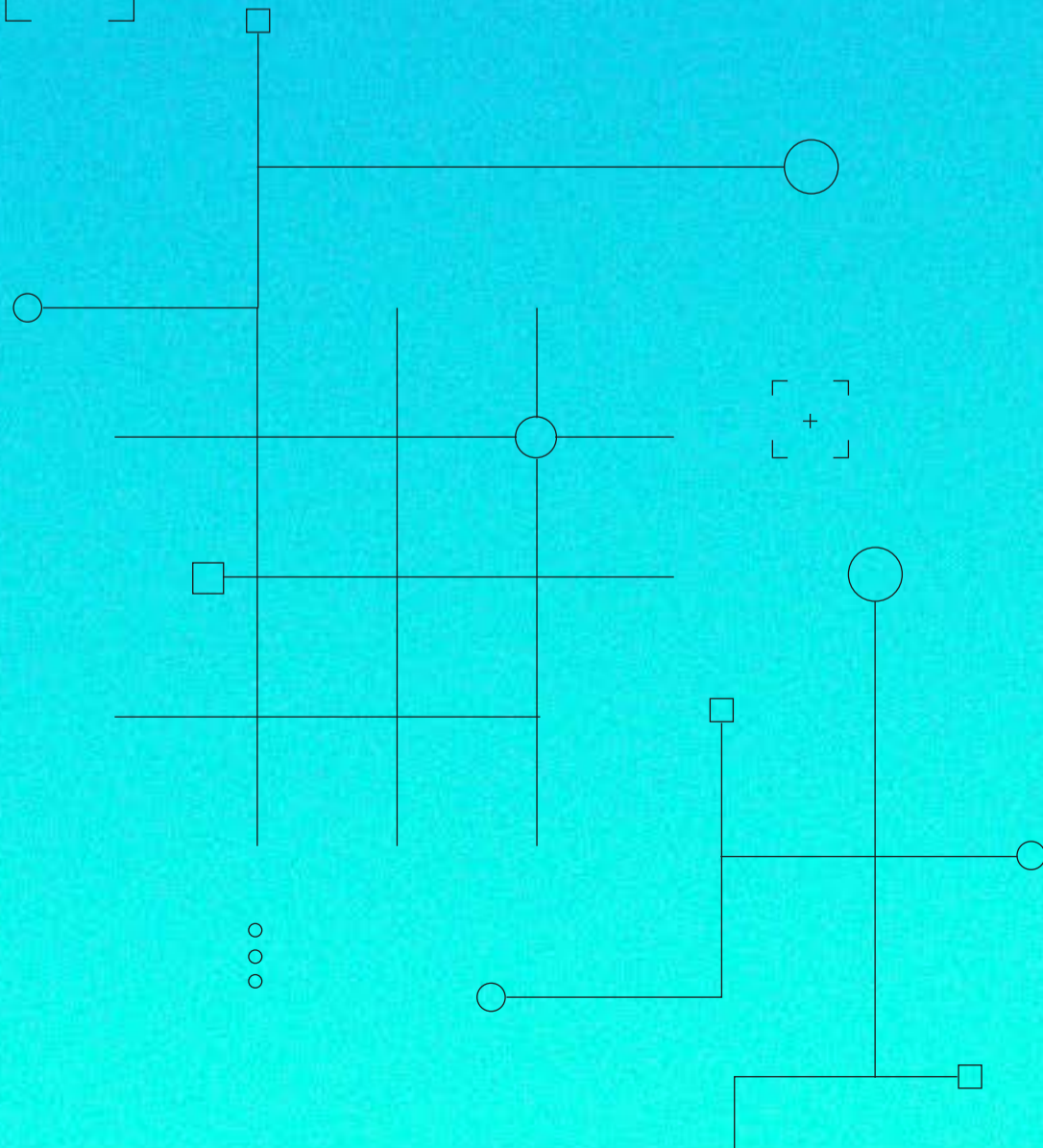
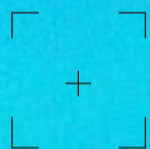
- 10** **Cenário atual das ordens globais de remoção de conteúdo na internet: aliadas ou adversárias dos usuários?**
LARISSA SAD COELHO ————— **PÁGINA 188**
- 11** **A importância da regulação da moderação de conteúdo em mídias digitais no combate à desinformação**
SABRINA WERVLOET ————— **PÁGINA 208**
- 12** **A utilização das criptomoedas para a solução dos problemas urbanos: Ecochain e Gestão Integrada dos Resíduos Sólidos**
GABRIEL MACIEL DE LIMA ————— **PÁGINA 225**
- 13** **Regulação e inovação na administração pública: a criação de uma startup na Prefeitura do Rio**
FÁBIO PIMENTEL DE CARVALHO ————— **PÁGINA 242**
- 14** **As contribuições e os desafios do open banking no mercado financeiro sob a perspectiva da proteção de dados e da concorrência**
RAFAELLA FERNANDES DOS SANTOS ————— **PÁGINA 260**
- 15** **Tributação de Software: uma análise sobre incidência do ICMS e do ISS**
BÁRBARA MILANESE PIMENTEL ————— **PÁGINA 275**
- 16** **Os critojogos “pay-to-play-to-earn” enquanto valores mobiliários carentes de regulação no Brasil**
MARCELO BATISTA GOMES DA CRUZ ————— **PÁGINA 290**
- 17** **As implicações penais da prática de scanlation**
LARISSA FERNANDA DE MESQUITA BARALDO ————— **PÁGINA 310**

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

1

Orientações normativas para o uso de inteligência artificial no sistema de justiça brasileiro

DANIELA CENCI LIMA



Sumário: Introdução. 1. Atual cenário do sistema de justiça brasileiro. 2. Quais contribuições podem ser aportadas pela inteligência artificial? 3. Usos da inteligência artificial nos tribunais do Brasil. 4. A importância da boa governança e de diretrizes éticas. 5. Quadro normativo para uso da inteligência artificial no Poder Judiciário. Considerações finais. Referências bibliográficas.

Introdução

O uso de novas soluções de tecnologia, sobretudo da inteligência artificial (IA), tem sido fortemente impulsionado no sistema de justiça brasileiro. Como veremos, tais ferramentas podem contribuir para o aprimoramento da administração da justiça e para a melhoria do serviço prestado, combatendo assim a morosidade e a burocracia que marcam a imagem do Poder Judiciário.

Serão exploradas a seguir as principais funcionalidades e as áreas de aplicação das ferramentas de IA em projetos em desenvolvimento ou já implantados pelos tribunais brasileiros. Considerando os novos desafios éticos, legais e de governança e atentando às implicações práticas, será abordada a importância da boa governança e de diretrizes éticas para o uso da IA em um campo sensível como a justiça. Nesse contexto, será dado destaque à necessidade de que as estratégias de abordagem e as estruturas normativas abarquem o design, o desenvolvimento, a implementação e a avaliação e o impacto das ferramentas de IA.

Para fazer frente a tais ponderações, serão mapeadas as iniciativas já existentes no Brasil para regulamentar o uso da IA no sistema de justiça, sobretudo através dos atos normativos do Conselho Nacional de Justiça (CNJ). Serão apresentadas as disposições voltadas ao estabelecimento de diretrizes éticas que incidem sobre todo o ciclo de vida das ferramentas de IA. Ao fim, serão pautadas as disposições referentes à estruturação tecnológica do Judiciário, o que permite impulsionar a inovação e o desenvolvimento de soluções de IA nos tribunais do país.

1. Servidora pública no Tribunal Regional Federal da 4ª Região. Especializanda em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Bacharela em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS).

1. Atual cenário do sistema de justiça brasileiro

O sistema de justiça brasileiro apresenta números expressivos quanto à quantidade de processos em tramitação, ao tempo médio de julgamento dos feitos e sua estrutura orçamentária e de pessoal. Segundo levantamento conduzido pelo Conselho Nacional de Justiça (CNJ), em dezembro de 2020, o número total de processos pendentes que aguardavam uma solução definitiva nos 90 tribunais do país – com exceção do Supremo Tribunal Federal – somava 75,4 milhões.

Somente nos 12 meses anteriores, haviam ingressado 25,8 milhões de novos casos. Para lidar com a demanda e viabilizar a prestação do serviço público, o Judiciário conta com uma força de trabalho de 433.575 pessoas e despende por ano cerca de 100 bilhões de reais. Calcula-se que, ainda que não houvesse ingresso de novas ações judiciais e fosse mantida a produtividade dos magistrados e dos servidores, seriam necessários aproximadamente 2 anos e 8 meses de trabalho para zerar o estoque de processos (CNJ, 2021a). O resultado é, portanto, a sobrecarga de trabalho dos servidores públicos e a demora do cidadão para obter respostas da justiça. Tais dados mostram a necessidade de buscar soluções inovadoras para aumentar o desempenho e a eficiência do serviço prestado, aperfeiçoando assim o acesso à justiça e fortalecendo a confiança da população.

Apesar dos esforços empreendidos sob a perspectiva da administração da justiça, a percepção da sociedade brasileira sobre a atuação do Judiciário ainda é marcada pelas ideias de morosidade e burocracia, conforme estudo da imagem do Poder Judiciário brasileiro finalizado no ano de 2019. Verificou-se que 54% da sociedade considera que a justiça funciona mal ou muito mal e, dentre as razões que desestimulam a busca por serviços judiciais, 64% entendem que “a Justiça é muito lenta e burocrática”. Um dos fatores que certamente conduz a tal conclusão é a percepção de 69% dos entrevistados de que “a Justiça não tem um funcionamento moderno” (AMB, FGV e IPESPE, 2020).

A transformação desse cenário objetivando uma melhor qualidade dos serviços do sistema de justiça, a qual tem sido impulsionada ainda pela adaptação forçada à pandemia COVID-19, atravessa a gestão e o uso de novas soluções de tecnologia, sobretudo da inteligência artificial (IA).

2. Quais contribuições podem ser aportadas pela inteligência artificial?

A inteligência artificial (IA) não corresponde a uma única ferramenta. Pelo contrário, seu conceito designa soluções tecnológicas – que agrupam redes neurais artificiais, algoritmos, sistemas de aprendizado, *big data*, entre outros – capazes de realizar atividades de um modo considerado similar às capacidades cognitivas humanas (CNJ, 2019). Em outras palavras, a IA é um conjunto de ciências e técnicas matemáticas, estatísticas e de ciência da computação que permite processar grandes volumes de dados para projetar tarefas de processamento computacional muito complexas (CEPEJ, 2019).

Os avanços na capacidade computacional, o aumento da disponibilidade de dados e a redução dos custos operacionais têm impulsionado a difusão do desenvolvimento e do uso da IA, inclusive no setor público.

Somam-se, ainda, os potenciais apresentados pelas técnicas de processamento de linguagem natural e de aprendizado de máquina, permitindo esta última que as máquinas aprendam e façam previsões a partir de dados históricos, com base na identificação de padrões, sem exigir para tanto as instruções prévias de um agente humano (CAF, 2021).

Dentre as capacidades da IA, destacam-se: (1) a automatização de tarefas repetitivas e burocráticas; (2) a precisão na execução dos comandos, sobretudo por sua capacidade de processar grandes volumes de dados simultaneamente e responder com rapidez; (3) a detecção de forma lógica – dentro de parâmetros para os quais foi programada – para captura de detalhes em tarefas que requerem um alto nível de atenção; (4) a predição para apoiar a tomada de decisões, com base em técnicas de simulação e modelagem, que informam sobre tendências e possíveis consequências de determinadas escolhas; (5) e o controle e a otimização de processos, através da análise de dados de várias fontes para obter uma visão integrativa que permite identificar possíveis ajustes nos fluxos de trabalho e, conseqüentemente, melhorar a eficiência dos sistemas utilizados (CAF, 2021).

No contexto do Poder Judiciário, tais habilidades podem contribuir para o aprimoramento da administração da justiça e a redução de custos, bem como para a celeridade, a assertividade e a coerência nos processos de tomada de decisão, tornando mais justas as respostas às demandas apresentadas pelos cidadãos.

3. Usos da inteligência artificial nos tribunais do Brasil

O uso da IA já é uma realidade no Poder Judiciário, e a perspectiva é de que os tribunais brasileiros implementem cada vez mais ferramentas que façam uso dessa tecnologia. O objetivo é, sobretudo, dar suporte às equipes de trabalho nas atividades administrativas, assim como apoiar a tomada de decisão e a produção textual.

Em levantamento realizado no ano de 2020 pela Fundação Getúlio Vargas, observou-se que cerca de metade dos tribunais brasileiros possuía projeto de inteligência artificial em desenvolvimento ou já implantado, totalizando à época 64 projetos em 47 tribunais, além da plataforma Sinapses do CNJ. Estima-se que o êxito na implementação de tais soluções tecnológicas possa melhorar os impactos econômicos e sociais atrelados à atuação judicial e, ao mesmo tempo, assegurar o cumprimento dos deveres organizacionais e constitucionais do Poder Judiciário (FGV, 2020).

Para tanto, dentre as funcionalidades contempladas pelos projetos de IA identificados no estudo, está o agrupamento de processos por similaridade, o que permite, por exemplo, agilizar a identificação e a análise dos feitos, tomar ações em bloco e conferir maior isonomia no julgamento de processos semelhantes. Documentos processuais isolados podem igualmente ser identificados por similaridade.

Técnicas de identificação de padrões, classificação e recomendação também têm sido amplamente utilizadas. Alguns projetos classificam as petições iniciais através do uso da técnica de processamento de linguagem natural e podem, de forma automatizada, sugerir classes e assuntos judiciais a partir do conteúdo identificado para fins de distribuição conforme o ramo do direito, facilitando assim a triagem e evitando a necessidade de redistribuição por incompetência, por exemplo. De igual modo, pode ser sugerida, com base na convergência com o conteúdo identificado, a vinculação do processo a temas de precedentes. Pode ser sugerido ao advogado peticionante o tipo da petição intermediária a ser juntada de acordo com o seu inteiro teor. Ou mesmo o movimento processual que pode ser aplicado no despacho, tais como gratuidade de justiça, mero expediente, dentre outros.

O uso da IA permite ainda auxiliar na identificação de casos de prevenção, na verificação das hipóteses de improcedência liminar do pedido ou mesmo na realização do juízo de admissibilidade dos recursos nos moldes enumerados pelo Código de Processo Civil.

Com relação à produção textual, avança-se para a sugestão e elaboração de minutas, de forma a facilitar e padronizar a edição de documentos. Assim, a solução tecnológica pode identificar a situação processual, buscar exemplos anteriores dentro da mesma jurisdição e, inclusive, prever qual tipo de decisão ou despacho deverá ser proferido na etapa do processo judicial. O teor do texto jurídico pode de igual modo ser objeto de sugestão.

A análise preditiva encontra-se, igualmente, em projetos que pretendem observar a probabilidade de reversão de sentenças ou acórdãos ou de sucesso em audiências de conciliação, para apoiar a seleção de processos com maior potencial de êxito.

Facilitando o andamento processual, mandados podem ser confeccionados e distribuídos de forma automatizada conforme classificação por urgência, natureza, complexidade e geolocalização dos endereços. A penhora online pode da mesma forma ser realizada com ajuda da IA, que executa as ações de consulta, bloqueio e desbloqueio no sistema Bacenjud a partir do teor do expediente do magistrado. A mesma técnica pode, ainda, ser replicada em outros procedimentos internos dos tribunais que impliquem interação com sistemas externos.

Com o fim de otimizar o atendimento aos advogados e ao público, foram desenvolvidos *chatbots* que, através de algoritmos de IA, simulam uma conversa humana de forma pré-definida com o usuário e automatizam tarefas repetitivas.

No âmbito da gestão administrativa do Judiciário, ferramentas de IA podem viabilizar a análise de dados para comparações, *insights* e previsões de performance de determinada unidade jurisdicional com base em informações do passado.

Os projetos ainda abarcam ações que vão do apoio na resolução de disputas online a sistemas de reconhecimento facial nos tribunais, do cálculo de prazos prescricionais à transcrição de voz para texto de audiências. Como é possível inferir das funcionalidades acima elencadas, o resultado do estudo mostra que as aplicações de IA incidem nas mais diversas áreas do sistema de justiça.

Tais tecnologias ainda estão em fase incipiente, de modo que a tendência é que os projetos avancem e se expandam a âmbitos cada vez mais distintos do Judiciário.

4. A importância da boa governança e de diretrizes éticas

Para além das oportunidades apresentadas, a IA traz consigo novos desafios éticos, legais e de governança. Os avanços objetivados pelo uso da tecnologia precisam estar alinhados aos valores e princípios do Poder Judiciário e, sobretudo, devem ser implementados a serviço dos cidadãos. É por isso que as estratégias de abordagem e as estruturas normativas devem dispor sobre o design, o desenvolvimento, a implementação e a avaliação das ferramentas de IA no sistema de justiça.

A análise dos benefícios esperados com o sucesso da inovação deve ponderar também os potenciais riscos associados. Tais questões envolvem, dentre tantas outras: a transparência e a explicabilidade para entender como a IA chegou a determinado resultado; os potenciais vieses em dados utilizados para treinar e testar os modelos de IA que podem perpetuar desigualdades sociais; as salvaguardas para garantir a preservação da privacidade e o uso adequado dos dados pessoais; a definição de papéis e de responsabilidades das equipes envolvidas a fim de viabilizar a prestação de contas; os custos para construção e manutenção da infraestrutura de IA e os eventuais prejuízos causados no caso de falha técnica ou se a implantação da ferramenta falhar; a concentração no desempenho quantitativo dos tribunais em detrimento do desempenho qualitativo; a necessidade de preservar o julgamento humano e a autonomia dos juízes; ou mesmo o risco de a jurisprudência estagnar e ficar imune às revisões e evoluções necessárias (CEPEJ, 2016; VIDHI, 2021).

É nesse contexto que o ecossistema digital para viabilizar – ética e tecnicamente – o uso da IA pela justiça brasileira demanda regulamentação. Sob um viés ético, envolve um conjunto de valores, princípios e técnicas que empreguem padrões amplamente aceitos para orientar a conduta moral no desenvolvimento e uso da IA, atentando assim aos danos individuais e sociais que podem ser ocasionados (OAI, 2020). Já quanto à perspectiva técnica, a governança abrange o estabelecimento de políticas e práticas padronizadas para gerenciar as tecnologias de IA no Poder Judiciário, incluindo definições relacionadas a pessoas, processos, dados e algoritmos.

As normativas são, portanto, primordiais para garantir que a IA seja utilizada pelo Judiciário de forma eficiente, responsável e garantindo, ao mesmo tempo, a confiança do público no funcionamento do sistema.

5. Quadro normativo para uso da inteligência artificial no Poder Judiciário

Com o objetivo de criar um panorama das iniciativas já existentes no Brasil para orientar o uso da IA no sistema de justiça, serão apresentadas as disposições voltadas ao estabelecimento de diretrizes éticas e, posteriormente, à estruturação tecnológica.

O Conselho Nacional de Justiça (CNJ) tem a competência para normatizar o Poder Judiciário. No exercício de suas atividades, ao longo dos últimos anos, o órgão implementou distintas políticas com o objetivo de impulsionar a transformação digital por meio de serviços e soluções digitais inovadoras – uma necessidade diante do contexto pandêmico – e de viabilizar a modernização da infraestrutura necessária para o aperfeiçoamento das ferramentas de IA.

A regulamentação sobre IA no âmbito do Poder Judiciário deu-se, inicialmente, por meio da Resolução CNJ n° 332/2020, a qual dispôs sobre ética, transparência e governança na produção e no uso de IA, e da Portaria CNJ n° 271/2020, que também aprimora a governança e busca harmonizar as ações como um todo de desenvolvimento de projetos de IA nos tribunais do país.

As normativas pretendem, em um primeiro momento, definir as funcionalidades que efetivamente constituem IA. Para tanto, através da Resolução CNJ n° 332/2020, conceituou-se como modelo de IA o conjunto de dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana. Ademais, estipulou-se, por meio da Portaria CNJ n° 271/2020, que devem ser considerados como de IA os projetos voltados a: (1) criar soluções para automação dos processos judiciais e administrativos e de rotinas de trabalho da atividade judiciária; (2) apresentar análise da massa de dados existentes no âmbito do Poder Judiciário; e (3) prover soluções de apoio à decisão dos magistrados ou à elaboração de minutas de atos judiciais em geral.

O uso de IA em um campo sensível como a justiça, como visto acima, demanda a identificação, a avaliação e o monitoramento constante de danos potenciais, bem como o estabelecimento de princípios éticos que guiem o uso adequado ao longo do ciclo de vida das ferramentas. Por isso, a Resolução CNJ n° 332/2020 inspirou-se nos princípios da Carta Ética sobre o Uso da IA em Sistemas Judiciais e seu Ambiente no âmbito da União Europeia e foi dividida em capítulos que versam sobre: (1) respeito aos direitos fundamentais; (2) não discriminação; (3) publicidade e transparência; (4) governança e qualidade; (5)

segurança; (6) controle do usuário; (7) pesquisa, desenvolvimento e implantação de serviços de IA; (8) prestação de contas e responsabilização.

De acordo com a normativa, a IA deve ser utilizada, no âmbito do Poder Judiciário, com o objetivo de promover o bem-estar dos jurisdicionados e a prestação equitativa da jurisdição, bem como descobrir métodos e práticas que possibilitem a consecução desses objetivos.

No capítulo sobre o respeito aos direitos fundamentais, há a determinação de que o uso da IA seja compatível, especialmente, com os direitos dispostos na Constituição Federal e nos tratados internacionais de que o Brasil seja parte. Nesse sentido, deverá ser garantida a segurança jurídica e o respeito à igualdade de tratamento a casos absolutamente iguais. Estipulou-se, ainda, que, quando o desenvolvimento e treinamento de modelos de IA exigir a utilização de dados, as amostras deverão ser representativas e observar as cautelas necessárias quanto aos dados pessoais sensíveis e ao segredo de justiça.

Os potenciais danos na utilização de ferramentas de IA no sistema de justiça podem envolver, por exemplo, resultados não transparentes, inexplicáveis, não confiáveis, discriminatórios ou de baixa qualidade (LESLIE, 2019).

Com o objetivo de mitigar tais riscos, o capítulo sobre não discriminação dispõe que as decisões judiciais apoiadas em ferramentas de IA devem preservar a igualdade, a pluralidade e a solidariedade, auxiliando no julgamento justo com a criação de condições que visem eliminar ou, ao menos, minimizar a opressão, a marginalização do ser humano e os erros de julgamento decorrentes de preconceitos.

Sem prever especificamente a realização de uma avaliação de risco, a normativa estabelece que, antes de ser colocado em produção, o modelo de IA deve ser homologado a fim de identificar se preconceitos ou generalizações influenciaram seu desenvolvimento, acarretando ou não tendências discriminatórias no seu funcionamento. Caso seja verificado viés discriminatório ou incompatibilidade com os princípios da Resolução CNJ nº 332/2020, deverão ser adotadas medidas corretivas. Contudo, se não for possível eliminar o viés discriminatório identificado no modelo, sua utilização será descontinuada e serão realizados os devidos registros sobre o projeto e as razões que levaram a tal decisão.

O capítulo sobre publicidade e transparência, por sua vez, atenta para a importância de estabelecer uma boa comunicação com os futuros usuários e todos aqueles que possam ser afetados pelas novas tecnologias (CEPEJ, 2016). Por isso, houve a definição de que a transparência no uso de IA no Poder

Judiciário abrange: (1) divulgação responsável, considerando a sensibilidade própria dos dados judiciais; (2) indicação dos objetivos e resultados pretendidos pelo uso do modelo de IA; (3) documentação dos riscos identificados e indicação dos instrumentos de segurança da informação e controle para seu enfrentamento; (4) possibilidade de identificação do motivo em caso de dano causado pela ferramenta de IA; (5) apresentação dos mecanismos de auditoria e certificação de boas práticas; e (6) fornecimento de explicação satisfatória e passível de auditoria por autoridade humana quanto a qualquer proposta de decisão apresentada pelo modelo de IA, especialmente quando essa for de natureza judicial.

Estimulando a transparência técnica, a Portaria CNJ nº 271/2020 também estipulou que os modelos de IA utilizados para auxiliar a atuação do Judiciário na apresentação de análises, de sugestões ou de conteúdo devem, necessariamente, adotar medidas que possibilitem o rastreamento e a auditoria das predições realizadas no fluxo de sua aplicação.

Com relação à governança e qualidade, o capítulo próprio da Resolução CNJ nº 332/2020 dispôs que qualquer modelo de IA que venha a ser adotado pelos órgãos do Poder Judiciário deverá observar as regras de governança de dados aplicáveis aos seus próprios sistemas computacionais, bem como as demais resoluções e recomendações do CNJ, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e o segredo de justiça.

No intuito de harmonizar o desenvolvimento dos projetos no país, determinou-se que os órgãos do Poder Judiciário deverão informar ao CNJ a pesquisa, o desenvolvimento, a implantação ou o uso da IA, bem como as necessidades que ensejaram sua criação e os respectivos objetivos e resultados que se pretendem alcançar.

A normativa busca ainda promover esforços para atuação em modelo comunitário, evitando a duplicidade de projetos similares e demonstrando preocupação com o gasto de recursos financeiros que decorrem da manutenção de diversos sistemas para a mesma finalidade entre os órgãos do sistema de justiça. Por isso, foi vedado o desenvolvimento paralelo quando a iniciativa possuir objetivos e resultados alcançados idênticos a outro modelo de IA já existente ou com projeto em andamento.

Foi disposto ainda, de modo complementar pela Portaria CNJ nº 271/2020, que o uso de IA deve se dar em uma plataforma comum, acessível por todos, que incentive a colaboração, a transparência, o aprimoramento e a divulgação dos projetos: o Sinapses, cujas funcionalidades serão em breve elencadas. As-

sim, a documentação dos projetos e os modelos de IA, os quais por determinação devem possuir interface de programação de aplicativos (API) que permita sua utilização por outros sistemas, serão todos depositados na Plataforma Sinapses.

No capítulo sobre segurança, estipulou-se que os dados utilizados no processo de treinamento de modelos de IA devem ser provenientes de fontes seguras, preferencialmente governamentais, e ser eficazmente protegidos contra os riscos de destruição, modificação, extravio ou mesmo acessos e transmissões não autorizados.

Já o capítulo que versa sobre o controle do usuário estabelece mecanismos para garantir a autonomia e o controle pelos usuários internos do sistema de IA. Os modelos em uso devem, portanto, proporcionar incremento no exercício das atividades no sistema de justiça – e não restrição – e possibilitar a revisão da proposta de decisão e dos dados utilizados para sua elaboração, sem que haja qualquer espécie de vinculação à solução apresentada pela IA. Ou seja, a solução não deve possuir caráter vinculante e será sempre submetida à análise da autoridade competente. Os usuários externos, por sua vez, devem ser devidamente informados, em linguagem clara e precisa, quanto à utilização de sistemas inteligentes nos serviços que lhes forem prestados.

Ademais, há previsão de que os sistemas computacionais que utilizem modelos de IA como ferramenta auxiliar para a elaboração de decisão judicial observarão, como critério preponderante para definir a técnica utilizada, a possibilidade de explicação dos passos que conduziram ao resultado.

Com relação à pesquisa, desenvolvimento e implantação de serviços de IA, o capítulo prevê que a composição de equipes responsáveis será orientada pela busca da diversidade em seu mais amplo espectro, incluindo gênero, raça, etnia, cor, orientação sexual, pessoas com deficiência, geração e demais características individuais. Ademais, tal participação representativa deve estar presente em todo o ciclo de vida do processo, do planejamento ao processamento dos dados, da construção à implementação dos modelos, tanto nas áreas técnicas como negociais.

Atentando para áreas em que o uso de IA revela-se de elevado risco, a normativa estabelece que modelos que utilizem técnicas de reconhecimento facial exigirão prévia autorização do CNJ para implementação. No mesmo sentido, as ferramentas de IA em matéria penal não devem ser estimuladas, sobretudo com relação à sugestão de modelos de decisões preditivas, excetuando-se especificamente as soluções computacionais destinadas à auto-

mação e ao oferecimento de subsídios destinados ao cálculo de penas, prescrição, verificação de reincidência, mapeamentos, classificações e triagem dos autos para fins de gerenciamento de acervo.

A Portaria CNJ nº 271/2020 acrescenta ainda, quanto às demais orientações acerca da pesquisa e do desenvolvimento em matéria de IA, 08 (oito) critérios que devem ser observados: a economicidade; a transparência; o acesso à informação; a interoperabilidade tecnológica dos sistemas processuais eletrônicos; a adoção de tecnologias, padrões e formatos abertos e livres; a capacitação humana e sua preparação para a reestruturação dos fluxos processuais e de trabalho; o foco na celeridade processual; e, ainda, o estabelecimento de mecanismos de governança colaborativa e democrática, com a participação do Poder Judiciário, daqueles que exercem funções essenciais à justiça, da comunidade acadêmica e da sociedade civil.

Por fim, há o capítulo final sobre prestação de contas e responsabilização. Com o fim de garantir o impacto positivo para os usuários finais e para a sociedade, determina-se que toda e qualquer solução do Poder Judiciário que utilize modelos de IA deve assegurar total transparência na prestação de contas.

A prestação de contas compreende, segundo o texto, os nomes dos responsáveis pela execução das ações, os custos totais envolvidos no projeto, a existência de ações de colaboração e cooperação entre os agentes do setor público ou desses com a iniciativa privada ou a sociedade civil, os resultados pretendidos e os que foram efetivamente alcançados, assim como a demonstração de efetiva publicidade quanto à natureza do serviço oferecido, técnicas utilizadas, desempenho do sistema e riscos de erros.

No que diz respeito à responsabilização, determinou-se que o desenvolvimento ou o uso de IA em desconformidade aos princípios e regras estabelecidos na normativa será objeto de apuração e, sendo o caso, punição dos responsáveis.

Por fim, no intuito de acompanhar os resultados dos projetos desenvolvidos no país e garantir o cumprimento das disposições acima elencadas, os órgãos do Poder Judiciário precisarão informar ao CNJ todos os registros de eventos adversos no uso da IA. No mesmo sentido, determinou-se na Portaria CNJ nº 271/2020 que os sistemas judiciais que fizerem uso dos modelos de IA devem informar eventual discordância quanto ao uso das predições – a ideia é que tal retorno poderá torná-los mais precisos ou mesmo corrigir eventuais falhas encontradas.

Cabe pontuar que, com relação ao respeito à privacidade e seus potenciais reflexos no uso da IA, houve a publicação da Resolução CNJ n° 363/2021, a qual estabelece medidas para o processo de adequação dos tribunais à Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709/2018). De igual modo, foi instituído pela Resolução CNJ n° 334/2020 o Comitê Consultivo de Dados Abertos e Proteção de Dados no âmbito do Poder Judiciário, com o objetivo de compatibilizar a política de dados abertos com a proteção de dados pessoais.

À vista disso, considerando o conjunto de princípios dispostos pela Resolução CNJ n° 332/2020, constata-se que há convergência com os principais documentos publicados no mundo que visam fornecer normas de orientação sobre sistemas baseados em IA. Isso porque, segundo estudo realizado pelo Centro Berkman Klein para Internet e Sociedade da Universidade de Harvard (2020), os 08 (oito) temas principais que representam o núcleo normativo de uma abordagem baseada em princípios para a ética e governança da IA abarcam questões substanciais sobre: promoção de valores humanos; justiça e não discriminação; transparência e explicabilidade; proteção e segurança; controle humano da tecnologia; responsabilidade profissional; prestação de contas; e privacidade.

Sucedo que, para além das diretrizes éticas, a coordenação estratégica dos projetos de IA entre todos os 91 tribunais brasileiros demanda por certo um olhar mais amplo. As normativas ora mapeadas estabelecem a estruturação tecnológica para o uso da IA no Poder Judiciário. Envolve, para além da ferramenta em si, uma transformação cultural e estrutural com o avanço da transformação digital, a migração dos serviços prestados e dos processos físicos para o meio eletrônico, a integração dos diferentes sistemas processuais no país e a ampliação dos bancos de dados.

A transformação digital é, justamente, um dos objetivos da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), disciplinada pela Resolução CNJ n° 370/2021. As ações elencadas para o sexênio 2021-2026 têm como meta promover a melhoria da governança, da gestão e da colaboração tecnológica.

No mesmo ano, foi instituída também a Política de Gestão da Inovação no âmbito do Poder Judiciário, através da Resolução CNJ n° 395/2021, que busca aprimorar as atividades dos órgãos judiciários por meio da difusão da cultura da inovação, com a modernização de métodos e técnicas de desenvolvimento do serviço judiciário, de forma coletiva e inclusive em parceria com atores externos. Para tanto, houve inclusive a criação da Rede de Inovação do Poder Judiciário Brasileiro (RenovaJud).

Nesse contexto, para produzir um diagnóstico do grau de inovação dos tribunais brasileiros e aferir o nível de cumprimento das diretrizes estratégicas, a Portaria CNJ nº 211/2021 criou o Índice de Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação do Poder Judiciário (iGovTIC-JUD). A meta é que, até dezembro de 2026, no mínimo 75% dos órgãos do Poder Judiciário alcancem um nível de maturidade satisfatório.

Dentre os levantamentos do iGovTIC-JUD, estão justamente questões que buscam saber sobre a existência de ações nos tribunais para desenvolver modelos de IA, se há incentivo da alta administração para tanto ou, até mesmo, se existem processos para assegurar a realização de estudos, pesquisas, ensino e treinamentos de IA livre de preconceitos (CNJ, 2021b).

Ainda no primeiro semestre de 2021, teve início o Programa Justiça 4.0, resultado de uma parceria entre o CNJ, o Conselho da Justiça Federal (CJF) e o Programa das Nações Unidas para o Desenvolvimento (PNUD), com o intuito de ampliar o acesso da população brasileira à justiça, dar celeridade à prestação jurisdicional e promover a redução de despesas orçamentárias.

O programa busca transformar a justiça em um serviço, seguindo o conceito de *justice as a service* (Jaas), para além de suas estruturas físicas como os conhecidos ‘fóruns’. Por isso, estabelece uma atuação estratégica de iniciativas digitais, através de um conjunto de ações e projetos desenvolvidos para o uso colaborativo de produtos a fim de ampliar o uso de novas tecnologias e de IA no Poder Judiciário (CNJ, 2021a).

Dentre as iniciativas que o Programa Justiça 4.0 pretende criar ou aperfeiçoar estão: a Plataforma Sinapses, a Base Nacional de Dados do Poder Judiciário (DataJud), o sistema Codex, a Plataforma Digital do Poder Judiciário (PDPJ-Br), o Juízo 100% Digital, o Balcão Virtual e os Núcleos de Justiça 4.0.

A Plataforma Sinapses, acima já mencionada e instituída pela Resolução CNJ nº 332/2020, busca centralizar o armazenamento, o treinamento supervisionado, o controle de versionamento, a disponibilização em larga escala e a auditoria dos modelos de IA do Poder Judiciário, criando assim uma “fábrica de modelos de IA”. Conforme regulamentado, os tribunais devem disponibilizar os modelos de IA na plataforma, os quais poderão ser aproveitados e operados por outros órgãos, de forma independente e adaptada ao contexto local, como se fossem microsserviços. Isso permite o ganho de escala, a economia de recursos humanos e financeiros e a construção de um ecossistema de serviços de IA (CNJ, 2019).

O que o Programa Justiça 4.0 busca é aprimorar e disseminar o uso da Plataforma Sinapses pelos tribunais brasileiros. Uma das barreiras para a governança do uso da IA é, justamente, a descentralização dos projetos existentes e a ausência de padronização dos sistemas processuais eletrônicos utilizados (SIPA, 2020). Embora o PJe seja o sistema oficial do Poder Judiciário, os projetos de IA têm sido desenvolvidos em grande parte para outros sistemas – e-Proc, e-SAJ, Projudi, entre outros –, razão pela qual a integração e a interoperabilidade pelo Sinapses tornam-se tão relevantes.

O Programa Justiça 4.0 objetiva também auxiliar os tribunais no processo de aprimoramento dos registros processuais primários, incluindo a consolidação, implantação, treinamento, limpeza e publicização dos dados para compor a Base de Dados Processuais do Poder Judiciário (DataJud).

A criação de ferramentas de IA demanda quantidades expressivas de dados confiáveis para criar e treinar seus algoritmos, por isso a integração de dados oriundos de diferentes fontes e com diferentes formatos e semântica em registros mostra-se muito significativa (SIPA, 2020). O DataJud foi criado pela Resolução CNJ nº 331/2020 para ser a grande base de dados dos tribunais do Brasil, centralizando os dados e metadados processuais relativos a todos os processos físicos ou eletrônicos em tramitação no país.

De modo complementar, o sistema Codex, que o Programa Justiça 4.0 busca implementar, possui duas funções principais: alimentar o DataJud de forma automatizada e transformar em texto puro as decisões e petições apresentadas nos tribunais, a fim de que possam ser utilizadas como insumo de soluções de IA (CNJ, 2021a). Instituído pela Resolução CNJ nº 446/2022 como ferramenta oficial de extração de dados dos processos judiciais eletrônicos em tramitação no Poder Judiciário, o Codex funciona como um *data lake* de informações processuais e é responsável por consolidar os metadados e dados disponíveis sobre os processos em uma base que engloba tanto os dados estruturados, como os dados não estruturados – a exemplo do conteúdo textual de peças e de documentos.

O projeto da Plataforma Digital do Poder Judiciário (PDPJ-Br), por sua vez, possibilita ampliar o grau de automação do processo judicial eletrônico e o uso de IA pelos tribunais. A plataforma foi criada pela Resolução CNJ nº 335/2020, a qual instituiu uma política pública para a governança e a gestão de processo judicial eletrônico, integrando todos os tribunais do país através da PDPJ-Br.

A plataforma deve servir como um *marketplace* de soluções tecnológicas que estará disponível para uso pelos tribunais brasileiros. A ideia é que todos os distintos sistemas judiciais de processo eletrônico possam se conectar à PDPJ-Br e, nesse ambiente unificado e de forma comunitária, compartilhar e consumir as soluções tecnológicas oferecidas como microsserviços, aplicações e modelos de IA, por meio da computação em nuvem (CNJ, 2021c). A Plataforma Sinapses integra justamente a PDPJ-Br.

Conforme consta da normativa, dentre outras características, as soluções da plataforma deverão ser adaptáveis ao uso de ferramentas de aprendizado de máquina e de IA, permitir a automação de atividades rotineiras, ter como foco prioritário a redução da taxa de congestionamento dos processos e significativa melhora na qualidade dos serviços prestados e utilizar, preferencialmente, tecnologias de código aberto. Cria-se, assim, um cenário próspero para o avanço do uso das ferramentas de IA em todo o sistema de justiça.

As demais iniciativas do Programa Justiça 4.0 consistem na implementação do Juízo 100% Digital, do Balcão Virtual e dos Núcleos de Justiça 4.0, dispostas respectivamente pelas Resoluções n° 345/2020, n° 372/2021, e n° 385/2021 do CNJ. Tais projetos permitem que todos os atos processuais sejam praticados por meio eletrônico e remoto, com um ambiente virtual de atendimento totalmente digital.

Outras normativas recentemente publicadas pelo CNJ, as quais também fortalecem o cenário inovador para o desenvolvimento das ferramentas de IA, incluem previsões sobre: a criação do Centro de Inteligência do Poder Judiciário com o objetivo de identificar e propor tratamento adequado de demandas estratégicas ou repetitivas e de massa (CNJ n° 349/2020); a realização de audiências e sessões por videoconferência e telepresenciais, bem como a comunicação de atos processuais por meio eletrônico (Resolução CNJ n° 354/2020); a criação de soluções tecnológicas para a resolução de conflitos por meio da conciliação e mediação (Resolução CNJ n° 358/2020); a conclusão da digitalização do acervo processual físico dos tribunais em eletrônico de forma integral até o final do ano de 2025 (Resolução CNJ n° 420/2021); e a criação do Banco Nacional de Precedentes (BNP) como repositório e plataforma tecnológica unificada de pesquisa textual e estatística (Resolução CNJ n° 444/2022).

Por fim, cabe reparar que as ações acima analisadas, ao integrarem o movimento de promoção do desenvolvimento tecnológico e da inovação no setor público, estão alinhadas com a Lei do Governo Digital (Lei n° 14.129/2021) e com a Estratégia Brasileira de Inteligência Artificial (Portaria MCTI n° 4.617/2021).

Considerações finais

A exposição acima buscou contextualizar as orientações normativas para o uso de IA no sistema de justiça brasileiro, sobretudo através das resoluções publicadas pelo CNJ.

Ponderou-se sobre as oportunidades que as ferramentas inteligentes podem gerar no contexto do Poder Judiciário, através do aprimoramento da administração da justiça, da otimização de recursos – orçamentários e humanos – e da possibilidade de alcançar maior celeridade e equidade nos processos de tomada de decisão.

Como visto, grande parte dos 91 tribunais do país já possui soluções de IA, segundo os parâmetros conceituais estabelecidos pelo CNJ. Os projetos implementados ou ainda em desenvolvimento abrangem distintas funcionalidades em áreas administrativas e jurisdicionais, desde o apoio à produção textual ao agrupamento inteligente dos acervos processuais.

Uma vez que tais projetos têm avançado rapidamente no curso dos últimos anos, é preciso compreender a importância de regulamentar o uso da IA na justiça brasileira. Em que pese os benefícios identificados, deve-se atentar para os riscos e os novos desafios éticos e legais que também emergem. O estabelecimento de uma boa governança e de diretrizes éticas faz-se, portanto, necessário para garantir que tais inovações tecnológicas sejam implementadas a serviço dos cidadãos e estejam alinhadas aos valores e princípios do Poder Judiciário.

Nesse sentido, elaborou-se um panorama das iniciativas já existentes no Brasil para orientar o uso da IA no sistema de justiça. Foram apresentadas as disposições voltadas ao estabelecimento de diretrizes éticas e de regras de governança, com destaque para a Resolução CNJ nº 332/2020 e a Portaria CNJ nº 271/2020. Por fim, foram levantadas as normativas relacionadas à estruturação tecnológica dos tribunais a fim de consolidar um ambiente adequado para a inovação e o desenvolvimento de soluções de IA.

Referências bibliográficas

AMB (Associação dos Magistrados Brasileiros); FGV (Fundação Getúlio Vargas); (IP-ESPE) Instituto de Pesquisas Sociais, Políticas e Econômicas. Estudo da Imagem do Judiciário Brasileiro. 2019. Disponível em: <https://www.amb.com.br/wp-content/uploads/2020/04/ESTUDO_DA_IMAGEM_DO_JUDICIARIO_BRASILEIRO_COMPLETO.pdf>. Acesso em: 28 nov. 2021.

BKC (Centro Berkman Klein para Internet e Sociedade). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI. 2020. Disponível em: <https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y>. Acesso em: 23 dez. 2021.

CAF (Banco de Desenvolvimento da América Latina). Experiencia: Datos e Inteligencia Artificial en el sector público. 2021. Disponível em: <<https://scioteca.caf.com/handle/123456789/1793>>. Acesso em: 30 nov. 2021.

CEPEJ (Comissão Europeia para a Eficiência da Justiça). Guidelines on how to drive change towards Cyberjustice. 2016. Disponível em: <<https://rm.coe.int/16807482de>>. Acesso em: 08 dez. 2021.

_____. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. 2019. Disponível em: <<https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>>. Acesso em: 30 nov. 2021.

CNJ (Conselho Nacional de Justiça). Inteligência Artificial no Poder Judiciário. 2019. Disponível em: <<https://bibliotecadigital.cnj.jus.br/jspui/bitstream/123456789/98/1/Intelig%c3%aancia%20Artificial%20no%20Poder%20Judiciario%20Brasileiro.pdf>>. Acesso em: 30 nov. 2021.

_____. Justiça em números 2021. 2021a. Disponível em <<https://www.cnj.jus.br/wp-content/uploads/2021/10/relatorio-justica-em-numeros2021-081021.pdf>>. Acesso em: 28 nov. 2021.

_____. Manual do Índice em Governança, Gestão e Infraestrutura de TIC do Poder Judiciário. 2021b. Disponível em: <<https://atos.cnj.jus.br/files/compilado121715202109036132124bc64c8.pdf>>. Acesso em: 09 dez. 2021.

_____. Justiça 4.0. 2021c. Disponível em: <<https://www.cnj.jus.br/wp-content/uploads/2021/08/cartilha-justica-4-0-20082021-vs-ml-dn-fp.pdf>>. Acesso em: 10 dez. 2021.

FGV (Fundação Getúlio Vargas). Inteligência Artificial: tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário brasileiro. 2020. Disponível em: <https://ciapj.fgv.br/sites/ciapj.fgv.br/files/estudos_e_pesquisas_ia_1afase.pdf>. Acesso em: 30 nov. 2021.

LESLIE, David. Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute. 2019. Disponível em: <https://www.turing.ac.uk/sites/default/files/2019-08/understanding_artificial_intelligence_ethics_and_safety.pdf>. Acesso em: 21 dez. 2021.

OAI (Office for Artificial Intelligence). A guide to using artificial intelligence in the public sector. 2020. Disponível em: <<https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector>>. Acesso em: 08 dez. 2021.

SIPA (School of International and Public Affairs) Capstone. The Future of AI in The Brazilian Judicial System-AI Mapping, Integration and Governance. 2020. Disponível em: <<https://itsrio.org/wp-content/uploads/2020/06/SIPA-Capstone-The-Future-of-AI-in-the-Brazilian-Judicial-System-1.pdf>>. Acesso em: 09 dez. 2021.

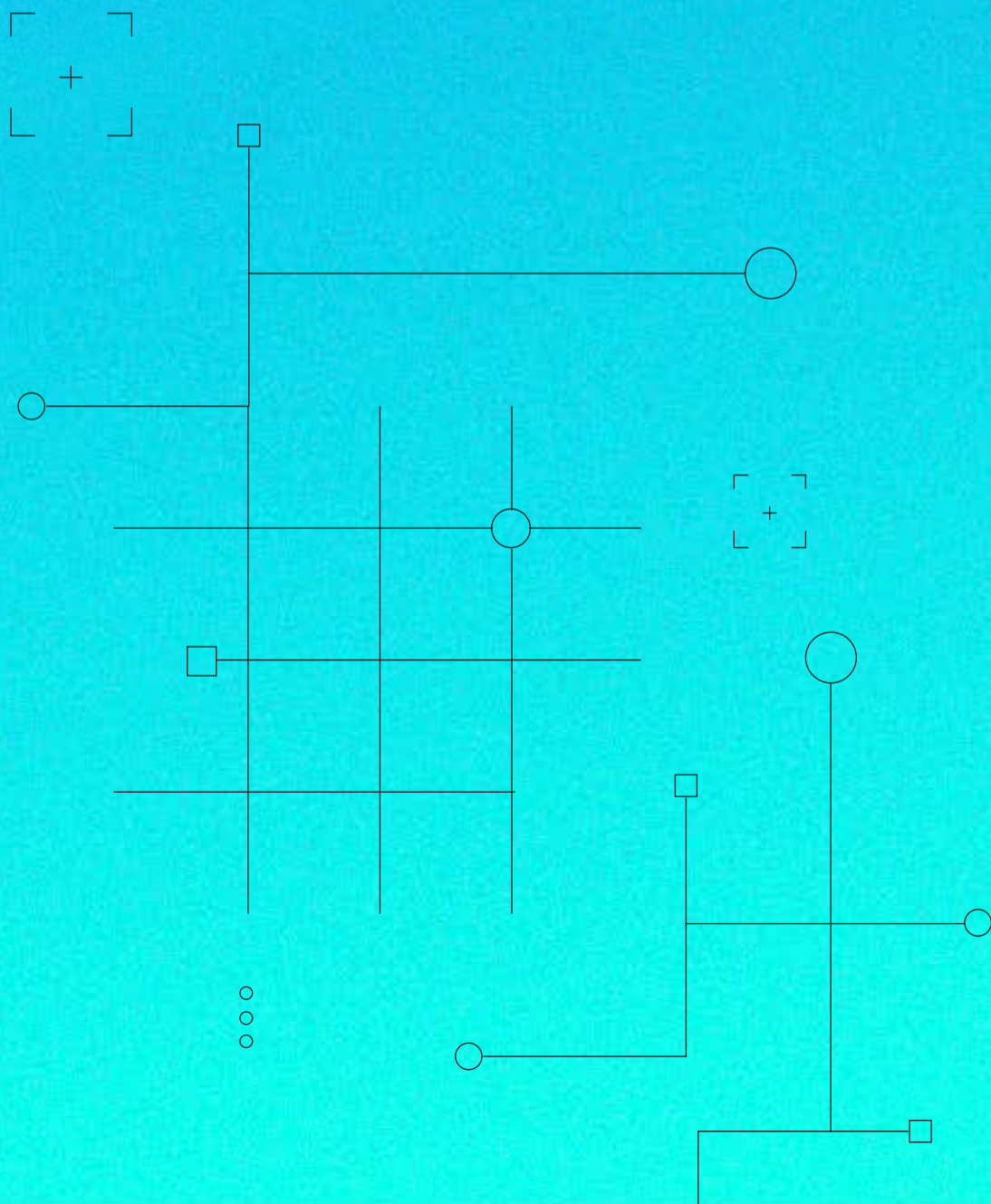
VIDHI (Vidhi Centre for Legal Policy). 2021. Responsible AI for the Indian Justice System – A Strategy Paper. Disponível em: <<https://vidhilegalpolicy.in/research/responsible-ai-for-the-indian-justice-system-a-strategy-paper>>. Acesso em: 08 dez. 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

2

Medicina de precisão e IA: implicações jurídicas

DAVI BRITO DE ALMEIDA



Sumário: Introdução. 1. Contexto político e econômico da medicina de precisão. 2. A IA na medicina de precisão: benefícios e malefícios. 3. Medicina de precisão e autonomia do médico. 4. Medicina de precisão e autodeterminação do paciente. 5. Medicina de precisão e IA: desafios no Brasil. Considerações finais. Referências.

Introdução

A humanidade passa por ciclos tecnológicos revolucionários, impulsionados por novas tecnologias transformadoras aplicadas ao cotidiano das pessoas. A Revolução Industrial 4.0, da contemporaneidade, está ligada estreitamente ao mundo digital: sistemas ciberfísicos, internet das coisas (IoT), inteligência artificial - IA (*Artificial Intelligence - AI*), aprendizado de máquina (*machine learning*), entre outras inovações.

Esses movimentos transformadores também atingiram o campo da medicina, permitindo o desenvolvimento da saúde inteligente (*smart health*). Assim, a medicina convencional ou tradicional do protocolo único (*one size fits all*) está sendo substituída pela medicina dos “4 Ps”: preventiva, preditiva, personalizada e proativa. Em outras palavras, os cuidados de saúde deixam de ser focados apenas na cura de patologias, abrangendo também medidas de prevenção de doenças, de antecipação de diagnósticos, de personalização de tratamentos e de atendimentos continuados (Neto e Nogaroli, 2020).

A transformação do atendimento médico nesse modelo “mais proativo, preventivo, preciso e centrado na individualidade de cada paciente tornou-se possível, nos últimos anos, a partir da combinação de grande volume de dados de saúde e *softwares* de inteligência artificial” (Neto e Nogaroli, 2020, p. 141).

É que não só os equipamentos diagnósticos se tornaram digitais, mas também o prontuário médico eletrônico passou a acumular informações clínicas, prescrições médicas e exames laboratoriais dos pacientes de forma mais detalhada. Ademais, *smartphones* e aparelhos digitais passaram a medir atividades físicas e sinais vitais ou ainda a registrar dietas de indivíduos. Isso possibilitou o compartilhamento e a acumulação de dados em grande volume, velocidade, variedade, veracidade e valor (*big data*), analisados por algoritmos fundados em IA, *machine learning* e *deep learning* (Ribeiro e Oliveira, 2019).

1. Mestrando do Programa de Mestrado Profissional em Direito, Regulação e Políticas Públicas da UnB/STJ. Pós-Graduação em Direito Digital (ITS Rio/UERJ/CEPED); Especialização em Assessoria Política, Governo e Políticas Públicas (IPol/UnB); LLM em Direito Empresarial (FGV). Analista Judiciário do TSE. E-mail: almeida.davi@gmail.com.

Paralelamente, com o sequenciamento do genoma humano e estudos de proteoma, metaboloma e transcriptoma, surgiram também novos saberes combinados, como a bioinformática (campo multidisciplinar que reúne genética, ciência da computação, matemática e estatística, isto é, uma ciência de dados voltada para solucionar problemas biológicos) e a farmacogenômica (desenvolvimento de fármacos adequados às características genéticas de subgrupos populacionais).

Para alguns estudiosos, o termo “medicina de precisão” e “medicina personalizada” são sinônimos, sendo mais indicado o primeiro, por traduzir melhor o sentido deste ramo médico (desenvolvimento de tratamentos e medidas preventivas específicos de estratos da população e não para o indivíduo em si):

De acordo com a definição de 2008 do National Research Council (NRC) norte-americano, a medicina de precisão “se refere à customização de tratamento médico para a característica individual de cada paciente. Isso não significa a criação de drogas ou dispositivos médicos que são específicos de um único paciente, mas sim a habilidade de classificar indivíduos em subpopulações que diferem na susceptibilidade a uma determinada doença ou na resposta a um tratamento específico. A prevenção ou intervenção terapêutica pode se concentrar naqueles que terão benefício, evitando gastos e efeitos adversos naqueles que não terão” (National Research Council, 2011, tradução nossa). Como o termo medicina personalizada induz à interpretação de que se trata de um tratamento único, indivíduo-específico, o comitê do NRC sugere o uso do termo medicina de precisão. (Negri e Uziel, 2020, p. 9)

Como a medicina de precisão busca a customização de tratamentos de saúde, na tentativa de maximizar a efetividade do cuidado médico e a prevenção de moléstias, considerando a variabilidade genética individual, o meio ambiente e o estilo de vida do paciente, utilizando-se de inteligência artificial, é de rigor o estudo de suas implicações jurídicas, tanto para o médico quanto para o paciente.

Nesse cenário, o presente ensaio visa refletir sobre possíveis problemas jurídicos e soluções para os usos da IA na medicina de precisão.

Nas próximas seções, serão analisados o contexto político-econômico da IA na medicina de precisão, os benefícios e malefícios desse ramo novo médico, a autonomia do médico, a autodeterminação do paciente e os desafios no Brasil. Após, serão feitas as considerações finais a título de conclusão.

1. Contexto político e econômico da medicina de precisão

Para os defensores da medicina de precisão, os algoritmos computacionais permitem formar uma representação virtual do paciente, desenvolvendo “modelos preditivos baseados nas interações conhecidas entre dados moleculares, ambientais e de estilo de vida, que permitirão a tomada de decisões terapêuticas individualizadas” (Iriart, 2019, p. 5). Logo, no lugar do tratamento da doença, o foco se deslocará para a manutenção da saúde do indivíduo por meio de uma medicina preventiva personalizada.

Dessa forma, os impactos na produção, distribuição e gerenciamento de informações em saúde provocados pelas novas tecnologias influenciam até mesmo as concepções de saúde e de doença. O complexo médico-industrial e científico, originado da integração entre a biomedicina e o interesse capitalista, fez surgir a importância da molecularização da biomedicina.

Assim, o “Complexo de Serviços Tecnológicos Biomédicos” é parte “desse processo de transformação tecnocientífico em que uma nova forma de olhar e compreender o corpo em seu nível molecular passa a complementar, senão suplementar, o olhar clínico tradicional”, trazendo “uma nova concepção da vida como um conjunto de mecanismos vitais que podem ser identificados, isolados, manipulados, mobilizados e recombinaados em novas práticas de intervenção em nível molecular.” (Iriart, 2019, p 3-4)

Nesse contexto, a medicina de precisão integra, no capitalismo globalizado, as denominadas “economias da vitalidade”, ou seja, uma visão “de um novo espaço econômico, a bioeconomia, com uma nova forma de capital, o biocapital, em que a manipulação da vida por biocorporações gera valor” (Iriart, 2019, p 4). Por outro lado, há, inclusive, autores que defendem a “economia orientada por dados pessoais”, pois, segundo argumentam, se os pacientes devem ter completo conhecimento e controle sobre o conjunto de seus dados médicos (autodeterminação informativa), torna-se possível gerenciá-los de modo a serem recompensados por produzirem dados úteis à pesquisa ou ao comércio, a permitir também incentivos para o monitoramento da própria saúde (Iriart, 2019).

Além disso, conforme antevisto por alguns, “a tecnocientização tem como características a mercantilização da saúde, transformada em bem de consumo, e a biomedicalização com extensão da jurisdição médica para além da doença, englobando a saúde em si mesma”, desdobrando-se o foco na saúde “na ênfase em práticas de avaliação de riscos e suscetibilidades e monitoramento constante, visando a manter-se saudável”. (Iriart, 2019, p 5)

Em contraposição a tal visão, alguns estudiosos levantam o alerta da criação, nas sociedades de controle (substituidoras das sociedades disciplinares), fundadas na noção de biopoder (conceito desenvolvido por Foucault), de verdadeiras sociedades de hipocondríacos, em que as pessoas se socorrem exponencialmente a medicamentos sem estarem realmente enfermas, sobretudo diante da crise da instituição hospital:

O hospital deu lugar à medicina “sem médico nem doente”. A ascensão da medicina preventiva torna todos “potencialmente” enfermos. O adiamento da doença tem como preço a constante vigilância, a observância radical das prescrições médicas nos horários pré-determinados durante toda a vida. É como se nos tornássemos “inválidos acompanhando a vida das janelas do hospital” (BAUMAN, 1998, p.195) desde que nascemos. O desenvolvimento da biotecnologia e da engenharia genética tem nos mostrado os riscos a que estamos sujeitos por nossas características hereditárias, o que exige um esforço redobrado e constante para minimizá-los, a fim de evitar ou adiar a enfermidade. Todos somos virtuais ou atuais “portadores” de patologias diversas. O surgimento veloz de novas tecnologias impulsiona a medicalização crescente – que inclui desde vitaminas e suplementos alimentares a remédios de uso ininterrupto -, produzindo uma sociedade de hipocondríacos. (Chevitarese e Pedro, 2005, p. 140)

Nesse contexto, embora a medicina de precisão seja voltada ao diagnóstico precoce de doenças ou a diagnósticos mais precisos e tratamentos mais efetivos, também pode ter “efeitos colaterais”, como a utilização desmedida de alguns biomarcadores para doenças, já que “a disseminação de biomarcadores na prática clínica pode potencializar a criação dos chamados ‘pacientes pré-sintomáticos’, quando pessoas saudáveis são medicalizadas por conta da probabilidade de ficarem doentes” (Iriart, 2019, p. 6) ou, ainda, provocar o chamado “efeito Angelina Jolie” (atriz conhecida por ter se submetido à mastectomia dupla profilática, pois é portadora de mutações nos genes BRCA 1 e 2, indicados na avaliação do risco de desenvolvimento do câncer de mama ou de ovário hereditários).

2. A IA na medicina de precisão: benefícios e malefícios

A medicina de precisão trouxe grandes alterações nos cuidados de saúde, havendo vantagens e desvantagens na utilização da inteligência artificial nos processos de diagnose e tratamento.

Entre os benefícios da IA na medicina de precisão, destacam-se tanto a prevenção de moléstias e a diminuição de abordagens terapêuticas desnecessárias, visto que os tratamentos são mais personalizados, quanto o aumento no ganho de escala, já que a atualização dos sistemas tecnológicos pode ser feita em tempo real em todas as máquinas, em nível global.

Schulman e Pereira também mencionam como benefícios da medicina digital:

i) a possibilidade de prever e fazer o controle da doença, predeterminar o seu tratamento; ii) a obtenção de melhores respostas dos tratamentos médicos adotados; iii) a redução de erros de diagnósticos e terapias; iv) a otimização, economia de custos, além de evitar desperdícios; v) o auxílio na realização de inferências em tempo real para alerta de risco à saúde e para a previsão de resultados de saúde; vii) as maiores habilidades de aprendizado e autocorreção para melhorar a precisão dos diagnósticos com base nos resultados; vii) a minimização de falhas na prestação de serviços, tratamentos excessivos, desnecessários; viii) a facilitação da coordenação de dados; x) maior capacidade de atualização e conectividade dos médicos; xi) a possibilidade de intervenções adaptativas personalizadas com tecnologias para atender às necessidades das pessoas com doenças crônicas, com deficiência, e outros grupos etc (Schulman e Pereira, 2020, p. 173).

Apesar desses aspectos positivos, a medicina de precisão não é imune a críticas, havendo também desvantagens como certo comprometimento da interação médico-paciente, tendo em vista a anulação da empatia, dada a neutralidade da máquina. Nesse aspecto, ganha importância a humanização da medicina. Além disso, também há o possível efeito multiplicador de erros da IA (multiplicam-se soluções, mas também erros). Os custos também são mais elevados, havendo seleção de pacientes com base no poder aquisitivo e estão presentes ainda os riscos de segurança inerentes aos sistemas informativos inovadores.

As desvantagens são assim sintetizadas por Schulman e Pereira:

Entre os aspectos negativos do uso da inteligência artificial, pode-se elencar: i) a utilização de dados de forma enviesada, acarretando discriminação, exclusão etc.; ii) a impossibilidade de acesso por determinadas pessoas de menor poder aquisitivo em razão dos custos elevados, fomentando a desigualdade social e a iniquidade na saúde (ou, eventualmente, pode até combater essa desigualdade); iii) a redução do papel do médico, que acaba por se converter

em funcionário de entrada de dados, piorando a exaustão dos profissionais e reduzindo a satisfação do paciente; iv) a falta de segurança, sigilo dos dados pessoais e sensíveis coletados do paciente e o desconhecimento do destino que lhes é dado; v) a inexistência de regulação própria para estabelecer a forma e limites ao uso da inteligência artificial; vi) o surgimento de novos danos e novas responsabilidades; vii) a pouca transparência e a falta de obtenção do consentimento dos pacientes quanto ao uso da inteligência artificial na condução do seu tratamento médico; viii) a quebra da privacidade dos pacientes; ix) a limitação da autonomia dos médicos no processo decisório acerca do tratamento médico empregado; x) os erros dos sistemas que utilizam inteligência artificial podem atingir um número ilimitado de pessoas, acarretar a replicação do erro, com resultados catastróficos, enquanto que o erro de um médico atinge o paciente individualizado; xi) a recusa de tratamentos indicados precocemente em razão de diagnóstico realizado previamente com o uso da inteligência artificial pode gerar a recusa, o cancelamento de plano de saúde, a demissão. (Schulman e Pereira, 2020, p. 173)

No tocante à saúde pública, altos valores das terapias de natureza crônico-degenerativa exercem pressão para que o diagnóstico seja preciso e que se identifiquem previamente os indivíduos que, de fato, responderão ao tratamento.

Destarte, com a medicina de precisão, seria possível utilizar dados genéticos para indicar “previamente a capacidade de resposta do indivíduo e, assim, triar quais grupos de pacientes seriam mais beneficiados por quais tipos de terapias. Isso tornaria o tratamento mais eficaz para o paciente, além de reduzir custos e eventuais desperdícios” (Negri e Uziel, 2020, p. 26).

Entretanto, nem sempre a medicina de precisão (MP) é tão efetiva quanto se propaga, consoante advertido por Iriart:

Outro ponto bastante questionável é a suposição de que a MP contribuirá para a adoção de medidas preventivas por parte das pessoas com base no conhecimento de suas suscetibilidades genéticas. Há vários estudos problematizando essa afirmação e mostrando que a informação genética com orientação personalizada não necessariamente leva à modificação de comportamentos por parte das pessoas em risco. O baixo impacto das ações voltadas para indivíduos em alto risco é um ponto frequentemente negligenciado pelos defensores da MP. (Iriart, 2019, p. 8)

Portanto, a medicina de precisão necessita do auxílio de outras especialidades da saúde, como a psicologia, nutrição e educação física, porquanto nem sempre o diagnóstico precoce e preventivo será efetivo na mudança de comportamento do paciente, o que poderá redundar no aparecimento ou agravamento da doença.

3. Medicina de precisão e autonomia do médico

A medicina de precisão (MP) pode ser dividida em duas fases: MP 1.0 e MP 2.0.

A MP 1.0 é aquela voltada ao diagnóstico mais preciso, utilizando informações de testes genéticos e outros dados pessoais extraídos de novas tecnologias, como biossensores e *wearables*, desenvolvidos para monitorar sinais vitais e hábitos de vida dos pacientes, em tempo real ou não (Negri e Uziel, 2020). Desta feita,

[...] as informações geradas pelos dois primeiros grupos de tecnologias – testes genéticos e monitoramento – podem ser, então, tratadas por ferramentas de *big data* e analisadas por algoritmos ou ferramentas de inteligência artificial capazes de processar a informação e auxiliar no diagnóstico precoce e na melhor escolha de tratamento para os pacientes. (Negri e Uziel, 2020, p. 12)

Quanto aos testes genéticos em geral, há no mercado três tipos: i) testes genéticos em humanos, que analisam variações na sequência, estrutura ou expressão do DNA e do RNA, a fim de diagnosticar doenças ou condições de saúde; ii) testes de diagnóstico complementar (*companion diagnostic devices*), destinados a analisar a eficiência e a segurança de uma droga ou produto biológico correspondente; e iii) testes genéticos diretos ao consumidor (ou recreativos), que incluem aplicações forenses, de ancestralidade, *fitness* e nutrição, entre outros (Negri e Uziel, 2020).

Por sua vez, a medicina de precisão 2.0 (MP 2.0 ou disruptiva), está relacionada à aplicação, como tratamento no paciente, de técnicas genéticas, a exemplo de terapias celulares e gênicas baseadas em “informações ômicas”, não se limitando ao simples diagnóstico. Assim, são técnicas de edição gênica, terapias de células-tronco e gênicas, entre outras (Negri e Uziel, 2020).

A empresa IBM é uma grande desenvolvedora de soluções tecnológicas na área da saúde, tendo desenvolvido, no âmbito da medicina de precisão, o Watson for Oncology. É um *software* inteligente que avalia as informações do

prontuário do paciente e as compara com as evidências médicas constantes de artigos científicos e estudos clínicos, exibindo provável diagnóstico com possíveis opções de tratamento para portadores de câncer, classificadas por nível de confiança. É uma ferramenta de auxílio ao médico, a quem caberá analisar as conclusões trazidas pela inteligência artificial e cotejá-las com outras para decidir pelo melhor tratamento a ser dispensado ao paciente em particular. O Watson apresenta 90% de acerto dos diagnósticos promovidos, segundo estudos (Nogaroli e Silva, 2020).

Ressalta-se que, em se tratando de inteligência artificial, que trabalha com probabilidades e *input* de dados (insumos dos algoritmos) não se pode garantir a certeza das conclusões geradas, ou seja, dos diagnósticos traçados, conquanto muitas vezes o *software* seja mais rápido, preciso e acerte mais que os diagnósticos feitos por humanos:

No Instituto de Tecnologia de Massachusetts (MIT) e no Massachusetts General Hospital, pesquisadores desenvolveram um modelo de inteligência artificial que possibilitou antecipar o diagnóstico do câncer de mama em até 05 (cinco) anos antes dele se manifestar. O modelo conseguiu identificar padrões sutis que não podiam ser constatados por seres humanos nos tecidos mamários, antevendo as chances do desenvolvimento do câncer. As técnicas tradicionais anteriores conseguiam diagnosticar somente 18% desses casos. Todavia, com a ajuda do modelo a possibilidade de diagnosticar subiu para 31%, o que é um avanço considerável no tratamento da doença.

[...]

Na China, o centro de pesquisa de inteligência artificial do Beijing Tiantan Hospital desenvolveu um sistema para realizar diagnósticos com maior precisão. Denominado como BioMind, o sistema obteve o êxito em 87% contra 66% nos diagnósticos realizados por profissionais humanos. Outra vantagem apresentada pelo sistema BioMind foi o tempo para realizar o diagnóstico. Enquanto os seres humanos demoraram 30 minutos para realizar 225 diagnósticos, o sistema de IA demorou apenas 15 minutos, ou seja, metade do tempo. É importante ressaltar que todos esses dados foram obtidos em uma competição que teve como objetivo fazer com que os médicos chineses entendessem o poder da inteligência artificial, em especial, com relação aqueles que são céticos ao avanço das tecnologias. (Damilano e Toniazzo, 2021, p. 3-4)

Ademais, há sempre problemas de vieses (*bias*) nos *inputs* e de falta de transparência sobre a maneira como a inteligência artificial processa as informações, problema enfrentado até pelos desenvolvedores, que não entendem adequadamente como os algoritmos funcionam, visto que o aprendizado de máquinas comumente apresenta o efeito *black box* (problema da caixa preta), em que a IA se autoajusta.

Cumprir mencionar o exemplo do Deep Patient, *software* inteligente desenvolvido em 2015 pelo Mount Sinai Hospital de Nova Iorque, preditivo de futuras doenças de pacientes a partir de uma base de conhecimento composta por cerca de 700 mil prontuários eletrônicos. Em estudos iniciais, constatou-se que a IA pode antecipar o aparecimento de diferentes doenças “como esquizofrenia, diabetes e alguns tipos de câncer. Contudo, o processo de aprendizado de máquina para chegar a um determinado diagnóstico é ainda uma verdadeira incógnita para os cientistas. Não se tem conhecimento de como a IA chega aos seus resultados.” (Neto e Nogaroli, 2020, p. 149)

Nesse cenário, a autonomia do médico em realizar diagnósticos a partir da inteligência artificial ganha especial relevância, ainda mais considerando potenciais erros de diagnóstico e sua responsabilização:

A dificuldade na identificação do percurso por meio do qual os algoritmos chegam a um resultado pode ser extremamente problemática, sobretudo, no setor da saúde, no qual são recorrentes os contextos de vida ou morte em que os pacientes podem se encontrar. O cenário é ainda mais delicado quando a inteligência artificial é utilizada não apenas para categorizar os pacientes em emergência, mas também para criar diagnósticos tangíveis. Nos casos em que um médico chega a uma conclusão que se desvia do diagnóstico automatizado, o profissional se encontrará na desafiadora tarefa de avaliar: “devo confiar no meu diagnóstico ou naquele resultado diferentemente obtido pela inteligência artificial?”. O equacionamento dessa e de outras indagações se relaciona diretamente com a definição do critério de imputação do dever de indenizar, uma vez que a delimitação do regime de responsabilidade civil incidente tornará mais ou menos necessária a valoração do comportamento concretamente adotado pelo agente. (Nogaroli e Silva, 2020, p. 77).

É por isso que, quanto à culpa médica por erro de diagnóstico, o equívoco resultante do uso da inteligência artificial poderá ser escusável se a falha na conduta do profissional não for grave, havendo, todavia, responsabilidade nos casos de erro grosseiro, negligência e imperícia, até porque o médico deve

esgotar todos os meios disponíveis para emitir o seu diagnóstico. Noutros termos, o médico não é refém da inteligência artificial, mas deverá ser cauteloso ao rejeitar a conclusão terapêutica da máquina, justificando concretamente sua escolha ao paciente. Afinal, tanto a inteligência humana quanto a inteligência artificial não são infalíveis. O médico é livre para escolher seus meios de diagnóstico e terapia, mas também é responsável por sua decisão.

Nesse sentido, “a falta de diligência do médico ao descartar irrefletidamente o resultado obtido pela inteligência artificial poderá constituir um critério para a sua responsabilização” (Nogaroli e Silva, 2020, p. 85), devendo ser reforçado que os aparelhos de diagnóstico “devem servir como apoio à tomada de decisão do médico, sem o condão de substituí-lo, de modo que a decisão final segue sob o controle (e sob a responsabilidade) do profissional da saúde. A tecnologia não retira, enfim, o caráter soberano da decisão do médico” (Nogaroli e Silva, 2020, p. 87-88).

4. Medicina de precisão e autodeterminação do paciente

Na medicina, por muito tempo, vigorou a visão paternalista da relação médico-paciente, em que o enfermo deveria ser tutelado pelo profissional da saúde, ocupando uma posição de objeto da atuação médica (Neto e Nogaroli, 2020).

Aos poucos, tal concepção foi-se modificando. Se, até o início do século XX, a permissão dada ao médico pelo paciente significava apenas o prosseguimento para a intervenção recomendada, a partir de meados do século passado passou-se a definir que o paciente deveria ser alertado de quaisquer riscos para que tomasse uma decisão inteligente sobre o seu tratamento. Desse modo, começou-se a privilegiar a autodeterminação do paciente por meio do consentimento informado (Neto e Nogaroli, 2020).

Logo, do princípio da beneficência, “o qual determina que o dever de o médico informar o paciente sobre os riscos inerentes ao procedimento é condicionado à obrigação primordial do profissional de levar em consideração os melhores interesses do doente” (Neto e Nogaroli, 2020, p. 145-146), o médico passou a ostentar também um papel consultivo, envolvendo um processo dialógico, para que o paciente pudesse compreender a sua condição clínica e os benefícios e riscos de tratamentos, de modo a tomar uma decisão bem informada, livre e esclarecida: “Desse modo, o dever do médico não é preenchido bombardeando-se o paciente com informações técnicas que ele não pode razoavelmente compreender, menos ainda exigindo sua assinatura em um termo padronizado e genérico de consentimento (Neto e Nogaroli, 2020, p. 146).

Macena (2020, p. 42) assinala que “o dever de informar é imperativo como requisito prévio para o consentimento, consagrando o princípio da autonomia, pelo qual o paciente tem o direito de ser autor do seu próprio destino e de optar pelo rumo que quer dar à sua vida”.

O efetivo cumprimento do dever de informação médica somente se dá quando os esclarecimentos se relacionarem especificamente ao caso concreto do paciente, sendo insuficiente informações genéricas. “Da mesma forma, para validar a informação prestada, não pode o consentimento do paciente ser genérico (*blanket consent*), necessitando ser claramente individualizado” (STJ, REsp nº 1.540.580/DF, Rel. para acórdão Ministro Luis Felipe Salomão, Quarta Turma, DJe 4/9/2018).

Nesse cenário, o consentimento do paciente e o direito de ser bem-informado, bem como o dever de informar do médico, estão previstos nos arts. 13, 22, 24, 31 e 34 do anexo da Res.-CFM nº 2.217/2018 (Código de Ética Médica) e em diplomas internacionais: arts. 5º e 6º da Declaração Universal sobre Bioética e Direitos Humanos de 2005 da UNESCO e na Declaração de Lisboa de 1991, emendada pela 47ª Assembleia Geral da Associação Médica Mundial de 1995, ocorrida em Bali (Indonésia).

Aliás, a Res.-CFM nº 2.232/2019 estabeleceu normas éticas para a recusa terapêutica por pacientes e objeção de consciência na relação médico-paciente, concretizando o princípio da bioética da autonomia do paciente².

Conforme Marione (2020),

O termo de consentimento livre e esclarecido ou o termo de consentimento informado são fundamentais para o pleno exercício da autonomia [do paciente], bem como para resguardo e proteção do médico. Acentua-se que o consentimento pode ser revogado a qualquer tempo da relação entre médico/paciente.

É necessário que o paciente seja esclarecido de todas as opções terapêuticas para que consinta de forma livre e espontânea com o tratamento oferecido pelo profissional da saúde de maneira consciente (para cada etapa do tratamento), caso o paciente esteja impedido de receber informações sobre seu tratamento as mesmas poderão ser repassada ao seu responsável legal.

Ressalta-se que o médico que deixar de prestar esclarecimentos de forma clara e precisa poderá responder judicialmente pela ausência de informação (Marione, 2020, p. 58).

2. A bioética se baseia em quatro princípios: beneficência, não maleficência, autonomia do paciente e justiça.

Nesse contexto, o paciente deve ser bem esclarecido acerca do uso da inteligência artificial em seu diagnóstico, bem como sobre o resultado, riscos e propostas terapêuticas, sendo essencial também o seu consentimento destacado se houver o compartilhamento de seus dados pessoais com o banco de dados do *software*.

De fato, tratando-se de dados sensíveis, é de fundamental importância a garantia do sigilo informacional e a privacidade do usuário (governança de dados), ainda que o tratamento de dados seja possível por bases legais diversas da do consentimento (art. 11 da Lei Geral de Proteção de Dados – LGPD), como a tutela da saúde. Consoante Neto e Nogaroli,

[...] tendo em vista a possibilidade da IA causar danos imprevisíveis, devido ao aperfeiçoamento pelo aprendizado de máquina, além da questão do tratamento de dados sensíveis e possibilidade de se ser incorreto, ou dos dados serem invadidos por terceiros, é de suma importância a investigação dos princípios éticos que devem ser seguidos pelos seus desenvolvedores e usuários (prestadores de serviços médicos apoiados em IA, por exemplo), especialmente no que diz respeito ao consentimento da pessoa submetida a cuidados da saúde apoiados nessa tecnologia (Neto e Nogaroli, 2020, p. 151).

Assim, deve ser sempre uma opção do paciente recusar-se a ser tratado por um robô ou ter seu caso examinado apenas por IA, mesmo nas hipóteses de diagnósticos preditivos. A autonomia e a autodeterminação do paciente devem ser observadas também na análise diagnóstica, devendo o profissional “fornecer ao paciente uma informação leal, completa e acessível, sobre todos os benefícios e riscos na utilização da inteligência artificial” (Neto e Nogaroli, 2020, p. 157). Em outras palavras, devem ser informados e explicados os riscos do *software* inteligente no apoio à tomada de decisão do médico, incluindo-se o grau de imprecisão da IA e falta de transparência na forma de processamento dos dados pelo algoritmo.

5. Medicina de precisão e IA: desafios no Brasil

Algumas das tecnologias abrangidas pelo conceito da medicina de precisão apresentam grande potencial de incorporação a políticas públicas, visto que possuem custos menores e alto potencial de impacto, podendo ser utilizadas em diversas situações. De fato, não só os testes genéticos passaram a ter preços mais reduzidos, mas a crescente utilização de *big data*, IA e dispositi-

vos de monitoramento da saúde das pessoas também permitem diagnósticos mais precisos, sobretudo quanto a doenças crônicas (como câncer, diabetes, doenças cardíacas, neurodegenerativas, autoimunes, entre outras). “Essas tecnologias têm sido vistas, também, como uma maneira efetiva de prevenção de ocorrências agudas e, portanto, como um mecanismo para reduzir os custos da atenção à saúde e do desenvolvimento de novas drogas.” (Negri e Uziel, 2020, p. 30-31)

No entanto, para melhor aproveitamento de todos os potenciais benéficos da medicina de precisão pela sociedade, é preciso a superação de grandes desafios, conforme orientação do próprio Fórum Econômico Mundial:

Segundo o Fórum Econômico Mundial, sua implementação [da medicina de precisão] no atendimento de saúde ainda apresenta grandes desafios, tais como: i) produção de evidências suficientes sobre a sua eficácia; ii) enfrentar a questão do compartilhamento de dados e da infraestrutura necessária; iii) repensar o sistema regulatório; iv) utilizar as informações genômicas provenientes da pesquisa na atenção à saúde; e v) criar modelos adequados de pagamento e compartilhamento de riscos.

Esses desafios são complexos e, para lidar com eles, formuladores de políticas deveriam atuar em proximidade com os *stakeholders* e com a sociedade em geral, a fim de garantir que os benefícios da medicina de precisão sejam mais amplamente utilizados pela sociedade. (Negri e Uziel, 2020, p. 33)

Ademais, como a medicina de precisão baseia-se em grandes bancos de dados, alimentados continuamente, torna-se necessário o desenvolvimento da interoperabilidade entre os diversos sistemas de saúde para haver o devido compartilhamento completo de informações, observadas as diretrizes da LGPD e do sigilo do paciente. A interoperabilidade é essencial para o aprimoramento dos diagnósticos inteligentes, que poderão ser mais precisos e preditivos (Negri e Uziel, 2020).

Vale ressaltar que os diagnósticos preditivos e continuados não podem ser utilizados em desfavor do paciente, sendo desaconselhado promover-se o compartilhamento desses dados a terceiros, ainda mais empregadores ou empresas de natureza comercial, como planos de saúde e seguradoras. Isso porque o diagnóstico precoce de possíveis males futuros e o acompanhamento da conduta cotidiana do indivíduo poderão ser usados por tais segmentos para perseguir empregados ou promover indevidas seleções de risco e aumentos do prêmio, prejudicando o real proprietário dos dados sensíveis. Por

outro lado, aqueles menos propensos a desenvolver doenças poderiam optar por não contratar planos de saúde, aumentando a seleção adversa no setor (Negri e Uziel, 2020).

Consoante Sarlet e Molinaro, todos possuem escolhas ao conduzir a vida, sendo apenas uma opção se portar de forma preventiva, de forma que não podem ser obrigados por empregadores ou operadoras de plano de saúde a seguirem hábitos saudáveis, até porque a saúde humana é complexa:

[...] a liberdade de moldar a vida e o autodesenvolvimento tem precedência sobre uma obrigação estrita e permanente de evitar todos os riscos para a saúde. Embora isto não se aplique indefinidamente, a coleta orientada e contínua de dados sobre os estilos de vida individuais e a utilização de grandes perfis de risco alimentados por dados que abrangem todas as áreas da vida dificilmente poderiam ser consideradas uma expectativa razoável de responsabilidade pela própria saúde.

Se/e como às instituições de seguro de saúde estatutárias é permitido levar em consideração a responsabilidade da saúde e influenciar o comportamento de saúde de seus segurados é discutível. Os sistemas de incentivo baseados em dados podem ter uma eficácia muito intensiva e de monitorização invasiva. No entanto, a divulgação diferenciada de fatores de risco por meio de análises de *big data* que, integrando dados de todas as áreas da vida, também pode mostrar no futuro que a maioria da população tem perfis de risco mistos que protegem e incluem fatores favoráveis, bem como fatores físicos, mentais, comportamentais e outros tipos negativos. (Sarlet e Molinaro, 2019, p. 191-192)

Contudo, a medicina de precisão ao categorizar o paciente em subpopulações pode acrescentar positivamente ao agregá-lo a pessoas que também sofrem de problemas semelhantes, podendo uns servirem de apoio aos outros. “Em várias áreas da medicina, o uso de tecnologias de *big data* já levou ao desenvolvimento de novas práticas de apoio pró-social, como a formação de grupos menores de pacientes” (Sarlet e Molinaro, 2019, p. 192), a exemplo de grupos de doenças raras, em que experiências são compartilhadas.

Outrossim, a medicina de precisão, a nível macro, também pode auxiliar políticas públicas de natureza preventiva, já que dados de sequenciamento genético de populações podem indicar se os indivíduos de uma nação possuem maiores riscos de desenvolver determinada doença, podendo, assim, ser estimulados a fazer tratamentos precoces, aumentando, como externalidade positiva, a eficiência dos serviços de saúde. Diversos países possuem progra-

mas de sequenciamento genético de suas populações, cabendo mencionar: a Holanda, que criou o programa *Genome of the Netherlands* como um polo da iniciativa europeia *Biobanking and Biomolecular Research Infrastructure*; o Reino Unido (*Genomics England* e *UK Biobank*); os Estados Unidos (*Precision Medicine Initiative* – PMI); a Alemanha, entre outros:

Há outras iniciativas buscando aplicações da genômica na saúde, de uma forma geral, em diversos países da Europa, como: i) *Belgian Medical Genomics Initiative*; ii) *Estonian Program for Personal Medicine*; iii) *Genomic Medicine 2025*, na França; iv) *Bench to Bedside Project*, em Israel; e v) *Implementation of Genomic Medicine Project*, no Japão. Há ainda programas mirando doenças específicas, como o de doença de Parkinson em Luxemburgo (*Centre for System Biomarkers*), para distrofia de córnea e câncer gastrointestinal em Singapura (Polaris) e estudos farmacogenômicos para drogas específicas na Tailândia (*Pharmacogenomics and Personalized Medicine*). Acredita-se que o sequenciamento clínico esteja crescendo nos países asiáticos, como China e Índia, mas que esses dados sejam menos explorados em publicações (Negri e Uziel, 2020, p. 40-41)

O Brasil possui forte incidência de doenças crônico-degenerativas, que são o principal foco da medicina de precisão. Assim, “a possibilidade, aberta pela medicina de precisão, de mapear subgrupos populacionais mais suscetíveis a essa doença pode contribuir com ações preventivas capazes de reduzir os custos dos tratamentos oncológicos no sistema de saúde brasileiro.” (Negri e Uziel, 2020, p. 42)

A ciência brasileira possui algumas iniciativas relevantes, sendo relevante mencionar a criação da *Brazilian Initiative on Precision Medicine* (BIP-Med), apoiada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), que objetiva desenvolver uma plataforma para armazenar e compartilhar dados genéticos provenientes de cinco centros de pesquisa consorciados. Há ainda, na Universidade de São Paulo (USP), a iniciativa DNA do Brasil, que visa mapear o genoma de 15 mil brasileiros entre 35 e 74 anos de idade, incluindo o Brasil nos estudos genômicos mundiais de identificação de variações genéticas relacionadas às características de saúde populacional. Nesse projeto o Ministério da Saúde contribuirá com o projeto Estudo Longitudinal de Saúde do Adulto (ELSA) Brasil (Negri e Uziel, 2020).

Outrossim, cumpre citar o Censo Nacional de Isolados (CENISO), que busca identificar aglomerados populacionais acometidos por doenças genéticas

e por anomalias congênitas decorrentes de fatores genéticos ou de fatores ambientais, realizado periodicamente pelo Instituto Nacional de Genética Médica Populacional (Inagemp), o qual busca orientar essas populações sobre políticas de saúde, aconselhamento genético e tratamentos médicos (Negri e Uziel, 2020).

Há também, em tramitação na Câmara dos Deputados, projeto de lei (PL nº 4010/2021) que “determina a implantação de rastreamento e teste genético a todos (as) cidadãos (as) com idade superior a 35 anos, conforme o disposto na Portaria nº 874, de 16 de maio de 2013 do Ministério da Saúde”, tendo sido mencionado um exame da medicina de precisão que se utiliza da tecnologia Exoma, segundo consta na justificativa do PL:

A forma de descobrir o câncer precocemente é o rastreamento. [...] Quando transpomos essa situação para o câncer, o rastreamento para descobrir precocemente a doença pode aumentar radicalmente as chances de cura. [...]

“O rastreamento é um recurso utilizado para detecção precoce de diferentes tipos de doenças, incluindo o câncer. Trata-se da realização de exames ou testes diagnósticos em pessoas que não apresentam sinais ou sintomas clínicos da doença, no intuito de se realizar o diagnóstico precoce do câncer ou de lesões sugestivas de câncer e reduzir a incidência e mortalidade da doença”, explica a biomédica Angela Maria Moed Lopes, Dra. em Ciências da Saúde, professora do curso de mestrado em Healthcare Management da MUST University (Flórida, EUA) e ex-consultora de projeto do Programa Nacional de Apoio à Atenção Oncológica do Ministério da Saúde.

[...]

No exame de rastreamento genético, o DNA é extraído pela saliva, podendo ser efetuada pelo próprio usuário em sua residência, devendo assim enviar a amostra para análise em laboratório. O DNA é analisado através da tecnologia Exoma, que faz um sequenciamento completo dos genes. Por meio de inteligência artificial e bioinformática, as informações são comparadas com bancos de dados genéticos, com o objetivo de verificar e definir quais são as variantes genéticas que podem causar esta doença.

Foram apensados ao PL nº 4010/2021 dois outros PLs correlacionados: o PL nº 4272/2021, o qual altera a Lei nº 14.238, de 19 de novembro de 2021, que institui o Estatuto da Pessoa com Câncer, para criar o sistema nacional de acompanhamento da pessoa com suspeita ou diagnóstico de câncer, com o objetivo de realizar a navegação desses pacientes no Sistema Único de Saú-

de, e o PL nº 191/2022, o qual altera a Lei nº 8.080, de 19 de setembro de 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, para assegurar atendimento voltado ao rastreamento de doenças crônicas não transmissíveis no âmbito do Sistema Único de Saúde (SUS).

Quanto às terapias gênicas, existem diversos estudos de universidades brasileiras em andamento, a exemplo da pesquisa desenvolvida pelo Centro de Terapia Celular (CTC) da USP, em Ribeirão Preto (Negri e Uziel, 2020).

Considerações finais

A produção em massa de dados pessoais ligados à saúde (*big data*) e o desenvolvimento da inteligência artificial possibilitaram o surgimento da medicina de precisão. Assim, por meio de cálculos de probabilidade realizados por máquinas dotadas de aprendizado (*machine learning* ou *deep learning*), os diagnósticos puderam ser feitos não só com maior rapidez ou exatidão, mas também de forma preditiva.

Se, por um lado, os tratamentos médicos podem ser mais específicos e direcionados à terapêutica do paciente, tornando ultrapassados determinados protocolos genéricos (diagnóstico preciso); por outro lado, pessoas saudáveis podem ser induzidas, pela indústria farmacêutica, a iniciar tratamentos precoces e contínuos desnecessários (diagnóstico apenas preditivo).

De fato, em diversos casos, o surgimento de uma doença somente surgirá quando presentes um conjunto complexo de fatores, sendo recomendável tão só a mudança de comportamento para hábitos mais saudáveis.

De qualquer maneira, a inteligência artificial deve constituir uma ferramenta de auxílio ao médico, que não deixa de perder seu poder e autonomia sobre o diagnóstico final do paciente. Em contrapartida, este deve ser cientificado do uso das máquinas inteligentes para poder tomar decisões conscientes sobre o seu tratamento, o que será obtido por processos dialógicos, humanizadores e empáticos. A autodeterminação do paciente não pode ser negligenciada.

Igualmente, o tratamento dos dados pessoais sensíveis na medicina de precisão deve ser conforme a LGPD, observando-se, entre outras disposições, as bases legais, o sigilo do paciente, a possível anonimização para compartilhamento consentido para pesquisas e bancos de dados e a segurança cibernética.

Para que haja o aperfeiçoamento dos estudos da medicina de precisão, a interoperabilidade dos sistemas de saúde é uma medida a ser pensada por órgãos reguladores.

Além disso, a medicina de precisão também é promissora para políticas públicas, pois possibilita estudos sobre grupos populacionais e desenvolvimento de moléstias, sobretudo as de natureza crônico-degenerativa, podendo ser desenvolvidas ações preventivas para estratos específicos, em prol da eficácia, eficiência e efetividade dos serviços de saúde e de sobrevivência dos indivíduos.

Por fim, o alto custo de diversos procedimentos da medicina de precisão pode ser um fator de barreira, limitando o acesso àqueles que não possam custeá-la, sendo premente investimentos públicos na área, seja fomentando o desenvolvimento de tecnologia própria seja fortalecendo a indústria e os órgãos de pesquisa nacionais, o que irá contribuir para o acesso mais igualitário dos serviços de saúde no Brasil.

Referências

ANDRADE, Fabio Siebeneichler de; FACCIIO, Lucas Girardello. Notas sobre a Responsabilidade Civil do Médico pela Utilização da Inteligência Artificial. *Revista Magister de Direito Civil e Processual Civil*, n. 91, p. 96-114, jul./ago. 2019.

ATTADEMO, Carolinne Vargas; CARNEIRO, Harthuro Yacintho Alves; ANDRADE, Hederson Pinheiro de; ANDRADE, Hélio Pinheiro de; MANCIA, Joel Rolim. Impacto do big data na implementação de políticas públicas voltadas à saúde. *Vita et Sanitas*, v. 15, n. 2, p. 41-52, jul. 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). *Inteligência artificial e direito: ética, regulação e responsabilidade*. São Paulo: Revista dos Tribunais, 2019, p. 207-228.

CHEVITARESE, Leandro; PEDRO, Rosa Maria L. R. Da Sociedade Disciplinar à Sociedade de Controle: a questão da liberdade por uma alegoria de Franz Kafka em O Processo, e de Phillip Dick, em Minority Report. *Estudos de Sociologia*. Revista do Programa de Pós-graduação em Sociologia da UFPE, Recife, v. 8, n. 1 e 2. p. 129-162, 2005.

DAMILANO, Cláudio Teixeira; TONIAZZO, Daniela Wendt. Responsabilidade Civil e o Uso da Inteligência Artificial na Área da Saúde. *Rede Interamericana de Direitos Fundamentais e Democracia: RED-IDD*, Anais da VIII Jornada de Direitos Fundamentais 2021, GT 3 – Sala Virtual 03-Direitos Fundamentais e Novas Tecnologias, p. 1-20.

GARCIA, Marcos Leite; MACIEL, Nicole Felisberto. Inteligência artificial no acesso a saúde: Reflexões sobre a utilização da telemedicina em tempos de pandemia. *Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI*, Itajaí, v. 15, n. 2, p. 623-643, 2º quadrimestre de 2020.

IRIART, Jorge Alberto Bernstein. Medicina de precisão/medicina personalizada: análise crítica dos movimentos de transformação da biomedicina no início do século XXI. *Cad. Saúde Pública*, v. 35, n. 3, p. 1-14, 2019.

MACENA, Eveline. Dever informacional na medicina e na odontologia. *In: ALMEIDA, Alessandra Varrone de (org.). Coletânea de Direito Médico* [recurso eletrônico]. São Paulo: Mizuno, 2020, p. 42-45.

MARIONE, Jussele Pires Romanin. Autonomia do paciente. *In: ALMEIDA, Alessandra Varrone de (org.). Coletânea de Direito Médico* [recurso eletrônico]. São Paulo: Mizuno, 2020, p. 56-60.

NEGRI, Fernanda de; UZIEL, Daniela. *O que é medicina de precisão e como ela pode impactar o setor de saúde?* Texto para discussão 2557, Rio de Janeiro: IPEA, 2020, 59 p.

NETO, Miguel Kfourri; NOGAROLI, Rafaella. O consentimento do paciente no admirável mundo novo de robôs de assistência à saúde e algoritmos de inteligência artificial para diagnóstico médico. *In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). O Direito Civil na era da inteligência artificial*. 1ª. ed., São Paulo: Thomson Reuters Brasil, 2020, p. 139-164.

NOGAROLI, Rafaella; SILVA, Rodrigo da Guia. Inteligência Artificial na Análise Diagnóstica: Benefícios, Riscos e Responsabilidade do Médico. *In: NETO, Miguel Kfourri; NOGAROLI, Rafaella (coord.). Debates contemporâneos em direito médico e da saúde*. São Paulo: Thomson Reuters Brasil, 2020, p. 70-91.

RIBEIRO, Antonio Luiz; OLIVEIRA, Gláucia Maria Moraes de. Rumo a uma Cardiologia Centrada no Paciente e Guiada por Dados. *Arq. Bras. Cardiol.*; v. 112, n. 4, p. 371-373, 2019.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Direitos Fundamentais & Justiça*, Belo Horizonte, v. 13, n. 41, p. 183-212, jul./dez. 2019.

SCHIRRU, Luca. A Inteligência Artificial e o Big Data no Setor da Saúde: Os Sistemas Especialistas e o Direito. *PIDCC*, Aracaju, ano V, v. 10, n. 3, p. 81-99, out. 2016.

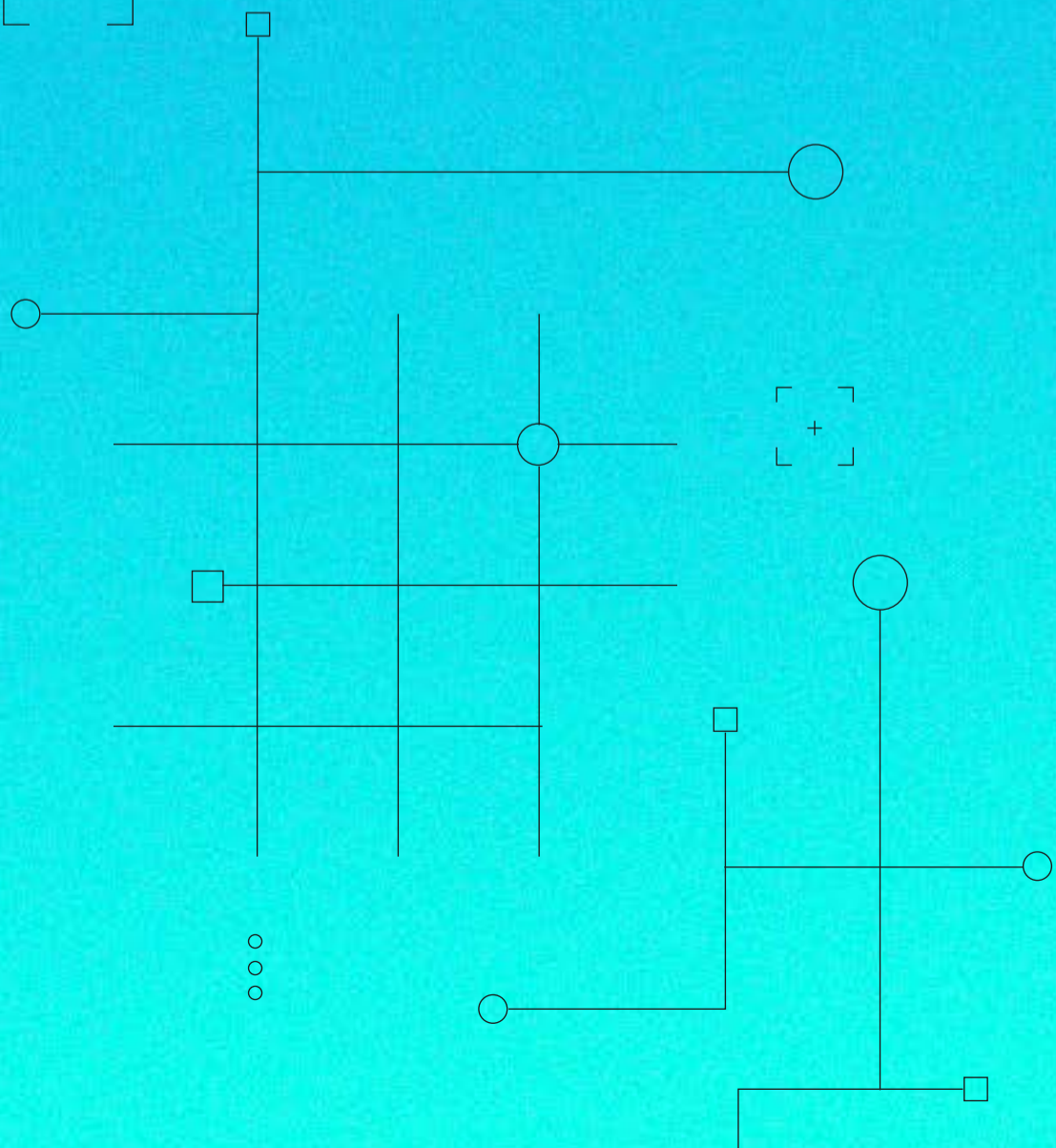
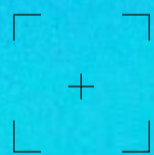
SCHULMAN, Gabriel; PEREIRA, Paula Moura Francesconi de Lemos. Futuro da saúde e saúde do futuro: impactos e limites reais da inteligência artificial. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). *O Direito Civil na era da inteligência artificial*. 1ª. ed., São Paulo: Thomson Reuters Brasil, 2020, p. 165-182.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

3

A questão da titularidade dos direitos autorais de música produzida por Inteligência Artificial no ordenamento jurídico europeu

RAFAEL LUCAS BORBA



Sumário: Introdução. 1. Regulamentação na União Europeia. 2. As obras geradas por Inteligência Artificial são protegidas pela atual legislação de direitos autorais da União Europeia? 3. As obras geradas por Inteligência Artificial devem ser protegidas? E se sim, quem deveria ser o titular dos direitos? Considerações finais. Referências.

Introdução

Nas últimas décadas, a inovação tecnológica experimentou um crescimento sem precedentes e até nos faz pensar sobre os limites (se houver) da tecnologia e seus usos potenciais. A inovação tecnológica disruptiva está progredindo exponencialmente, enquanto os sistemas legais e as instituições reguladoras não conseguem acompanhar todas essas mudanças, criando o chamado “problema de ritmo” (Downes, 2009, p. 55-58). Mais cedo ou mais tarde, legisladores de todo o mundo e organizações internacionais terão que começar a fazer mudanças para adaptar o atual quadro jurídico ao aspecto dinâmico do setor de tecnologia.

Uma das tecnologias mais proeminentes e em constante crescimento é, sem dúvida, a Inteligência Artificial (IA), com previsão de se tornar uma indústria de mais de US\$ 70 bilhões em pouquíssimo tempo (Yanisky-Ravid *et al.*, 2017, p. 665-666). O desenvolvimento de novas ferramentas de aprendizagem algorítmica, associadas ao acesso a uma vasta rede de dados computacionais, têm levado à criação de sistemas de autoaprendizagem complexos, os chamados aprendizados de máquina (Sartor *et al.*, 2018, p. 2), que impulsionam a criação de IA capaz de produzir performances criativas e inovadoras, independentemente de contribuição humana substancial no processo criativo. Assim, não mais ficção ou uma mera ferramenta para a criação humana, agora a IA está sendo usada para gerar uma ampla variedade de obras, tais como obras artísticas, literárias, musicais, dentre outras. Neste contexto, ganha especial destaque o campo da música, que se antecipa aos demais ramos artísticos e

1. Advogado; Bacharel em Direito pela Universidade Federal do Espírito Santo (2012); Pós-graduação em Direito Individual e Processual do Trabalho pela Faculdade de Direito de Vitória (2017); Pós-graduação em Direitos Fundamentais pelo Instituto Brasileiro de Ciências Criminais e Instituto *Ius Gentium Conimbrigae*, Faculdade de Direito da Universidade de Coimbra (2017); Mestrado em Direito Empresarial e Tecnologia (Law & Tech) pela NOVA School of Law, Universidade NOVA de Lisboa (2022); Mobilidade acadêmica para pesquisa na Faculdade de Direito da Ludwig-Maximilians-Universität München (2021); Pós-graduação em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio e Faculdade de Direito da Universidade do Estado do Rio de Janeiro (2022); MBA em Digital Business pela Universidade de São Paulo/Escola Superior de Agricultura Luiz de Queiroz (2022).

abraça essas novas tecnologias, abrindo novas possibilidades para a criação musical. No entanto, o desenvolvimento de tais ferramentas algorítmicas, associado ao desaparecimento da contribuição humana no processo criativo, representam um desafio para a estrutura da Propriedade Intelectual. Devido ao “problema do ritmo”, recentemente muitas questões legais têm surgido com o uso da IA para fins imprevistos e inovadores.

Neste breve artigo, abordaremos a questão da Propriedade Intelectual (PI), ou seja, a possibilidade (ou não) de proteção de direitos autorais de músicas geradas por IA. Certamente, as respostas às dúvidas existentes passam pela análise dos diferentes sistemas de proteção dos direitos autorais existentes hoje, e encontram pontos comuns e dissonantes entre os diversos estudiosos do tema, como será demonstrado a seguir.

Deu-se preferência, no presente trabalho, à análise da temática sob a luz do ordenamento jurídico da União Europeia (UE), uma vez que lá as discussões encontram-se mais aprofundadas e avançadas, com ricas fontes doutrinárias e jurisprudenciais. Sendo assim, este artigo buscou, no seu primeiro tópico, apresentar quais são as principais normas que regulam os direitos autorais na UE, e quais requisitos devem ser cumpridos a fim de que uma obra possa ser protegida por tais normas. Deu-se especial destaque às discussões em torno da originalidade, e às orientações contidas em importantes Diretivas e decisões do Tribunal de Justiça da União Europeia (TJUE). Por sua vez, o segundo tópico deste artigo buscou discutir se as obras geradas por IA seriam ou não protegidas pela atual legislação de direitos autorais da UE. Neste sentido, apesar de terem sido discutidas diferentes questões, mostrou-se crucial analisar o nível de contribuição humana no processo de criação de uma obra em conjunto com uma IA, a fim de se determinar se tal obra é passível ou não de proteção por meio de direitos autorais.

Por fim, buscou-se discutir, no terceiro tópico, se as obras geradas por IA deveriam ou não ser protegidas pelos direitos autorais e, em caso positivo, quem deveria ser o titular de tais direitos. Diante disso, foi feita uma análise dos prós e contras de diferentes alternativas, chegando-se à conclusão de que a titularidade dos direitos das obras produzidas por Inteligência artificial deve ser examinada caso a caso.

1. Regulamentação na União Europeia

O mais importante acordo internacional sobre direitos autorais é a Convenção de Berna de 1886. Também importantes no campo do direito de pro-

priedade intelectual são a Convenção de Roma, o Acordo TRIPS (*Agreement on Trade-Related Aspects of Intellectual Property Rights*)² e os tratados da Organização Mundial da Propriedade Intelectual (OMPI) sobre Internet de 1996, a saber, o Tratado da OMPI sobre Direito Autoral³ e o Tratado da OMPI sobre Performances e Fonogramas⁴ (Pila *et al.*, 2016, p. 246). Na União Europeia (UE), não existe uma lei de direitos autorais comum a todos os países. Cada Estado Membro tem sua própria legislação para proteger os direitos autorais e direitos conexos. No entanto, a estrutura regulatória foi harmonizada através de 11 (onze) diretivas, incluindo a Diretiva da Sociedade da Informação 2001/29/CE, a Diretiva de Software 2009/24/CE, a Diretiva de Banco de Dados 96/9/CE e a Diretiva de Prazo 2006/116/CE.

Pode-se dizer, de uma forma geral, que a estrutura de Propriedade Intelectual foi projetada por (e para) seres humanos, com base na premissa básica de recompensar a criatividade humana e as conquistas intelectuais – por meio de direitos econômicos e morais – e promover o desenvolvimento cultural e tecnológico (Lauber-Rönsberg *et al.*, 2019, p. 572-573). Mais especificamente, o sistema de direitos autorais busca um equilíbrio entre os interesses de autores e titulares de direitos, de um lado, e a disseminação pública da cultura e o direito de acessar informações, de outro (Bohler, 2017, p. 10).

Para que possa ser protegida pela legislação de direitos autorais da UE, a obra deve cumprir certos requisitos. Primeiramente, a obra deve estar enquadrada numa das matérias protegidas por direitos de autor, ou seja, deve ser uma produção no domínio literário, científico ou artístico⁵. Assim, uma vez que os sistemas de IA são capazes de produzir vários tipos de obras artísticas, tais como pinturas, livros e música, o requisito previsto no art. 2 da Convenção de Berna encontra-se cumprido. Em segundo lugar, para ser protegida pelos direitos autorais, é preciso que uma obra cumpra o requisito de originalidade. Embora não exista uma diretiva de direitos autorais que defina uniformemente a exigência de originalidade para todos os tipos de assuntos protegidos por direitos autorais, as disposições específicas do Artigo 1 (3) da Diretiva de Sof-

2. Em português, “Acordo ADPIC (Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio)”.

3. Em inglês, “WIPO Copyright Treaty (WCT)”.

4. Em inglês, “WIPO Performances and Phonograms Treaty (WPPT)”.

5. Artigo 2 da Convenção de Berna.

tware, do Artigo 6 da Diretiva de Banco de Dados, e do Artigo 16 da Diretiva 2006/116 com relação a fotografias, deixam claro que uma obra deve ser uma “criação intelectual do próprio autor” a fim de qualificar-se para a proteção de direitos autorais (Lauber-Rönsberg *et al.*, 2019, p. 572).

Dessa forma, uma vez que a legislação é limitada, ficou a cargo da jurisprudência do Tribunal de Justiça da União Europeia (TJUE)⁶ definir os contornos da “originalidade”. Com a importante decisão do *Infopaq*⁷ de 2009, este Tribunal confirmou a interpretação de que a proteção é concedida se a obra (ou o elemento da obra) expressa “a criação intelectual do próprio autor”. Além disso, com a decisão do *Infopaq* o TJUE estendeu essa definição de originalidade (contida nas 3 diretivas acima destacadas) a todo o direito autoral, independentemente do objeto de proteção (obras artísticas, literárias, musicais ou técnicas) (Deltorn *et al.*, 2018, p. 8; Bonadio *et al.*, 2018, p. 11; Senja, 2018, p. 27). Dessa forma, é possível dizer que o TJUE harmonizou o conceito de originalidade na União Europeia. Posteriormente, as decisões do TJUE em *Murphy*⁸, *Painer*⁹ e *Football Dataco*¹⁰ esclareceram e aprofundaram ainda mais o significado de originalidade na UE. Especificamente na decisão *Painer*, o Tribunal esclareceu que os direitos resultantes de uma criação intelectual são de titularidade de um autor se refletir a sua personalidade. Este seria o caso se o autor fosse capaz de expressar suas habilidades na produção da obra, fazendo escolhas livres e criativas. Estas escolhas que permitiriam, portanto, ao autor, carimbar a obra com o seu “toque pessoal” (Bonadio *et al.*, 2018, p. 12; Senja, 2018, p. 29; Lauber-Rönsberg *et al.*, 2019, p. 573).

Até agora, pode-se concluir que a ênfase na “criação intelectual própria” e no “toque pessoal” do autor sugere que a exigência de originalidade requer algum nível de contribuição humana, de maneira que obras geradas de forma completamente autônomas por IA não seriam elegíveis para a proteção dos direitos autorais (Lauber-Rönsberg *et al.*, 2019, p. 573). Esta interpretação é

6. Em inglês, “*Court of Justice of the European Union (CJEU)*”.

7. ECJ Case C-5/08 *Infopaq International A/S v. Danske Dagblades Forening*, [2009] ECR I-6569, ECLI:EU:C:2009:465. (*Infopaq*)

8. Joined Cases C-403/08 and C-429/08 *Football Association Premier League v. QC Leisure and Karen Murphy v. Media Production Services Ltd*, [2011] ECR I-9083, ECLI:EU:C:2011:631. (*Murphy*)

9. ECJ Case 145/10 *Eva-Maria Painer v. Standard VerlagsGmbH and others*, [2011] ECLI:EU:C:2011:798. (*Painer*)

10. ECJ Case 604/10 *Football Dataco Ltd et al v. Yahoo! UK Ltd et al.*, [2012] ECLI:EU:C:2012:115. (*Football Dataco*)

confirmada pelas legislações da França¹¹, Alemanha¹², Espanha¹³, e dos Estados Unidos da América¹⁴ (Deltorn *et al.*, 2018, p. 09; Bonadio *et al.*, 2018, p. 13).

Apesar disso, é possível dizer que o desenvolvimento exponencial da tecnologia e o uso de IA criativa para realizar atividades complexas empurrarão os limites da originalidade e da criatividade cada vez mais, exigindo assim uma minuciosa análise caso a caso a fim de determinar o nível de interferência humana no processo criativo (Bonadio *et al.*, 2018, p. 13).

2. As obras geradas por Inteligência Artificial são protegidas pela atual legislação de direitos autorais da União Europeia?

O desenvolvimento atual da tecnologia de Inteligência Artificial tem dificultado a identificação da contribuição humana e da contribuição da IA na produção de uma obra. Hoje, a IA não só auxilia no processo de criação (como uma ferramenta), como também gera obras de forma relativamente autônoma. Essa evolução se deve à utilização de redes neurais artificiais que “ensinam” a IA a combinar regras de montagem, após terem sido “treinadas” numa base de dados de obras pré-existentes (Senja, 2018, p. 43).

Para determinar se uma obra gerada por IA pode ser protegida pela legislação atual, é preciso analisar se tal obra atende aos requisitos de proteção de direitos autorais da UE. Tendo em vista que nem a legislação da UE nem os instrumentos internacionais contêm uma definição geral de “autor” (Pila, 2016, p. 293), a análise do requisito de originalidade torna-se o cerne da questão. Conforme ficou demonstrado, o TJUE entende que uma obra original é a “criação intelectual própria do autor” (“*Infopaq*”), expressa por seu “toque pessoal” e “livre escolha criativa” (“*Painer*”) (Ramalho, 2017, p. 8). Dessa forma, ao declarar que a criação deve refletir a personalidade do autor, pode-se interpretar

11. Artigo L.111-1 do Código Francês da Propriedade Intelectual refere-se ao trabalho protegido por direitos autorais como uma “criação da mente”.

12. A Seção 7 da legislação da Alemanha sobre direitos autorais afirma que “o titular dos direitos é o criador da obra”.

13. Ver Preâmbulo, da Lei 22/11 sobre Propriedade Intelectual de 1987: “os direitos que correspondem ao autor, que é quem realiza a tarefa puramente humana e pessoal de criar a obra e, portanto, constituem o núcleo essencial do objeto desta Lei”.

14. Escritório de Direitos Autorais dos Estados Unidos da América (U.S. Copyright Office), Compendio de Práticas do Escritório de Direitos Autorais dos Estados Unidos da América (Compendium of U.S. Copyright Office Practices) § 101 (3d ed. 2017), 306, que prevê que “o Escritório de Direitos Autorais dos Estados Unidos da América registrará uma obra original de autoria, desde que a obra tenha sido criada por um ser humano”.

que o Tribunal exige a existência de contribuição humana, de modo que obras geradas por IA de forma completamente autônomas não seriam elegíveis para proteção por direitos autorais. Esse entendimento demonstra que o requisito da originalidade está intrinsecamente ligado à análise do processo que conduz à obra e não às características da produção final. Isso significa que é necessário que o autor da obra tenha o efetivo controle sobre o processo criativo, realizando escolhas criativas livres, o que significa que essas escolhas não podem ser limitadas por requisitos ou regras técnicas – como no caso dos limites naturalmente impostos às linhas de código de um programa de software.

Dessa forma, torna-se necessário analisar caso a caso, a fim de se concluir se o nível de envolvimento humano é suficiente para atrair a proteção dos direitos autorais. Assim, a fim de facilitar essa análise, a doutrina legal estabeleceu duas categorias de obras de computador considerando o nível de contribuição humana: (I) *Obras assistidas por computador*, que são aquelas com uma influência humana substancial no processo criativo, executando o programa, tomando as decisões criativas e gerando o resultado pretendido; (II) e *Obras geradas por computador*, que são aquelas com mínima ou nenhuma contribuição humana, permitindo que a máquina gere autonomamente o resultado (Bonadio *et al.*, 2018, p. 10). De acordo com esta classificação, as obras assistidas por computador poderiam ser protegidas por direitos de autor, como quando um músico utiliza software como ferramenta para fazer arranjos e criar música, pois, neste caso, o resultado refletirá os impulsos criativos do artista e, portanto, sua personalidade; no entanto, as obras geradas por computador, como as músicas compostas por IA de forma completamente autônoma, não poderiam ser objeto de direitos de autor. Essa perspectiva é bastante conservadora e, por essa razão, vem sofrendo uma forte oposição a fim de conceder às obras geradas por IA um status de proteção.

De uma forma geral, pode-se dizer que para que uma obra seja protegida pelos direitos autorais, é necessário que a contribuição humana no processo criativo supere a contribuição da máquina, no sentido de pertencer ao ser humano o controle real sobre o processo criativo – por exemplo, através da escolha de parâmetros criativos executados pelo computador –, a fim de que o resultado final reflita predominantemente a criação intelectual do autor humano. Já em relação à criatividade, pode-se dizer que esta é ambígua e menos limitada, mas, em termos gerais, pode ser considerada a “capacidade de inventar ideias ou artefatos que são novos, surpreendentes e valiosos” e “a capacidade de usar um objeto, técnica ou ferramenta para resolver um problema de uma forma útil e previamente desconhecida” (Bridy, 2016, p. 399). Além dis-

so, alguns estudiosos mencionam a capacidade de fazer julgamentos, a aleatoriedade mínima e a autocrítica como requisitos para a criatividade da IA (Ramalho, 2017, p. 3). Nesse mesmo sentido, conclui-se da jurisprudência do TJUE que, para que uma obra seja criativa e, portanto, original, é necessário que se possa estabelecer a existência de uma consciência da sua produção (Bridy, 2012, p. 9). A máquina ainda não pode ser considerada consciente e, portanto, verdadeiramente criativa. A criatividade engloba intenções, emoções, valores, consciência pessoal e senso moral. Coisas que um algoritmo, a base de um sistema de IA, ainda não domina. Assim, o espaço para a verdadeira liberdade criativa é limitado. Por fim, corrobora também a impossibilidade da IA ser autora, a referência feita à “morte do autor”, no Artigo 7 (1), da Convenção de Berna, o que indicaria o propósito do legislador de determinar o autor como um ser humano, uma vez que uma IA não é capaz de morrer (Senja, 2018, p. 33).

Diante de todo o exposto, considerando a atual estrutura de Propriedade Intelectual, que ainda é fortemente antropocêntrica e tradicional (*sistemas droit d’auteur*), a música gerada autonomamente por IA (ou seja, sem contribuição humana substancial no processo de criação) não preenche todos os requisitos e, portanto, não está protegida pela lei de direitos autorais.

3. As obras geradas por Inteligência Artificial devem ser protegidas? E se sim, quem deveria ser o titular dos direitos?

A concessão de proteção por direitos autorais a obras geradas por IA não apenas promoveria o desenvolvimento dessa tecnologia, mas também atrairia ainda mais investimentos em vista dos direitos exclusivos e da vantagem competitiva oferecida pelos direitos autorais. As empresas de IA poderiam recuperar seus investimentos e se defender contra concorrentes desleais (Bonadio *et al.*, 2018, p. 2-3). Além disso, uma harmonização legislativa a nível comunitário na UE garantiria um mesmo nível de proteção nos Estados-Membros, permitindo, assim, a livre circulação de serviços e produtos relacionados à Propriedade Intelectual. Não bastasse, a existência de condições previsíveis e suficientemente claras é crucial para incentivar a inovação europeia no domínio da robótica e da IA, permitindo que a UE seja competitiva e acompanhe o ritmo de outras economias, tais como China, Estados Unidos da América, Coreia do Sul e Japão. Por fim, alguns estudiosos também apontam que o fato de as obras geradas por IA trazerem benefícios à sociedade é mais uma razão para protegê-las com direitos autorais.

Portanto, diante de todo o exposto, pode-se concluir que o ajustamento da legislação em matéria de direitos de autor a nível da UE, a fim de levar em conta as alterações introduzidas pela IA, deverá ser, e provavelmente será, implementado (Bohler, 2017, p. 27). Entretanto, uma vez que os direitos autorais estejam disponíveis para obras geradas por IA, a atribuição de autoria criará alguns problemas para legisladores e formuladores de políticas. Por exemplo, quem deve ser o titular legal dos direitos? O domínio público? A Inteligência Artificial? O programador? O usuário final? (Yu, 2017, p. 1257; Hristov, 2017, p. 443). Esta questão é extremamente importante, pois é o titular dos direitos que se beneficiará comercialmente das obras geradas pela IA, seja através de acordos de venda ou de licenciamento.

O primeiro ponto de vista a ser analisado é o dos que argumentam que não deve haver autoria em obras geradas por IA e que a obra assim criada deve cair no domínio público. A permanência dos direitos de obras geradas por IA em domínio público implica que ninguém detém os direitos sobre tais obras. Conforme destaca Sérgio Branco (2011, p. 58), *“o principal efeito da entrada de determinada obra no domínio público é a possibilidade de sua utilização independentemente de autorização do autor ou do titular dos direitos autorais”*. Os estudiosos que defendem essa posição argumentam que os autores humanos não seriam elegíveis, pois a IA agiria de forma independente tanto em relação ao programador quanto ao usuário final. Quanto aos programadores, porque estes apenas criariam a possibilidade de geração da obra pela IA, e não a obra em si mesma. Quanto aos usuários, porque a IA atuaria para além da contribuição destes, que seria mínima. Sendo assim, tendo em vista que a legislação da UE declara que a falta de autor humano significa uma falta de originalidade, conclui-se que uma obra gerada autonomamente por IA não seria passível de ser protegida por direitos de autor (Dusollier, 2011, p. 24). Consequentemente, ao se admitir que a obra gerada por IA não seria de autoria humana (devido à falta de criação intelectual humana) e nem da própria IA (devido a restrições da lei), torna-se defensável que nenhum privilégio de autoria deveria ser aplicado e as obras geradas autonomamente por IA deveriam pertencer ao público (Gervais, 2019, p. 24).

Além disso, os estudiosos que defendem o domínio público, também argumentam que: (I) as obras geradas por IA podem inundar os mercados, uma vez que a IA tem potencial para gerar um número incalculável de novas obras em um curto espaço de tempo, com baixos custos de produção. Como consequência, isso poderia representar uma concorrência desleal para os autores humanos, e colocar em risco a própria criatividade humana. Diante disso, o

domínio público se apresentaria como uma solução para evitar essa desproporcionalidade na disputa entre obras produzidas por seres humanos e obras produzidas autonomamente por IA; (II) outro argumento é o de que a atribuição das obras geradas autonomamente por IA ao domínio público vai ao encontro de um dos principais objetivos das legislações de direitos autorais, que é expandir a utilização pública das obras, a fim de permitir a disseminação pública da cultura e o direito de acessar informações, impulsionando assim o desenvolvimento cultural e tecnológico da sociedade. Ora, sob a ótica do domínio público, o potencial da IA para produzir um volume massivo de novas obras em um curto espaço de tempo acaba assumindo uma nova conotação, que é a de alavancar a criatividade humana, ao invés de colocá-la sob risco de extinção. Ao inundar a sociedade com novas fontes de inspiração, agora gratuitas, a IA acabaria por tornar-se um importante vetor de desenvolvimento da sociedade como um todo.

No entanto, em que pesem os argumentos a favor do domínio público, a viabilidade desta opção depende também da análise econômica se e até que ponto a proteção da propriedade intelectual é necessária para promover investimentos no desenvolvimento da IA sem correr o risco de efeitos adversos (Lauber-Rönsberg *et al.*, 2019, p. 577). Sendo assim, é possível destacar, em geral, que grande parte dos estudiosos argumentam que se não for concedida proteção às obras de IA, o esforço intelectual ou o investimento colocado no desenvolvimento de máquinas criativas de IA provavelmente será limitado (Senja, 2018, p. 27-28). Isso porque o uso livre, por parte do público, das obras produzidas autonomamente por IA, sem qualquer autorização ou pagamento de taxa, pode significar um golpe mortal para as empresas que investem grandes quantidades de dinheiro no desenvolvimento de sistemas robustos de IA. Não bastasse, terceiros poderão comercializar essas obras de várias formas sem incorrer em qualquer custo e, assim, competir de forma desleal com as empresas que investiram dinheiro no desenvolvimento da IA (Samuelson, 1986, p. 1185; Ahuja, 2020, p. 278). Além disso, mesmo que as empresas invistam grandes quantias de dinheiro e desenvolvam os sistemas de IA, a não proteção às obras geradas de forma autônoma pela IA fará com que a maioria dos produtos não seja trazida à sociedade. E com as inovações mantidas em segredo, não há progresso tecnológico nas artes e na ciência, o que torna impossível para a sociedade evoluir. Dado o exposto acima, a solução que mais parece estar de acordo com os princípios e a lógica dos direitos autorais é a atribuição de direitos a alguém (Senja, 2018, p. 27-28).

Tradicionalmente, o autor da obra também é considerado o titular dos direitos da obra. Entretanto, não é tão simples definir quem seria o titular correto dos direitos de uma obra gerada pela IA, porque neste caso, muitas vezes, há várias partes que participam do processo de criação da obra. Embora tais partes ajudem no processo de criação, nenhuma delas fornece uma contribuição humana suficiente à luz do requisito de originalidade da UE para reivindicar a autoria e, conseqüentemente, a titularidade (Senja, 2018, p. 52).

Uma possibilidade seria conceder a autoria à própria máquina de IA. Segundo Abbott (2016, p. 1102), a concessão de direitos a autores não humanos seria uma forma inovadora de incentivar o desenvolvimento da IA, pois evitaria que as obras geradas pela IA caíssem em domínio público e, ao mesmo tempo, proporcionaria aos programadores e às empresas alguma exclusividade sobre as obras resultantes que poderiam ser protegidas por direitos autorais. Além disso, contribui para a defesa da IA como autora (e titular dos direitos) o argumento de que, apesar dos programadores e usuários poderem participar da criação, é a própria IA quem controla e dirige de fato a essência do processo criativo das obras por ela geradas de forma autônoma. A atuação da IA se daria, no final das contas, de forma independente tanto em relação ao programador quanto ao usuário final.

Em que pese a força de tais argumentos, a atribuição dos direitos à IA não estaria de acordo com a lógica dos direitos econômicos e morais de PI, nem com os requisitos atuais dos direitos autorais, embora alguns estudiosos adotem a ideia de uma “e-Personalidade” como pessoas jurídicas com direitos e obrigações legais e comerciais (Senja, 2018, p. 52-55). Embora a atribuição da autoria (e conseqüentemente dos direitos legais) à IA tenha o benefício de seguir a lógica de que o autor do fato (a máquina) é o titular dos direitos da obra, ela não é consistente com o objetivo dos direitos autorais, que é precisamente o de proporcionar incentivos para que o autor inove. Uma IA não precisa de incentivos financeiros para inovar. Além disso, uma IA não pode pensar e agir como um ser humano, nem pode fazer valer seus direitos em um tribunal de justiça, nem celebrar acordos e licenças. Não bastasse, já que a IA não é capaz de morrer, o tempo para a proteção dos direitos seria eterno (Senja, 2018, p. 52-55). Inclusive, os estudiosos que consideram discutível e equivocada a atribuição da titularidade de direitos autorais à IA argumentam que o fato do ser humano ser mortal e experimentar fadiga enquanto trabalha faz com que crie obras limitadas durante a sua vida. Nesse sentido, os direitos autorais são justificáveis, pois funcionam como uma forma de recompensa pelos seus esforços. A IA, por sua vez, por ser imortal e capaz de produzir um número imenso

de obras sem experimentar fadiga, não necessita de recompensa (Peng, 2018, p. 181).

Além disso, é preciso destacar que a ausência de personalidade jurídica da IA levanta questões importantes. Por exemplo, tendo em vista que os algoritmos do sistema de IA são treinados com bancos de dados pré-existentes, uma escolha pouco criteriosa de tais bancos pode levar ao desenvolvimento de uma IA enviesada, que reproduza e fortaleça opressões existentes na sociedade. A IA, assim, pode desenvolver uma linguagem tendenciosa e tóxica, capaz de difamar e incitar violências de gênero, raça e religião. Diante desse cenário, como fixar a responsabilidade civil e criminal da IA, uma vez que ela não possui personalidade? Da mesma forma, como considerar a IA infratora no caso em que esta gere uma obra substancialmente semelhante a outra obra pré-existente, protegida por direitos autorais (Ahuja, 2020, p. 275)?

Tendo em vista tais argumentos, parece razoável que a titularidade dos direitos das obras geradas pela IA não deva ser atribuída à própria IA, mas ao ser humano que está por trás da máquina. Este, com consciência e personalidade jurídica (Senja, 2018, p. 52-55). A questão seria saber quem: programador ou usuário final?

Alguns estudiosos entendem que uma possibilidade seria atribuir direitos ao programador, que foi o responsável pela concepção do algoritmo de aprendizado. Assim, como o programador é quem faz os esforços e investimentos necessários para a criação de um bom sistema de IA, atribuir-lhe os direitos legais dos trabalhos produzidos pela IA seria uma forma de recompensar seu trabalho. Desta forma, o desenvolvimento da IA seria encorajado. Corroborando a ideia do programador como titular, destaca-se recente julgado chinês, no processo *Tencent Computer System Co., Ltd contra Shanghai Yingxun Technology Co., Ltd.*, em que o Tribunal Popular do *Distrito Shenzhen Nanshan* entendeu que o programador contribuiu com originalidade para uma obra gerada por IA e, por esse motivo, deveria ser o titular dos direitos legais (Du et al., 2020). De uma perspectiva de direito comparado, este caso é excepcional, uma vez que é incomum que um Juízo decida que os programadores exerceram perícia e julgamento numa obra gerada autonomamente por IA (Matulionyte et al., 2022, p. 17).

No referido julgamento, a obra analisada foi um artigo sobre a bolsa de Xangai, escrito pelo software de IA *Dreamwriter* (este, de propriedade da *Tencent*). Esta IA, utilizando seus algoritmos de aprendizado de máquina, recolheu, analisou e verificou os dados de diversas fontes e, com base nestes dados,

escreveu e publicou um artigo. O Réu (*Shanghai Yingxun*) alegou que a obra não poderia ser protegida por direitos autorais, pois não havia criatividade humana na sua produção. No entanto, o tribunal ficou convencido de que seria sim possível perceber a originalidade humana em diversas etapas do processo de criação da obra pela IA. De acordo com o Juízo, embora a IA precisasse de pouquíssimo tempo para produzir o artigo (cerca de 2 minutos), através de regras, algoritmos e modelos estabelecidos sem qualquer participação humana, e embora esta mesma IA não fosse autoconsciente, o seu funcionamento não ocorreu sem uma razão. Pelo contrário, a atuação autônoma da IA refletia importantes escolhas do programador, tais como a seleção e disposição personalizada dos dados, o formato dos dados, as circunstâncias que motivaram a escrita do artigo, os modelos de composição do artigo, a escolha do modelo, e o treinamento do modelo de algoritmo de verificação inteligente. Diante disso, o tribunal entendeu, com base na doutrina da originalidade, que o desenvolvedor da IA *Dreamwriter* era o titular dos direitos da obra. De acordo com o Juízo, as escolhas do desenvolvedor, utilizadas pela IA, exprimiam originalidade ao definir os critérios de seleção e organização dos dados (Matulionyte et al., 2022, p. 17-18; Du et al., 2020).

Apesar do julgado chinês sobre originalidade representar um marco notável para o credenciamento da IA como força criativa, ele não é aplicável a todas as criações de IA. Isso porque nem todo sistema de IA possui um processo de tomada de decisão que pode ser explicado plenamente. Devido às técnicas de aprendizado de máquina (e mais recentemente, de *deep learning*), muitas das decisões sobre o funcionamento de sistemas de IA são tomadas de forma completamente aleatórias/arbitrárias pelos programadores (Bathae, 2018, p. 901-906; Deeks, 2019, p. 1832-1838). Isso faz com que o funcionamento de diversos modelos de IA se dê de forma obscura, sem que os próprios programadores sejam capazes de compreender, interpretar e explicar plenamente o processo de tomada de decisão da IA ou de prever as decisões e resultados gerados pela IA (Banteka, 2021, p. 547-548; Schnader, 2019, p. 34). Dessa forma, fica claro que o programador não controla sempre o processo de criação da obra, sendo impossível perceber o reflexo da sua habilidade e julgamento em todas as etapas desenvolvidas pela IA. Por esse motivo, a constatação da originalidade em *Tencent* não é aplicável universalmente. (Matulionyte et al., 2022, p. 18-19). Por outras palavras, em muitos casos a obra é criada independentemente pela IA, não sendo prevista pelo programador. O programador apenas cria as condições para a produção de tal obra, não a obra em si (Senja, 2018, p. 55). Além disso, há situações em que a IA é desenvolvida com partici-

pação de outras partes, tais como treinadores e fornecedores de dados, que atuam de forma independente quanto aos programadores que criaram a IA. E justamente por não haver controle ou planejamento quanto ao comportamento desses terceiros é que se torna ainda mais difícil para os programadores originais preverem as obras que serão geradas pela IA (Matulionyte *et al.*, 2022, p. 19).

Outro argumento contrário ao programador, é que este tem a propriedade sobre o algoritmo e, adicionalmente, pode obter a proteção dos direitos autorais do software (Lauber-Rönsberg *et al.*, 2019, p. 572). Isto porque, de acordo com a Diretiva de Software 91/250/CE, o programador tem os direitos de propriedade sobre o próprio algoritmo de aprendizagem. Em outras palavras, o programador já é recompensado por seu trabalho. Se os direitos das obras geradas pela IA fossem atribuídos ao programador, ele seria super-recompensado, o que não é o propósito do sistema de PI (Senja, 2018, p. 56-57). Não bastasse, há casos em que a IA é criada por vários programadores que, por sua vez, seriam titulares dos direitos das obras geradas pela IA. Isto certamente causará problemas, pois se a IA for vendida ou licenciada a terceiros, será necessário o consentimento de todos os programadores. Isto aumentará os custos de transação dos acordos comerciais e diminuirá a eficácia do mercado (Senja, 2018, p. 56).

Por outro lado, alguns estudiosos argumentam que os usuários finais poderiam reivindicar a autoria de obras geradas por IA, dado o fato de que a obra em si não existiria se não fosse pelo comando do usuário. Este argumento falha em cumprir com o requisito de tomada de decisão criativa pela mesma razão que a autoria do programador acima mencionada, ou seja, porque a obra gerada não é uma criação direta do usuário final (Senja, 2018, p. 57-58; Hristov, 2017, p. 444-445). No entanto, há estudiosos, como Senja (2018, p. 57-59), que entendem que os direitos das obras produzidas pela IA devem ser atribuídos aos usuários finais, de modo que eles seriam encorajados a empregar sistemas avançados de IA na criação de novas obras. E uma vez que os usuários finais procurem utilizar cada vez mais sistemas avançados de IA, eles investirão no mercado, o que certamente recompensará indiretamente os programadores. Isto significa que os programadores serão encorajados a desenvolver sistemas de IA sofisticados a fim de se distinguirem no mercado. Isto aceleraria o ritmo da inovação e beneficiaria a sociedade como um todo, alcançando assim os objetivos gerais da legislação de direitos autorais da UE. Senja (2018, p. 57-

59) também destaca que a atribuição de titularidade ao usuário final eliminaria a necessidade de distinguir entre obras assistidas por IA e obras geradas por IA, o que, por sua vez, tornaria mais fácil o julgamento nos tribunais.

No recente julgado chinês *Feilin* contra *Baidu*, o Tribunal da Internet de Pequim decidiu que o usuário final era o titular dos direitos de uma obra produzida por uma IA. De acordo com o tribunal, nem o programador e nem o usuário podiam ser os autores da obra: o programador, porque não foi ele quem fez a pesquisa no banco de dados através de palavras-chave; o usuário, porque ele apenas digitou as palavras-chave utilizadas na pesquisa. Segundo o Juízo, nenhum dos dois atores-chave agiu de forma a exprimir originalidade ao abrigo da lei de direitos autorais. No entendimento do tribunal, a obra foi criada, na verdade, pelo *Banco de Dados Wolters Kluwer*. Mas como este não é uma pessoa natural, não poderia ser o autor. Diante disso, e reconhecendo que seria melhor atribuir a titularidade dos direitos da obra a um particular, ao invés de deixá-la no domínio público, o tribunal entendeu que a melhor opção seria atribuí-la ao usuário: (I) primeiro, porque o programador já havia recuperado seu investimento através de uma taxa de licença sobre o software; (II) segundo, porque ao se atribuir a titularidade ao usuário, este teria maior motivação para utilizar e divulgar a obra gerada pela IA. Dessa forma, haveria uma maior promoção do desenvolvimento cultural e científico, contribuindo para a evolução da sociedade (China, 2019).

Apesar do mérito desse pensamento, é preciso destacar que a atribuição da titularidade ao usuário sofre do mesmo problema que a atribuição ao programador: não é um entendimento que possa ser aplicado universalmente a qualquer caso envolvendo obras geradas autonomamente por IA. Isso porque nem todos os usuários finais de IA possuem os mesmos interesses e objetivos de utilização das obras, como os do usuário no caso *Feilin*. Tais interesses e objetivos variam de caso para caso. Além disso, também varia de caso para caso o nível de contribuição dos utilizadores para a geração de obra por IA (Matulionyte *et al.*, 2022, p. 22).

Alguns estudiosos, como Bridy (2012, p. 27-28), argumentam que as obras geradas por IA seriam prontamente assimiladas à estrutura de direitos autorais através da Doutrina “*Work-Made-For-Hire*” (presente na “Lei de Direitos Autorais”¹⁵ dos Estados Unidos da América), que é uma ficção legal refletida

15. Em inglês, “*Copyright Act*”.

por uma escolha política a fim de beneficiar o autor de direito (programador ou mesmo uma empresa) em detrimento do autor de fato (máquina de IA).

Alguns sistemas legais adotaram abordagem semelhante à proposta de Bridy para proteger obras geradas estritamente por IA. Por exemplo, o Reino Unido (UK)¹⁶ adotou uma solução prática para o dilema da autoria, estabelecendo na Seção 9 (3) da “Lei de Direitos Autorais, Desenhos e Patentes do Reino Unido” de 1988¹⁷ que “no caso de uma obra literária, dramática, musical ou artística gerada por computador, o autor deve ser considerado a pessoa por quem os arranjos são feitos”¹⁸. Esta lei cria uma ficção legal que estende o conceito do autor (e do titular dos direitos econômicos relevantes) para incluir uma pessoa (natural ou jurídica) que pode não ter desempenhado nenhum papel na produção da obra, mas apenas tomou medidas para que esta produção acontecesse.

Pode-se argumentar que o regime britânico pode ser útil para identificar a autoria - e consequente titularidade - em casos de obras produzidas pela IA sem contribuição humana. No entanto, a identificação da pessoa que fez os arranjos necessários para que a máquina criasse torna-se um problema, uma vez que a “Lei de Direitos Autorais, Desenhos e Patentes do Reino Unido” (1988) não fornece nenhum parâmetro. Foi o programador? O usuário? O investidor? Certamente tal legislação não cria segurança jurídica (Bonadio *et al.*, 2018, p. 14). Além disso, a abordagem britânica tem sido criticada por não focar nos seres humanos como centro de proteção dos direitos autorais, e por tornar desnecessários os critérios de originalidade (Celik, 2020, p. 10).

Finalmente, deve-se destacar que existe também a ideia de se criar um regime jurídico diferente para a proteção de obras geradas por IA, um direito *sui generis*. No entanto, esta ideia não é bem recebida pela maioria dos estudiosos, pois há dúvidas sobre quais requisitos substantivos de proteção devem ser aplicados a tais direitos de PI para produtos gerados por IA, e a quem o direito deve ser atribuído (Lauber-Rönsberg *et al.*, 2019, p. 577).

16. Esta solução também foi adotada por outros países do sistema “*Common Law*”, tais como Irlanda, Nova Zelândia, Índia, África do Sul e Hong Kong.

17. Em inglês, “*UK Copyright, Designs and Patents Act (1988)*”.

18. Em inglês, “*in the case of a computer-generated literary, dramatic, musical or artistic work, the author must be considered the person by whom the arrangements are made*”.

Considerações finais

Olhando para a lei existente, parece que em sistemas de *droit d'auteur*, que são baseados em um conceito antropocêntrico de direitos autorais, obras criadas estritamente pela IA ou sem contribuição humana substancial não podem ser protegidas por leis de direitos autorais. E mesmo que haja uma contribuição humana, esta deve ser eficaz no sentido de exercer controle sobre o resultado gerado. Por outro lado, no sistema apresentado pelo Reino Unido, baseado em um conceito econômico de direitos autorais, torna-se possível a proteção de produções em que não há a participação do ser humano. Ao criar uma ficção legal que amplia o conceito de direitos de autor (e o consequente titular dos direitos econômicos) o sistema abrange uma pessoa que pode não ter participado de nenhuma etapa da produção da obra.

Independentemente do sistema, é preciso ter em mente que à medida que a tecnologia avança e permite que as máquinas se tornem mais autônomas para produzir obras intelectuais – incluindo música –, torna-se também cada vez menos possível diferenciar tais obras das obras produzidas por humanos. Portanto, será necessário que os sistemas jurídicos se desenvolvam como um todo, a fim de responder aos casos cada vez mais complexos que começam a surgir. Além disso, a sobrevivência e o desenvolvimento do setor de tecnologia, e mais especificamente do setor de IA, dependem de uma proteção legal mais eficaz, capaz de gerar um nível mais elevado de segurança jurídica. Assim, consciente da importância sempre crescente da tecnologia no mundo globalizado e em rápida mudança de hoje, e das contribuições ilimitadas da IA no campo artístico, literário, musical e em muitos outros campos, o Direito na Economia 4.0 deve avançar em direção a um sistema inovador e adaptável, em vez de impor limitações à criação e ao uso de tecnologias. O dilema da autoria em relação à música composta por IA é apenas uma das muitas questões decorrentes da insuficiência do atual quadro legal para lidar com todas as tecnologias emergentes.

É um fato que proteger as obras geradas por IA através de direitos autorais é mais vantajoso do que prejudicial. No entanto, determinar quem deve ser o titular dos direitos é uma questão que deve ser estudada mais detalhadamente através de uma análise caso a caso, na qual deve-se sempre levar em consideração quem controlou efetivamente o processo criativo da obra, de forma a ter exprimido de fato uma originalidade.

Referências

ABBOTT, R. (2016). *I think, Therefore I Invent: Creative Computers and the Future of Patent Law*. 57 Boston College Law Rev: 1079-1126.

AHUJA, V. K. (2020). *Artificial Intelligence and Copyright: Issues and Challenges*. ILLI Law Review Winter Issue 2020.

BANTEKA, N. (2021). *Artificially Intelligent Persons*. 2021 58(3) Houston Law Review, p. 537-596.

BATHAEE, Y. (2018). *The Artificial Intelligence Black Box and the Failure of Intent and Causation*. 2018 31(2) Harvard Journal of Law & Technology, p. 889-938.

BOHLER, H. (2017). *EU copyright protection of works created by artificial intelligence systems*. Master's Thesis. The University of Bergen.

BONADIO, E.; MCDONAGH, L.; ARVIDSSON, C. (2018). *Intellectual Property Aspects of Robotics*. 2018. European Journal of Risk Regulation 4/2018: 1–20.

BRANCO, S. (2011). *O Domínio Público no Direito Autoral Brasileiro*. Rio de Janeiro: Lumen Juris.

BRIDY, A. (2012). *Coding Creativity: Copyright and the Artificially Intelligent Author*. 2012. Stanford Technology Law Review. 5/2012: p. 1-28.

BRIDY, A. (2016). *The Evolution of Authorship: Work Made by Code*. Columbia Journal of Law & the Arts, 39(3): p. 395-401.

CELIK, E. (2020). *How Ip Struggles to Define AI-Generated Products and the Ownership Dilemma*. Disponível em <https://ssrn.com/abstract=3763885>. Acessado em 04 de Abril de 2022.

CHINA. Beijing Internet Court -Civil Judgment. (2018) Jing 0491 Min Chu No. 239. Disponível em: [http://www.chinadaily.com.cn/specials/BeijingInternetCourtCivilJudgment\(2018\)Jing0491MinChuNo.239.pdf](http://www.chinadaily.com.cn/specials/BeijingInternetCourtCivilJudgment(2018)Jing0491MinChuNo.239.pdf). Acessado em: 10 de abril de 2022.

DEEKS, A. (2019). *The Judicial Demand for Explainable Artificial Intelligence*. (2019) 119(7) Columbia Law Review, p. 1829-1850.

DELTORN, J.M.; MACREZ, F. (2018). *Authorship in the age of machine learning and artificial intelligence* Center for International Intellectual Property Studies Research Paper. 10:3-23.

DOWNES, L. (2009). *The laws of disruption*. 1st ed. New York: Basic Books.

DU, G.; YU, M. (2020). *Tencent v. Yingxun Tech*. China Justice Observer. Disponível em <https://www.chinajusticeobserver.com/law/x/2019-yue-0305-minchu-14010>. Acessado em 06 de Abril de 2022.

DUSOLLIER, S. (2011). *Scoping Study on Copyright and Related Rights and the Public Domain*. World Intellectual Property Organisation Publication.

ESTADOS UNIDOS DA AMÉRICA. Compendium of U.S. *Works that lack human authorship*. Section 313.2. Copyright Office Practices, Third Edition (December 22, 2014).

GERVAIS, D. J. (2019). *The Machine as Author*. 105 Iowa Law Review 19.

HRISTOV, K. (2017). *Artificial Intelligence and the Copyright Dilemma*. The Journal of the Franklin Pierce Center for Intellectual Property, 57(3).

Joined Cases C-403/08 and C-429/08 Football Association Premier League v. QC Leisure and Karen Murphy v. Media Production Services Ltd, [2011] ECR I-9083, ECLI:EU:C:2011:631. (Murphy)

LAUBER-RÖNSBERG, A.; HETMANK, S. (2019). *The concept of authorship and inventorship under pressure: Does artificial intelligence shift paradigms?* 2019. Journal of Intellectual Property Law & Practice 14(7):570-579.

MATULIONYTE, R.; LEE, J. (2022). *Copyright in AI-generated Works: Lessons from Recent Developments in Patent Law*. SCRIPTed: A Journal of Law, Technology & Society. Volume 19, Issue 1, 2022. The Chinese University of Hong Kong Faculty of Law Research Paper No. 2021-73. Disponível em: <https://ssrn.com/abstract=3974280>. Acessado em: 05 de Abril de 2022.

PENG, S. C. (2018). *Artificial Intelligence and Copyright: The Author's Conundrum*. WIPO-WTO Colloquium Papers.

PILA, J.; TORREMANS, P. (2016). *European Intellectual Property Law*. Oxford University Press, 2016.

RAMALHO, A. (2017). *Will Robots Rule the (Artistic) World? A Proposed Model for the Legal Status of Creations by Artificial Intelligence Systems*. Journal of Internet Law, 21(1).

REINO UNIDO. *Copyright, Designs and Patents Act 1988*. Section 72. The Intellectual Property Office (April 20, 2016).

SAMUELSON, P. (1986). *Allocating Ownership Rights in Computer-Generated Works*. Vol. 47. University of Pittsburgh Law Review.

SARTOR, G.; LAGIOIA, F.; CONTISSA, G. (2018). *The use of copyrighted works by AI systems: Art works in the data mil.* 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3264742. Acessado em: 07 de janeiro de 2022.

SCHNADER, J.A. (2019). *Mal-Who? Mal-What? Wal-Where? The Future Cyber-Threat of A Non-Fiction Neuromance: Legally Un-attributable, Cyberspace-Bound, Decentralized Autonomous Entities.* (2019) 21(2) North Carolina Journal of Law & Technology, p. 01-40.

SENJA, A. (2018). *European Union Copyright Protection for AI-Generated Works.* Master's Thesis. University of Turku.

UNIÃO EUROPEIA. Diretiva 91/250/CEE de 14 de maio de 1991 relativa à proteção jurídica dos programas de computador, [1991], JO L 122/42; republicada como Diretiva 2009/24/CE do Parlamento Europeu e do Conselho de 23 de abril de 2009 relativa à proteção jurídica dos programas de computador, [2009] JO L/16. (“Diretiva de Software 91/250/CE”).

UNIÃO EUROPEIA. Diretiva 2006/116/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa ao prazo de proteção dos direitos autorais e de certos direitos conexos, [2006], JO L 372/12; originalmente publicada como Diretiva 93/98/CEE do Conselho, de 29 de outubro de 1993, que harmoniza o prazo de proteção dos direitos autorais e de certos direitos conexos, [1993] JO L 290/9. (“Diretiva de Prazo 2006/116/EC”).

UNIÃO EUROPEIA. Diretiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à proteção jurídica de bancos de dados, [1996] JO L 77/20. (“Diretiva 96/9/CE relativa a bancos de dados”).

UNIÃO EUROPEIA. Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de maio de 2001, relativa à harmonização de certos aspectos dos direitos autorais e direitos conexos na sociedade da informação, [2011], JO L 167/10. (“Diretiva Infosoc 2001/29/CE”).

UNIÃO EUROPEIA. ECJ Case 604/10 Football Dataco Ltd *et al* v. Yahoo! UK Ltd *et al.*, [2012] ECLI:EU:C:2012:115. (Football Dataco)

UNIÃO EUROPEIA. ECJ Case 145/10 Eva-Maria Painer v. Standard VerlagsGmbH and others, [2011] ECLI:EU:C:2011:798. (Painer)

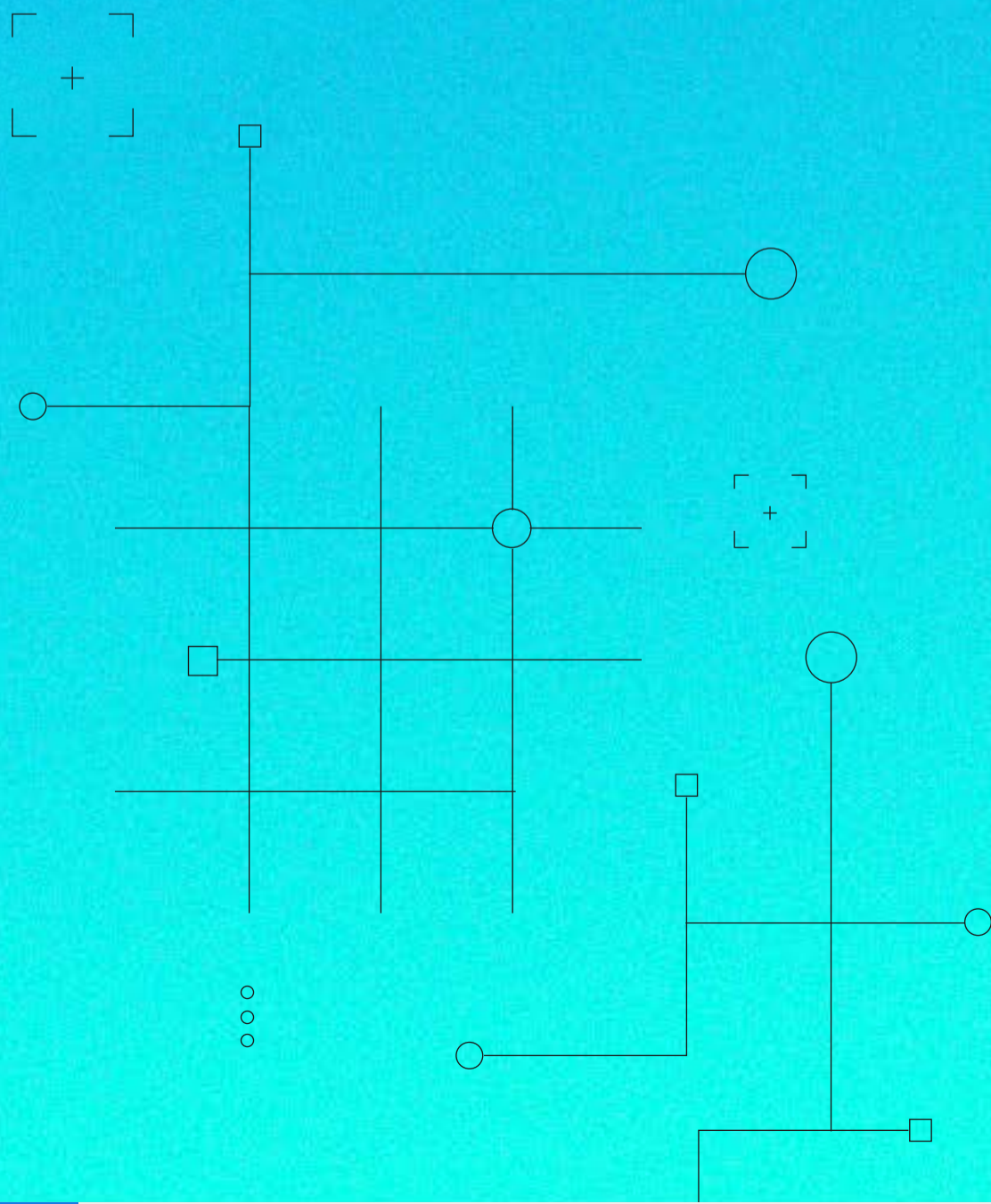
UNIÃO EUROPEIA. ECJ Case C-5/08 Infopaq International A/S v. Danske Dagblades Forening, [2009] ECR I-6569, ECLI:EU:C:2009:465. (Infopaq)

YANISKY-RAVID, S.; VELEZ-HERNANDEZ, L. (2017). *Copyrightability of Artworks Produced by Creative Robots, Driven by Artificial Intelligence Systems and the Concept of Originality: The Formality - Objective Model*. Minnesota Journal of Law, Science & Technology, 19(1).

YU, R. (2017). *The Machine Author: What Level of Copyright Protection Is Appropriate For Fully Independent Computer-Generated Works?* University of Pennsylvania Law Review, 165/2017.

Tracking Pixels: riscos invisíveis à privacidade

MARIA LUIZA CORREIA FERNANDES



Sumário: Introdução. 1. Afinal, o que são cookies e por que se discute seu fim? 1.1. “Nós usamos cookies e outras tecnologias semelhantes”. Que tecnologias? 2. Relação da tecnologia com a Lei Geral de Proteção de Dados Pessoais (LGPD) 3. Segurança da Informação e vulnerabilidades 4. The Digital Standard. Considerações finais. Referências

Introdução

Em um momento no qual muito se discute sobre o fim dos cookies e suas consequências para a publicidade digital, pouco se menciona o uso de outras tecnologias semelhantes que podem representar riscos ainda maiores à privacidade no ambiente digital. Por isso, a pesquisa pretende explorar que outras tecnologias são essas, com enfoque em uma específica, os *tracking pixels* ou pixels de rastreamento.

Em seguida, serão abordados alguns dispositivos da Lei Geral de Proteção de Dados, sobretudo transparência, um dos princípios trazidos pela Lei, direito dos titulares e a dificuldade na definição de uma hipótese legal que sustente o tratamento dos dados por meio dessa ferramenta para as finalidades mais comuns - acompanhamento de métricas de e-mail marketing e veiculação de anúncios publicitários no ambiente online, de modo a refletir sobre o uso dessa ferramenta à luz da LGPD.

Em seguida, são abordados alguns aspectos dos riscos de segurança da informação, principalmente a possibilidade de exploração de vulnerabilidades por terceiros pela execução de pixels e a impossibilidade de adoção de medidas protetivas pelos usuários.

Ao longo do estudo são apresentadas algumas possibilidades para repensar e avaliar o uso dessa tecnologia, seja por parte do próprio usuário, quanto pelos atores envolvidos no seu desenvolvimento e aplicação, como tentativa de torná-la menos invasiva.

1. Aluna da pós-graduação em Direito Digital da UERJ e ITS-Rio. Formada em Direito pela Universidade Presbiteriana Mackenzie, atua com privacidade e proteção de dados com foco em desenvolvimento de produtos digitais.

1. Afinal, o que são cookies e por que se discute seu fim?

Nos deparamos frequentemente com textos padronizados como “nós usamos cookies e outras tecnologias semelhantes para melhorar a sua experiência em nossos serviços”. Mas o que seriam cookies? Tal tecnologia, quando criada, visava melhorar a experiência do usuário no navegador, sobretudo no comércio eletrônico, a fim de guardar algumas informações durante uma sessão e evitar o preenchimento repetido de informações por um usuário da internet.

Em 1995, a NetScape Communication Corporation desenvolveu os *magic cookies*, que tecnicamente, mantinham o estado do protocolo HTTP para que as informações não se perdessem. O HTTP é um protocolo de comunicação que permite a troca de dados entre clientes e servidores. Essa troca permite que os conteúdos sejam reconstruídos por meio das requisições iniciadas pelo destinatário, que reúne texto, layout, imagens, vídeos e scripts (MOZZILA).

Nesse sentido, ao manter o protocolo HTTP, os cookies armazenados passaram a permitir que o navegador lembrasse os itens de um carrinho de compras, autenticasse o usuário, personalizasse a exibição da página quanto ao idioma, medidas para otimização da tela -considerando o tamanho do dispositivo utilizado-, hora local, dentre outros (PALHARES, 2020, p. 12).

Ocorre que, com a expansão da internet e um aumento significativo de usuários, tal tecnologia passou a ser utilizada para finalidades diversas da inicial, principalmente na publicidade digital “para se viabilizar algum tipo de tática de marketing digital como *targeting*, *remarketing* ou mesmo para medições de campanhas *on-line* com controles de alcance e frequência” (NÓBREGA, 2021). e prover às empresas métricas para as suas atividades no ambiente digital. Com isso, muito dificilmente se encontra um *website* que não se utilize de cookies.

Com o aumento do debate relacionado à privacidade e proteção de dados, seja pela aprovação de leis que buscam garantir maior proteção aos indivíduos, como também pelo aumento significativo de incidentes envolvendo dados pessoais, alguns navegadores deixaram de se utilizar de cookies de terceiros (*third-party cookies*). Nessa discussão os navegadores tornaram-se os guardiões da internet, posicionando-se fortemente em favor da privacidade dos usuários. Para entender melhor, o levantamento mais recente da Net Applications realizado em 2021 apontou que o Firefox possui 2,18% dos usuários e o Safari 13,92% (CANALTECH).

O Firefox passou a limitar a execução de cookies de terceiros por meio do ETF “*Enhanced Tracking Prevention*” (IAB Brasil, 2021, p. 13), mas é o Safari que “acumula a história mais longa de iniciativas de proteção de dados” (IAB Brasil, 2021, p. 15) com adoção da Prevenção contra o Rastreamento Inteligente (ITP-*Intelligence Tracking Prevention*), que bloqueia cookies de terceiros usando *machine learning* há mais de dois anos.

Já foram lançadas diversas funcionalidades de privacidade pelos navegadores e desde então cada atualização aumenta os níveis de proteção, no entanto, o debate fica nas mãos do Google, que possui a maior fatia de usuários (66%)². Em 2020 a empresa comunicou que descontinuará o apoio a cookies de terceiros no Chrome com previsão para 2022 (CHROMIUM BLOG, 2020). Já em 2021 anunciou o adiamento da medida para 2023, enquanto testa soluções no Privacy Sandbox.

Apesar das preocupações crescentes com a privacidade dos usuários, ainda há pouca abertura para discutir os riscos à privacidade oferecidos por tecnologias similares aos *cookies* e que por vezes sequer são de conhecimento do usuário.

1.1 “Nós usamos cookies e outras tecnologias semelhantes”. Que tecnologias?

Pixels são imagens (.png ou .gif) de 1x1 cujo carregamento é responsável por enviar uma requisição - ou uma mensagem - para um servidor. Apesar de não ser visualizado pelo usuário, por se tratar de uma imagem minúscula e imperceptível ou até mesmo transparente no fundo da página, pixels são largamente utilizados tanto em *e-mail marketing*, como em *banners* publicitários. Por meio deles é possível medir o engajamento dos usuários seja na taxa de abertura e leitura de e-mails ou no rastreamento de comportamentos como compras de produtos e serviços. A imagem abaixo mostra como a ferramenta é instalada, junto ao código, de modo que um titular de dados pessoais dificilmente conseguiria identificar sua execução ao carregar uma página *web* sem um conhecimento técnico.

2. Dados de 2021 (CANALTECH, 2021) mostram que o Google Chrome possui a maior fatia de usuários dos navegadores em geral (66.64%), enquanto os principais concorrentes apresentam números bem menos expressivos como 13.92% (Safari), 4,55% (Microsoft Edge). Por essa razão, foi com a adoção do Google ao fim dos third party cookies que o tema ganhou maior expressividade.

Imagem 1: Visualização da instalação de um pixel



“Most website tracking tools require you to add a small snippet of JavaScript code to every page you want to track.” (HOTJAR)

Em que pese não seja o foco do estudo, cabe mencionar além dos *pixels*, a existência de outras tecnologias de rastreamento, semelhantes e mais persistentes que os *cookies* como *E-tags*, *flash cookies*, *HTML5 Web Storage*, *ever-cookie* e *fingerprints* (BIONI, 2019, p. 153).

A diferença entre os *cookies* e os *pixels* está na entrega. Enquanto os *cookies* armazenam uma informação no navegador -que inclusive pode ser instalado com uma data de expiração pré-definida ou removido proativamente pelo usuário com a limpeza ou reinstalação do navegador -, o carregamento de *pixels* independe de qualquer armazenamento. Por estarem integrados em um código HTML, toda vez que um usuário carrega uma página que contém um *pixel*, este é carregado e, conseqüentemente, comunicado ao servidor. Sendo assim, ao contrário dos *cookies* que dependem de uma instalação no navegador, levando, conseqüentemente, à instalação em casa dispositivo que o usuário utiliza, os *pixels* podem acompanhar o comportamento do usuário em diferentes dispositivos.

Em matéria divulgada pela BBC, Leo Kelion (2021) defende que “*pixels* espiões” ou invisíveis tornaram-se uma epidemia, uma vez que $\frac{2}{3}$ dos e-mails enviados às contas pessoais de usuários se utilizam de *pixels*. Em contrapartida, os defensores dos rastreadores argumentam ser esta uma prática comum de mercado. A utilização da ferramenta em um número expressivo como $\frac{2}{3}$ dos e-mails, deve nos levar ao seguinte questionamento: ainda que seja uma prática comum de mercado, estariam esses usuários bem-informados a respeito da existência de *pixels*, seu uso em e-mails e possíveis impactos?

O acompanhamento de onde os visitantes clicaram ou mantiveram o cursor do mouse por mais tempo também é um possível uso da ferramenta. Esse tipo de prática é chamada de *heat map* ou mapas de calor, uma visualização de dados comportamentais do usuário em um site ou aplicativo às quais são atribuídas intensidades por meios de cores conforme as interações são feitas com o cursor ou movimentação dos olhos. Será que usuários da internet têm visibilidade do uso de seus dados comportamentais - nem sempre de forma agregada - durante uma interação com um *website*?

Uma vez esclarecidas a utilidade e diferenças entre essas tecnologias (*cookies* e *pixels*), cabe investigar qual a relação com a Lei Geral de Proteção de Dados (LGPD).

2. Relação da tecnologia com a Lei Geral de Proteção de Dados Pessoais

Embora se argumente que no Brasil não exista uma legislação que se assemelhe à e-Privacy³ ou às diretrizes específicas para publicidade como no GDPR na Europa, a mera análise de alguns dos artigos da LGPD já deveria revelar alguma preocupação com o tema.

A LGPD traz como um de seus princípios a transparência (art. 6º, VI)⁴. Nesse sentido, é necessário que as organizações atuem de forma proativa, fornecendo informações quanto ao tratamento de dados de forma clara, precisa e acessível. No entanto, ao analisar avisos de privacidade disponibilizados em *websites*, dificilmente se encontram informações detalhadas a respeito do tratamento de dados pessoais realizados em razão do uso de ferramentas como os *pixels*, menos ainda detalhamento quanto à extensão dessa coleta e o impacto que “outras tecnologias” podem ter sobre o comportamento e a privacidade dos titulares de dados.

Some-se à ausência de transparência das organizações o fato de que, por se tratar de uma ferramenta invisível, o usuário não possui meios de identificar quem é o responsável pelo tratamento dos dados (controlador), impossibilitando o cumprimento de um outro requisito da lei, que é o exercício de direitos pelo titular como confirmação da existência de tratamento, acesso, bloqueio

3. Legislação específica aplicável às comunicações eletrônicas.

4. “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”

do tratamento ou descarte dos dados e principalmente informações quanto à finalidade do tratamento.⁵

Ainda que as principais fornecedoras de ferramentas de rastreamento possuam avisos de privacidade em seus sites com algum esclarecimento, cabe ao controlador dos dados disponibilizar de forma facilitada informações sobre os dados coletados, finalidades de tratamento e eventual compartilhamento com terceiros. No entanto, a identificação deste responsável não é clara e imediata pelo titular de dados, pois a própria cadeia de fornecimento torna-se opaca, dado o *design* dos *pixels*.

Desse modo, da forma como a ferramenta está formatada hoje, com pouca ou nenhuma transparência seja quanto ao mero uso da tecnologia, seja quanto ao fornecedor escolhido para provê-la, inviabiliza a identificação de (i) uma finalidade clara, definida e lícita para o tratamento dos dados e, conseqüentemente, (ii) se seria viável determinar uma hipótese legal de tratamento (definição de uma base legal).

Felipe Palhares (2020, p. 22) ilustra a situação de forma didática:

Imagine o cenário: você participa de uma reunião presencial, na qual um dos participantes lhe entrega um cartão de visitas que tem um rastreador invisível dentro, que permite que todos os seus passos sejam monitorados, especialmente as lojas que você vai, os produtos que compra e as pessoas com que você se comunica, sem lhe informar nada sobre a existência desse rastreador. Você se sentiria confortável? E se ele lhe informasse que o rastreador estava dentro do cartão, mas que essa é uma ferramenta padrão, que acompanha todos os novos cartões de visita, melhoraria o seu conforto?

Para além dos dispositivos da LGPD analisados anteriormente que corroboram com o fato de que, a inexistência de uma legislação tal como a e-Privacy⁶ ou diretrizes específicas para a publicidade digital como no GDPR não são impeditivas para se jogar luz no uso de ferramentas como os pixels, cabe acrescentar que mesmo tais legislações, existentes e aplicadas no contexto europeu talvez não supram de forma adequada às necessidades dos titulares,

5. Conforme previsto no artigo 18 da LGPD.

6. “A Diretiva de Privacidade Eletrônica (Diretiva 2002/58 / CE) exige consentimento para qualquer operação de armazenamento ou acesso não essencial de informações obtidas por meio dos dispositivos dos usuários finais, independentemente de serem consideradas dados pessoais.” IAB Brasil, op cit., p. 11.

nem sirvam satisfatoriamente como referencial, posto que exigem a coleta de consentimento do titular, consentimento que se torna inviabilizado pela própria arquitetura da ferramenta.

Dessa forma, evidencia-se a necessidade de trazer um debate fundamental sobre valores e normas, pois ainda que seu uso seja uma prática comum de mercado, há que se atentar aos potenciais riscos à privacidade e segurança dos usuários, sobretudo no que diz respeito à assimetria informacional e à não equiparação dos *pixels* ao tratamento dispensado aos *cookies*.

De todo modo, a proposição de um caminho para aumentar a transparência não deve considerar meramente a inserção de mais um tópico em avisos de privacidade ou a criação de uma caixa de seleção na qual o usuário pode assinalar ativamente, pois tais caminhos já encontram seus próprios desafios, a exemplo da “fadiga do consentimento” (FERNANDES; SUNDFELD, 2021) e a baixa adesão à leitura desses avisos. Em levantamento realizado pela OpenText (BOLZANI, 2021):

Mais de 84% dos brasileiros nunca entraram em contato com alguma empresa para checar como a companhia usa seus dados pessoais ou se utiliza essas informações de maneira responsável, aponta pesquisa feita pela OpenText. A média internacional é de 78%.

Além disso, “70% dos brasileiros não têm conhecimento nenhum ou têm apenas uma vaga ideia sobre o que essa lei trata” somados a 14,8% que confiam na forma como as organizações se utilizam e mantêm seus dados seguros (BOLZANI, 2016), demonstrando que há um longo caminho a percorrer não apenas na garantia de uma maior maturidade nas organizações, mas também e, principalmente, dos próprios titulares dos dados.

Diminuir a assimetria informacional e prover maiores níveis de transparência “no fim do dia, não é o tamanho da fonte em uma política de privacidade ou a inclusão de check-boxes nas configurações avançadas do navegador que legitimarão ou deslegitimarão o rastreamento do comportamento online do usuário.” (POLONETSKY; TENE, 2012, p. 285), especialmente quando se tratam se usuários com baixo nível de maturidade em relação a temas como educação digital e preocupação com privacidade e proteção de seus dados pessoais.

Se a Lei Geral de Proteção de Dados é uma legislação que tem por objetivo principal dar maior controle aos titulares quanto ao tratamento de seus dados pessoais, tal controle não deve se limitar ao aceite em termos, mas a um conhecimento mais profundo sobre o funcionamento de tecnologias e os reais impactos que apresentam.

3. Segurança da Informação e vulnerabilidades

Proteção de dados e segurança da informação caminham lado a lado. Por isso, para além de dispositivos legais, é necessário analisar quais riscos e vulnerabilidades podem advir dos pixels.

Um levantamento realizado pela Unisys para o Unisys Security Index (2020) mostrou que 75% dos brasileiros temem invasões cibernéticas. O estudo analisou 15 países, dentre os quais, o Brasil se mostrou o país com maior preocupação com o tema, tendo aumento significativo durante a pandemia da Covid-19. A maior preocupação foi segurança financeira (80%), seguida de segurança pessoal, segurança na internet e segurança nacional.

Acompanhando a evolução do levantamento, no ano seguinte o Brasil passou a ocupar o terceiro lugar do índice, no entanto, mesmo ocupando uma das primeiras posições, os usuários desconhecem as ameaças digitais que podem colocar em risco.

O design do Pixel impede qualquer bloqueio por parte do usuário ou validação quanto ao nível de segurança - se é enviado por uma fonte confiável -, de modo que pode ser utilizada de forma maliciosa por terceiros para obtenção de informações e explorar posteriormente vulnerabilidades.

Muitas vezes o Pixel é implementado a partir da imagem de uma assinatura de e-mail, por exemplo. A partir do momento em que o destinatário do e-mail abre a mensagem e, conseqüentemente, executa o pixel de rastreamento de um servidor, ele registra seu endereço de IP, que é como a internet sabe onde seu computador está tanto física quanto digitalmente. Além do IP, é possível também rastrear automaticamente o número de vezes que o destinatário abriu o e-mail, e a partir disso, entender quais linhas de assunto de e-mail determinada pessoa normalmente clica. Essa técnica é comumente utilizada por Spammers e Phishers para obter sucesso nas suas campanhas de e-mails maliciosos.

Observando essas práticas, o Google criou uma solução para os usuários do Gmail que consiste em redirecionar cada pedido de imagem através de seus próprios servidores. Assim, os pixels de rastreamento ainda saberão

quando o destinatário tiver lido um e-mail, mas não visualizarão sua localização ou obterão seu perfil comportamental porque não poderão ver seu IP (Eles veem o IP do Google).

Mapear dispositivos utilizados por um usuário ou organização, detectar o endereço IP, pessoas mais sujeitas a um golpe, arquitetura da rede incluindo sistemas utilizados, bem como rastrear suas atividades online (CHECKPOINT).

Uma maneira de impedir a execução da ferramenta não apenas no e-mail é pelo bloqueio do JavaScript. Recorrer a essa solução inviabilizaria o uso de aplicações importantes, que prejudicam a experiência do usuário, já que as páginas atualmente são muito mais interativas, compostas por textos, imagens, mapas e gráficos (ANONYMANIA, 2021).

Alguns dos principais fornecedores de pixels ensinam meios de bloquear o rastreamento, com adoção de extensões que mostrem ao usuário se está sendo rastreado, uso de navegadores que ofereçam funcionalidades de privacidade, uso de VPN para mascarar IP - deixando claro, inclusive, que essa medida não impedirá o rastreio por outros métodos além dos cookies, ou seja, não sendo efetivas para pixels.⁷

Ainda que adotadas as medidas recomendadas, não há qualquer garantia de não rastreamento, além de se manter as principais preocupações que deveriam estar no cerne do debate: ausência de transparência ao titular -aquele que não é profissional da área de privacidade e proteção de dados, segurança da informação ou que não possui conhecimento técnico para uma leitura aprofundada de código-, e que se utiliza diariamente da internet para desenvolver atividades pessoais ou profissionais sem o conhecimento de que está sendo constantemente rastreado por meio de uma tecnologia que não é capaz de visualizar.

4. The Digital Standard

O Digital Standard é um *framework open source* que avalia como as tecnologias respeitam interesses e necessidades do ponto de vista dos consumidores. Está disponível para ser utilizado por organizações, pesquisadores e times de produto, podendo ser inclusive um ponto de partida interessante à

7. "A VPN (Virtual Private Network), will hide your IP address from websites. This does not stop websites from tracking you through other methods (e.g. cookies, pixels, or fingerprinting), but it will stop your ISP (Internet service provider) from collecting data on the websites you browse." **Hojtjar**, op. cit.

criação de um framework de *privacy by design* para times de desenvolvimento. Sua divisão atualmente considera quatro quesitos: Segurança, Privacidade, Governança e Ownership (THE DIGITAL).

Uma vez que a análise desse artigo foca principalmente no desconhecimento do titular de dados quanto à adoção de pixels em comunicações eletrônicas e distribuição de anúncios no ambiente digital, foi feita uma breve seleção dos parâmetros propostos pelo *framework* que se relacionam à privacidade e proteção de dados.

Com foco nas seções de Privacidade e parte da seção de governança foi feita uma tradução livre do framework, o qual recomenda-se aplicação por times de produto, UX, desenvolvimento e privacidade.

Em razão da própria ausência de transparência dos principais fornecedores de pixels, optou-se por não analisar um caso concreto neste artigo e limitar-se à sugestão de aplicação do *framework*.

Tabela 1: Framework The Digital Standard

Área	Seção	Parâmetro
Privacidade (Is it private?)	Controle de Dados	Posso ver e controlar tudo que a ferramenta sabe sobre mim: <ul style="list-style-type: none"> • A definição de 'informações do usuário' inclui informações coletadas de terceiros. • Usuários podem controlar quais dados são coletados, a forma como suas informações são usadas para segmentar a publicidade. • Há clara explicação de como os usuários podem controlar se suas informações são usadas para publicidade direcionada. • Usuários podem, ainda, obter uma cópia de suas informações simples e sem custo. • Há explicação sobre quais informações o usuário pode obter e tal obtenção das suas informações ocorre por meio de Dados Estruturados. • Usuários podem obter todas as informações do usuário de revestimento público e privado que a empresa segura sobre eles.
		Posso ver e controlar tudo que a ferramenta sabe sobre mim: <ul style="list-style-type: none"> • Os controles de privacidade estão disponíveis na interface do usuário.
		Posso ver e controlar tudo que a ferramenta sabe sobre mim: <ul style="list-style-type: none"> • Os controles de privacidade na interface do usuário são efetivos.
	Uso e Compartilhamento de dados	O compartilhamento de dados é transparente e possui finalidades determinadas: <ul style="list-style-type: none"> • A ferramenta só compartilha informações com terceiros quando é razoavelmente necessário para fornecer serviço para usuários • A ferramenta divulga claramente quais dados são compartilhados e com quem. • A organização responsável pela ferramenta divulga claramente os tipos de terceiros com os quais compartilha informações do usuário. • A organização responsável pela ferramenta divulga claramente os nomes de terceiros com os quais compartilha informações do usuário. • A organização responsável pela ferramenta divulga claramente se ele compartilha informações do usuário com o governo ou as autoridades legais. • Terceiros relacionados à ferramenta são nomeados na política de privacidade.
		O uso de dados é consistente com o contexto da relação com o usuário e é transparente.
	Retenção e Descarte dos dados	A retenção dos dados ocorre apenas pelo tempo necessário e razoável para fornecer o serviço. <ul style="list-style-type: none"> • A empresa por conta própria descarta dados pessoais desatualizados e desnecessários, ou torna esses dados razoavelmente desidentificados (anonimização). • A empresa fornece períodos de retenção específicos para diferentes tipos de informações com escopo razoável para descarte de dados pessoais desatualizados e desnecessários.
		Eu posso excluir os dados que a empresa tem sobre mim que não são necessários para fornecer o Serviço.
		Minha conta e informações são excluídas quando deixo o serviço.
	Benefícios de dados	Cada dado pessoal que forneço me traz um benefício; Não apenas ajuda a empresa.
	Coleta de dados	Eu sei quais dados pessoais esta empresa está coletando e quando.
	Coleta de dados mínima.	O único dado pessoal que a empresa coleta sobre mim é o que é necessário para fazer o produto ou serviço funcionar corretamente.
	Privacy by default	As configurações padrão desta ferramenta prioriza minha privacidade; Para abrir mão da minha privacidade, na verdade, preciso alterar as configurações.

Governança & Compliance	Termos de Uso e Documentos da Política de Privacidade	Eu posso facilmente encontrar, ler e entender o aviso de privacidade ou os termos de uso.
Governança & Compliance	ToS & Privacy Policy change notification	A organização responsável pela ferramenta provê notificações para informar o titular quando altera sua política de privacidade ou altera seus termos de uso.
Governança & Compliance	Solicitações de terceiros para dados do usuário	A organização responsável pela ferramenta está em conformidade apenas com solicitações legais e éticas de terceiros para informações do usuário.
Governança & Compliance	Política de identidade	Eu posso me registrar usando apenas o nome e identificar características que desejo ou manter minha identidade completamente anônima.
Governança & Compliance	Notificação de ameaça	A empresa notifica as autoridades apropriadas e aquelas afetadas quando ocorre uma violação de dados.
Governança & Compliance	Relatórios de transparência	A empresa é transparente sobre suas práticas para compartilhar dados do titular com o governo e outros terceiros.
Governança & Compliance	Notificação do usuário sobre solicitações de terceiros para informações do usuário	A empresa me diz se o governo ou outros terceiros pedirem minhas informações.

Fonte: tradução livre

Apesar de não ser possível localizar informações detalhadas sobre os principais *pixels* disponíveis no mercado, por uma breve análise é possível verificar a ausência de iniciativas/medidas que concederiam aos titulares maior controle sobre os seus dados pessoais. A inexistência de informações claras, somada à impossibilidade de requerer por meio de um canal os direitos trazidos pela LGPD e o próprio desenho da ferramenta, que dificulta a adição de controles efetivos na interface do usuário são alguns dos desafios a serem enfrentados na defesa do uso dos *pixels*.

Considerações finais

Em que pese o foco atualmente recaia sobre os cookies, foi possível verificar que existem outras tecnologias - sendo os *pixels* apenas uma delas - que oferecem maiores riscos à privacidade e que são pouco exploradas.

O debate em torno dessas ferramentas não deve se limitar a como oferecer maiores controles aos titulares, tampouco ao acréscimo de seções específicas em avisos de privacidade para informar de maneira genérica sobre seu uso.

É necessário não apenas debater os limites deste tipo de coleta de dados, como também investir na educação de um público que começa a se familiarizar com conceitos relacionados à internet, à segurança dentro deste ambiente

e a uma consciência quanto ao que deve ser considerado um uso adequado dos seus dados pessoais por terceiros.

Há uma dificuldade peculiar em como se proteger do rastreamento por pixels, dado que no momento atual se utilizar de um ambiente digital sem imagens e outros elementos por bloqueio da execução do JavaScript não é uma solução razoável tanto técnica quanto operacionalmente. A melhor solução para melhor proteger os dados de titulares não deve ser tão inacessível.

Por isso, se sugere a aplicação do framework para analisar melhor o funcionamento atual deste tipo de tecnologia e o convite para contribuir com a evolução do Digital Standard, uma vez que está aberto ao uso e à contribuição.

Referências

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BOLZANI, Isabela. 84% dos brasileiros nunca checaram como empresas usam seus dados pessoais, diz pesquisa. 3/02/2021. **Folha de S. Paulo**. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/02/84-dos-brasileiros-nunca-checaram-se-seus-dados-sao-usados-de-maneira-responsavel.shtml> Acesso em: 08 jan. 2022.

BRASIL. Lei nº 13709, de 14 de agosto de 2018. DISPÕE SOBRE A PROTEÇÃO DE DADOS PESSOAIS E ALTERA A LEI Nº 12.965, DE 23 DE ABRIL DE 2014 (MARCO CIVIL DA INTERNET). **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jan. 2022.

BUILDING a more private web: A path towards making third party cookies obsolete. A path towards making third party cookies obsolete. 14/01/2020. **Chromium blog**. Disponível em: <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>. Acesso em: 09 jan. 2022.

CANALTECH. **Quais foram os navegadores mais usados em 2021**. 26/12/2021. Disponível em: <https://canaltech.com.br/navegadores/quais-foram-os-navegadores-mais-usados-em-2021/#:~:text=Conclus%C3%A3o,usada%20nesse%20segmento%20de%20aparelhos> Acesso em: 15 abr. 2022.

ENGLEHARDT, Steven et al. I never signed up for this!: Privacy implications of email tracking. **Proceedings on Privacy Enhancing Technologies**, 2018. Disponível em: https://www.ftc.gov/system/files/documents/public_comments/2017/11/00054-141912.pdf Acesso em: 08 jan. 2022.

FERNANDES, Maria Luiza. SUNDFELD, Philippe. LGPD e UX: um equilíbrio para o consentimento. 16/07/2021. **Jota** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-ux-um-equilibrio-para-o-consentimento-16072021> Acesso em: 08 jan. 2022.

IAB BRASIL. **Um guia para a era pós-cookies de terceiros.** novembro 2021, p. 13. Disponível em: <https://iabbrasil.com.br/wp-content/uploads/2021/11/guia-para-era-sem-cookies-final-V2.pdf>. Acesso em: 04 dez. 2021.

JANG, Dongseok et al. **An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications.** Disponível em: https://www.researchgate.net/profile/Dongseok-Jang/publication/221609722_An_Empirical_Study_of_Privacy-Violating_Information_Flows_in_JavaScript_Web_Applications/links/00463517e8448c91dd000000/An-Empirical-Study-of-Privacy-Violating-Information-Flows-in-JavaScript-Web-Applications.pdf Acesso em: 08 jan. 2022.

KELION, Leo. “Spy pixels in emails have become endemic”. 17/02/2021. **BBC.** Disponível em: <https://www.bbc.com/news/technology-56071437> Acesso em: 07 jan. 2022.

MOZZILA. **Uma visão geral do HTTP.** Disponível em: <https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Overview>. Acesso em: 08 jan. 2022.

NOBREGA, Cristiano. **O fim dos cookies third-party:** tudo que você precisa saber neste momento. tudo que você precisa saber neste momento. 23/04/2021. IAB Brasil. Disponível em: <https://iabbrasil.com.br/artigo-o-fim-dos-cookies-third-party-tudo-que-voce-precisa-saber-neste-momento/>. Acesso em: 29 nov. 2021.

PALHARES, Felipe. Cookies: Contornos atuais. In: Felipe Palhares (Coord.) **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters, 2020.

PETERSON, Ralph. The Pros and Cons of Disabling JavaScript on Your Browser. 27/05/2021. **Anonymania.** Disponível em: <https://anonymania.com/disabling-javascript-browser-cons-pros/> Acesso em: 08 jan. 2021.

PIXEL Tracking: a Hacker’s tool. **Checkpoint.** Disponível em: <https://blog.checkpoint.com/2016/09/08/pixel-tracking-a-hackers-tool/> Acesso em: 08 jan. 2021.

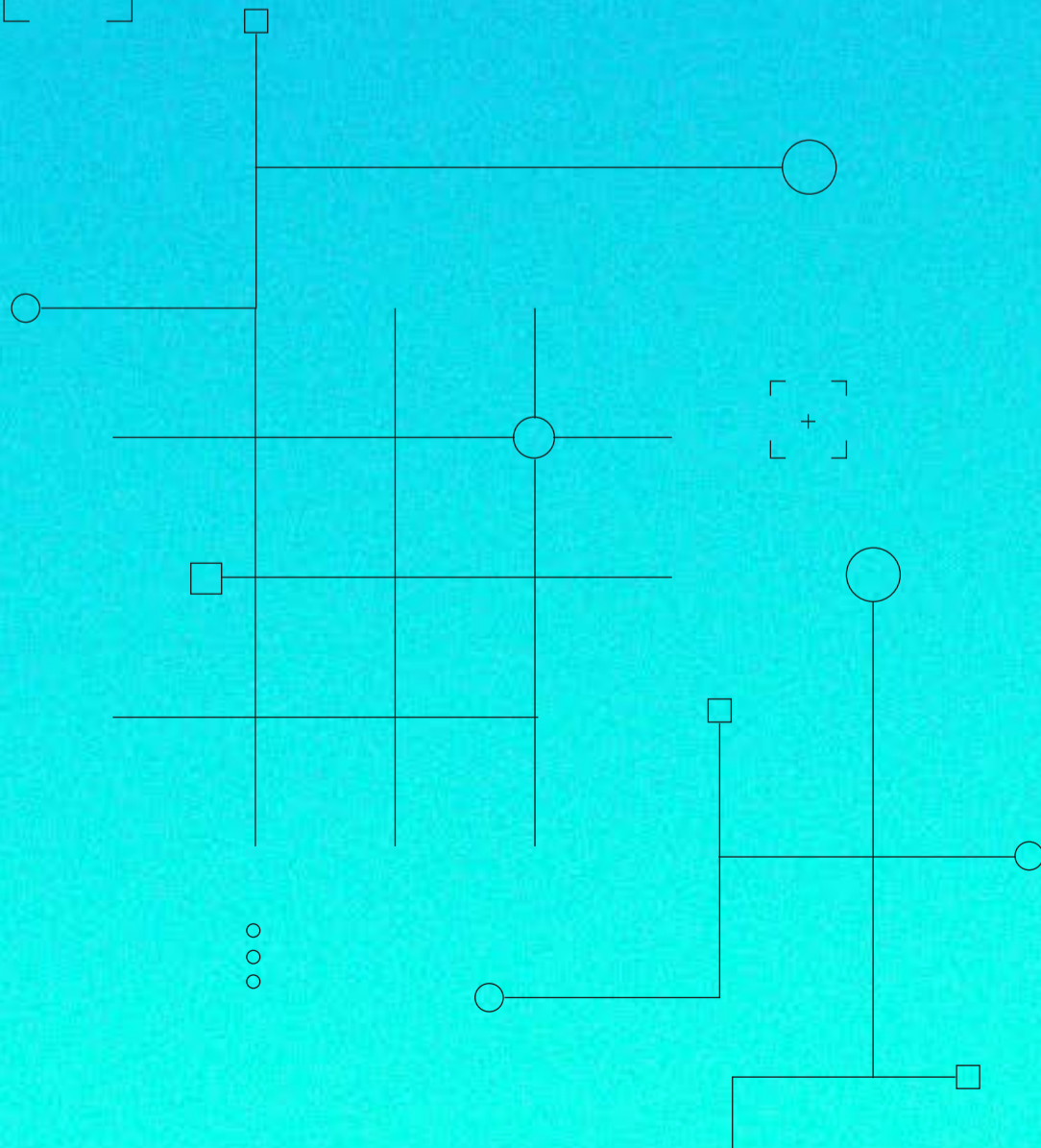
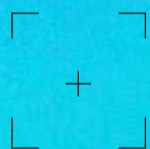
POLONETSKY, Jules; TENE, Omer. **To track or do not track:** advancing transparency and individual control in online behavioral advertising. 2012. Disponível em: https://iapp.org/media/pdf/knowledge_center/Tene_to_track_or_do_not_track.pdf. Acesso em: 10 jan. 2022.

UNYSIS. 2020 **Unisys Security Index**: global edition. 2020. Disponível em: <https://www.unisys.com/siteassets/microsites/unisys-security-index-2020/unisyssecurityindexreport2020.pdf> Acesso em: 08 jan. 2020.

WEBSITE tracking guide. 22/09/2021. **Hotjar**. Disponível em: <https://www.hotjar.com/website-tracking/#what-is-website-tracking>. Acesso em: 08 jan. 2022.

O atendimento dos direitos dos titulares dos dados pessoais: o case do TJSC com o aplicativo LGPDjus

DENISE DE SOUZA LUIZ FRANCOSKI



Sumário: Introdução. 1 Os direitos dos titulares dos dados pessoais constantes na LGPD. 2. Formas e prazos para as requisições propostas pelos titulares. 3 O papel do Encarregado na gestão do atendimento das solicitações apresentadas pelos requisitantes. 4. A necessidade de autenticação do titular do dado pessoal para o atendimento de suas solicitações. 5. O case do TJSC com o aplicativo LGPDjus. 6. A importância do painel de gerenciamento interno do Encarregado no LGPDjus para o controle efetivo dos fluxos das requisições dos titulares. Considerações finais. Referências.

Introdução

A Lei Geral de Proteção de Dados Pessoais-LGPD inaugurou no meio jurídico brasileiro, a necessidade de se promover uma nova cultura de proteção de dados pessoais e privacidade, empoderando sobremaneira a pessoa o titular do dado pessoal quanto aos direitos por ela estabelecidos.

Dentro desta vertente, temos que o presente artigo objetiva inicialmente, apresentar os direitos dos titulares dos dados pessoais, constantes no artigo 18 e seus incisos, bem como, as formas e os prazos para o atendimento das requisições que forem por eles apresentadas.

Em seguida, será referido qual deve ser o papel do Encarregado na gestão do atendimento das respectivas solicitações, além de focar de maneira pontual, a importância da autenticação da pessoa do titular do dado pessoal, que possa refletir em uma identificação segura, quando o Encarregado tiver que responder tais pedidos na organização em que esteja atuando.

Logo após, será apresentado o case do TJSC, quanto a adoção do aplicativo LGPDjus, com enfoque nas premissas de segurança versus inclusão, no atendimento do titular, quando esse estiver exercitando os direitos que estão disciplinados na legislação protetiva.

1. FORMAÇÃO ACADÊMICA - Pós-graduanda em Direito Digital pela UERJ/ITS (2021-II/2022-II). Mestre em Ciência Política e Jurídica pela Universidade do Vale do Itajaí - UNIVALI (2002/2004). Mestre em Relações Internacionais pela Universidade do Sul de Santa Catarina - UNISUL (1999/2001). Especialista em Direito Econômico Europeu pela Europa University Lisboa (1997). Especialista em Administração Pública e Sociedade pela Universidade do Estado de Santa Catarina - UDESC (1997). Pós-graduada pela Escola da Magistratura Catarinense, na 2ª Turma (1987-1988). Bacharel em Direito pela Universidade Federal de Santa Catarina (1980-1985). FORMAÇÃO PROFISSIONAL - Atualmente, é Desembargadora no Tribunal de Justiça de Santa Catarina - TJSC e integrante da 5ª Câmara de Direito Público. Coordenadora do Comitê Gestor de Proteção de Dados - CGPD (TJSC), desde a sua criação em 2018 (com recondução ao biênio 2019/2021). Encarregada pelo Tratamento de Dados Pessoais do Poder Judiciário de Santa Catarina. Membro do Grupo de Trabalho destinado à elaboração de estudos e de propostas voltadas à adequação dos tribunais à Lei Geral de Proteção de Dados, do Conselho Nacional de Justiça - CNJ. Compôs o Conselho da Magistratura e o Comitê de Organização de Divisão e Organização Judiciárias (TJSC) no biênio 2018/2019.

Ao final, pretende-se ainda explicar de que maneira funciona o painel interno do LGPDjus, pontuando sua importância, e como ele possibilita imprimir agilidade e segurança, para a gestão das requisições dos titulares, ao Encarregado, quando esse estiver no exercício efetivo de suas funções junto à Corte Catarinense, resultando em um atendimento eficiente e dentro dos prazos legais, esperando-se que em breve o aplicativo venha a ser utilizado por muitas outras organizações.

1. Os direitos dos titulares dos dados pessoais constantes na LGPD

No contexto da Lei Geral de Proteção de Dados-LGPD (BRASIL, 2018), encontramos no capítulo III, artigos 17 a 22, as disposições relativas aos direitos dos titulares dos dados pessoais, especialmente aqueles que estão descritos de forma ordenada no artigo 18 incisos I a IX, estando esses direitos baseados principalmente no conceito de autodeterminação informativa², que nada mais é do que o direito que o indivíduo tem de saber como seus dados pessoais estão sendo tratados dentro das organizações.

Assim, temos que é nos incisos do artigo 18 que efetivamente encontramos os direitos dos titulares dos dados pessoais em um rol claramente exemplificativo, sendo decorrência de inspiração evidente do Regulamento Europeu –GDPR³, influência essa que podemos visualizar em vários aspectos da legislação brasileira, salientando, entretanto, que a lei nacional seguiu um rumo próprio em seus dispositivos.

Todavia, convém ressaltar que nos capítulos I e II da LGPD, também encontramos referências a outros direitos, tais como: direito à liberdade – art. 1º., liberdade de expressão, de informação, de comunicação e de opinião – art. 2º., livre desenvolvimento da personalidade – art. 1º. e 2º., autodeterminação informativa, honra, imagem, direitos do consumidor, direito à cidadania dentre outros.

É relevante, também mencionar, que os direitos constantes nos incisos dos artigos 18 da LGPD, são decorrentes de forma direta da sua principiologia, que vem reproduzida no artigo sexto e seu incisos, sendo que a partir do arti-

2. Autodeterminação informativa: é o poder que cada cidadão tem sobre os seus próprios dados pessoais. Nota da autora

3. [RGPD \(GDPR\) -Regulamento Geral sobre a Proteção de Dados \(gdprinfo.eu\)](https://gdprinfo.eu) Acesso em 30.11.2021.

go sétimo até o artigo dezesseis, outros diversos conteúdos cuidam também da temática dos direitos dos titulares, como por exemplo: quando a lei faz referência a revogação do consentimento, do direito do titular do dado de ser informado pela utilização de seus dados pessoais pela administração, e ainda, direito a transparência do tratamento de dados que tenha por base o legítimo interesse do controlador.

Entretanto, percebe-se que a dinâmica dos direitos dos titulares dos dados pessoais dispostos na legislação protetiva deve ser entendida e interpretada conjuntamente com outros dispositivos de seu contexto, como tão bem se posiciona a advogada Ana Frazão (FRANCOSKI, 2021. p.578-579) quando diz:

Somente com a visão conjunta e sistemática da LGPD é que se pode compreender a exata dimensão do seu Capítulo III, que, ao tratar dos direitos dos titulares, retoma uma série de precisões e de conceitos já estabelecidos inicialmente, tal como será mais bem explorado no próximo artigo desta série.

Dentro da esfera de análise dos incisos descritos no artigo 18 da LGPD, podemos dizer então, que o titular do dado pessoal de acordo com esse artigo consegue exercitar os seguintes direitos, tais como:

Direito de confirmação da existência de tratamento – Art. 18. Inciso I: o titular poderá obter informações precisas sobre a existência de tratamento de seus dados pessoais, em qualquer espécie de instituição pública ou privada.

Direito de acesso – Art. 18. Inciso II: O titular aqui terá condições de ter acesso aos seus dados pessoais, podendo obter do controlador, informações amplas e completas a respeito deles. Em sua resposta caberá ao controlador mencionar a origem de seus dados pessoais, quais foram as entidades receptoras, e qual foi o objetivo que fora considerado para o seu armazenamento.

Direitos à correção de seus dados – Art. 18. Inciso III: o titular poderá invocar este direito, quando seus dados estiverem incompletos, inexatos ou mesmo desatualizados, tendo o mesmo, relação direta ao princípio da qualidade dos dados (BRASIL, 2018)⁴, referido no artigo sexto, inciso quinto da LGPD.

Direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos, ou tratados contrariamente aos dispositivos da LGPD – Art. 18, inciso IV: em todos os casos citados no presente inciso, caberá ao titular exer-

4. V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/ccivil_03/leis/2018/05/lei13709-2018.html) Acesso em 30.11.2021.

cer esse direito assim que puder verificar as condições desfavoráveis e que estão citadas no corpo do inciso IV, frisando apenas que o bloqueio é medida de caráter temporário, ao contrário da eliminação que é de forma definitiva, devendo esta última também ser aplicada quando houver finalização do tratamento dos dados pessoais do titular.

Direito à portabilidade – Art. 18, inciso V: o titular tem o direito, mediante requisição expressa, de requerer a portabilidade de seus dados pessoais, ou seja, a transposição de suas informações pessoais, para qualquer outra empresa ou órgão público de sua escolha ou preferência, cabendo à Autoridade Nacional de Proteção de Dados-ANPD (BRASIL, 2018) regulamentar os procedimentos adequados para a sua efetivação.

Direito à eliminação de dados pessoais tratados com o consentimento do titular – Art. 18, inciso VI: nesse caso caberá ao titular requerer esse direito através de requerimento expresso dirigido aos agentes de tratamento, ou seja, controlador e/ou operador. Ao agente de tratamento caberá atender de forma imediata o pedido do titular, podendo, todavia, tomar as providências mencionadas no parágrafo quarto do artigo 18, caso haja impossibilidade de atender a demanda, informando que não é o agente de tratamento responsável, mas devendo informar quem o seja, ou ainda, fazer constar quais seriam as razões de fato ou de direito que justifiquem o seu impedimento em cumprir o pedido.

Direito de informação das entidades públicas ou privadas com as quais o controlador tenha feito uso de compartilhamento de dados pessoais do titular – Art. 18, inciso VII: aqui verifica-se de forma imediata a intervenção do princípio da transparência contido no artigo 6º. Inciso VI (BRASIL, 2018)⁵ da lei protetiva, onde ao titular do dado pessoal tem o direito de obter informações claras, precisas e de acesso facilitado, sobre a existência ou não da realização de tratamento dos seus dados pessoais, e quais foram os agentes de tratamento responsáveis, lembrando que aqui devem ficar preservados os segredos comerciais e industriais.

Direito do titular de ter informações sobre a possibilidade de não fornecer o seu consentimento – Art. 18, inciso VIII: caberá aqui aos agentes de tratamento o dever de informar ao titular do dado, que ele poderá não conceder o seu consentimento para o referido tratamento, devendo ser alertado das con-

5. VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/ccivil_03/leis/2018/05/lei_13709-2018.html) Acesso em 30.11.2021.

sequências de sua negativa, possibilitando a ele avaliar qual seria a melhor decisão a respeito do tratamento de suas informações pessoais.

Direito à revogação do consentimento- Art. 18, inciso IX: seguindo o que vem descrito no § 5º. do art. 8º. (BRASIL, 2018)⁶ da lei geral de proteção de dados, o titular poderá a qualquer momento revogar o seu consentimento, desde que o faça através de manifestação expressa, com procedimento sem custos e de forma facilitada, devendo ser ratificado todos os tratamentos anteriormente realizados, enquanto não ocorrer por parte do titular requerimento expresso para a sua eliminação.

No artigo 18 § 1º., visualizamos que o titular do dado pessoal tem o direito de peticionar sobre eles perante a Autoridade Nacional de Proteção de Dados-ANPD, além de poder se dirigir perante os organismos de defesa do consumidor (art.18 § 8º). Em seguida o § 2º., informa que o titular do dado pessoal tem direito a oposição ao tratamento de dados que for realizado com fundamento em uma das hipóteses de dispensa de consentimento, quando ocorrer o descumprimento da lei protetiva. Por fim, no § 3º, encontramos a forma pela qual o titular do dado pessoal poderá exercitar os seus direitos perante o agente de tratamento, deixando claro que isso deverá ocorrer através de requerimento expresso do titular, ou de seu representante legal devidamente constituído.

Após esta breve apresentação dos direitos dos titulares dos dados pessoais, seguiremos esse estudo, analisando as formas e prazos de resposta para as requisições propostas por eles, examinando posteriormente todos os desdobramentos que o exercício desses direitos poderá causar junto aos projetos de gestão e *compliance*⁷ de todas as organizações, quer sejam órgãos públicos ou empresas da iniciativa privada.

6. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. [L13709 \(planalto.gov.br\)](https://planalto.gov.br) Acesso em 30.11.2021.

7. *Compliance* vem o verbo em inglês “*to comply*”, que significa agir de acordo com uma ordem ou um conjunto de regras, sendo que a conformidade com tais regramentos se refere a expressão “estar em *compliance*”. Nota da autora.

2. Formas e prazos para as requisições propostas pelos titulares dos dados pessoais.

No primeiro item deste estudo, já fizemos referência que o titular do dado pessoal no momento do exercício de qualquer um dos seus direitos referidos na LGPD, poderá fazê-lo através de requerimento expresso, pessoalmente ou através de representante legal, perante o agente de tratamento (BRASIL, 2018)⁸envolvido, segundo a premissa constante no artigo 18 §3º., da legislação aqui em evidência.

Logo após, vê-se que o comando inserido no artigo 18 § 4º da LGPD, deixa claro, que nas hipóteses em que o controlador (BRASIL, 2018)⁹ não tiver condições de atender o titular do dado de forma imediata, deverá responder o pedido alegando: que não é o agente de tratamento daqueles dados, indicando quem for se possível, ou indicar as razões de fato ou de direito que o impedem o atendimento imediato do requerimento, informando-se, desde já, que o titular do dado deverá ser atendido sem cobrança de qualquer custo (art.18 § 5º), asseverando entretanto, que esta última afirmativa não é absoluta, pois quando tais requisições forem feitas, por exemplo, perante as serventias extrajudiciais, estas em razão de normativas específicas (BRASIL, 1994), ficam autorizadas a cobrarem os respectivos emolumentos constantes em suas tabelas de serviços, não estando portanto, vinculadas aos preceitos da LGPD, questão esta que certamente em futuro próximo merecerá um debate mais detalhado.

Pela leitura do contexto do artigo 19 da lei protetiva podemos concluir, que apresentada a requisição pelo titular do dado pessoal ao controlador da organização, este poderá responder de duas formas:

1. Em formato simplificado e imediatamente, quando por exemplo, a resposta for apenas sim ou não para a indicação de existência ou não de dados pessoais naquela organização.
2. No prazo de 15 dias, quando houver necessidade de uma explicação mais detalhada sobre o pedido do titular, a qual deverá ocorrer por meio de declaração clara e completa, contendo essencialmente, a origem dos da-

8. X - Art. 5º Para os fins desta Lei, considera-se: agentes de tratamento: o controlador e o operador; [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/legis/l13709.htm) Acesso em 30.11.2021.

9. Art. 5º Para os fins desta Lei, considera-se: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/legis/l13709.htm) Acesso em 30.11.2021.

dos pessoais, ou sua inexistência dentro da organização, os critérios que foram utilizados para o tratamento dos dados pessoais, bem como, para qual finalidade o tratamento foi efetivamente realizado, importando dizer, que sempre será esperado que o controlador forneça alguma resposta ao titular do dado pessoal, objetivando que este último nunca fique sem nenhum *feedback*,¹⁰ como determinada a LGPD.

Com relação aos prazos estipulados pela lei, para resposta ao titular do dado pessoal, por parte do controlador, ou seja, de forma imediata ou em 15 dias, convém sublinhar, que por vezes, em razão do volume de dados pessoais que estão armazenados nas organizações, tais prazos não poderão ser devidamente cumpridos no prazo determinado. Para a solução dessa problemática, espera-se que a ANPD, utilize das prerrogativas referidas no § 4º do art. 19¹¹ da LGPD (BRASIL, 2018), e conceda uma flexibilização dos prazos a determinadas instituições.

Sobre este assunto, convém transcrever a opinião de Daniel Becker e Roberta de Brito Rodrigues, quando assim mencionam:

Não é preciso dizer que a obrigação pode se tornar por vezes inexecutável ou extremamente onerosa para os agentes de tratamento de dados por conta do exíguo prazo. Por esta razão, há uma disposição no § 4º., que excepciona o cumprimento dos referidos prazos a depender de determinação da autoridade nacional que criará regras para os setores, criando prazos factíveis. É curioso destacar que o GDPR, em seus artigos 12º., 14º., e 15º., não cria prazos para o fornecimento das informações; apenas há menção ao prazo de um mês para o prosseguimento do pedido, deixando a questão do prazo como cláusula aberta para regulamentação posterior (FEIGELSON; SIQUEIRA, 2019. p.126).

Segundo o comando do § 1º. do artigo 19 a LGPD (BRASIL, 2018)¹², as organizações deverão armazenar os dados pessoais em formato que venha a favorecer o pleno exercício de acesso por parte dos titulares dos dados pessoais,

10. *Feedback*: palavra de origem inglesa, que na tradução literal significa uma forma de avaliação ou comentário ou uma maneira de expor uma opinião a respeito de uma tarefa que fora realizada. Nota da autora.

11. Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: § 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos. [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/ccivil_03/_ato2018-2019/2018_012/L13709.htm) Acesso em 30.11.2021.

12. Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/ccivil_03/_ato2018-2019/2018_012/L13709.htm) Acesso em 30.11.2021.

alertando a norma em seu § 2º. do citado artigo, que ficará a critério do titular a forma pela qual as suas informações poderão ser fornecidas pelo controlador, podendo solicitá-las por meio eletrônico seguro e idôneo ou através de documento impresso.

Na sequência, no art. 19 § 3º., é mencionado que, quando o tratamento dos dados pessoais do titular tiver origem no seu consentimento, ou em razão da existência de contrato, o requerente poderá solicitar ao controlador cópia eletrônica integral dos seus dados pessoais coletados, observados os segredos comercial e industrial, ficando a cargo da ANPD a devida regulamentação, de modo que o titular possa fazer sua utilização subsequente, inclusive em outras operações de tratamento.

Cabe ainda aqui por fim, um breve comentário sobre o conteúdo existente no artigo 20 da LGPD e seus parágrafos (§ 1º. e 2º.) (BRASIL, 2019)¹³, que trata do direito que o titular do dado tem em solicitar a revisão de decisões que forem tomadas unicamente com base em tratamento automatizado de dados pessoais, que afetem seus interesses, incluindo-se as decisões que possam definir seu perfil pessoal, profissional, de consumo, de crédito ou de aspectos que envolvam sua personalidade, sendo que nesses casos o controlador tem a responsabilidade de prestar as devidas informações, sobre os critérios e procedimentos que foram utilizados para a decisão automatizada, observados, mais uma vez, os segredos comercial e industrial.

3. O papel do Encarregado na gestão do atendimento das solicitações apresentadas pelos titulares dos dados pessoais

A figura do Encarregado vem definida na LGPD no art. 5º. Inciso VIII, como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a ANPD, sendo

13. Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. ([Redação dada pela Lei nº 13.853, de 2019](#)) Acesso em 30.11.2021

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. [Lei 13709 \(planalto.gov.br\)](#) Acesso em 30.11.2021.

que é no artigo 41 § 2º. que suas atribuições e ou atividades vêm especificadas da seguinte forma:

Cabe ao Encarregado aceitar as requisições, reclamações e ou comunicações dos titulares dos dados pessoais, prestando a eles os devidos esclarecimentos, além de adotar as respectivas providências.

Deve receber todas as comunicações que forem expedidas pela autoridade nacional, adotando da mesma forma os devidos encaminhamentos.

O Encarregado também deve orientar todos os membros da organização a respeito de todas as boas práticas que forem sendo tomadas dentro do programa geral de implementação da LGPD na respectiva instituição.

Além disso, deve estar habilitado a executar todas as demais atividades que forem determinadas pelo controlador, ou que venham a ser estabelecidas em normas complementares.

No artigo 41 § 3º. (BRASIL, 2018)¹⁴, encontramos a disposição na qual ficou deliberado, que caberá à ANPD estabelecer outras normas complementares sobre a definição e as respectivas atribuições da figura do Encarregado, incluindo as hipóteses da real necessidade de sua indicação, a depender da natureza, o porte da organização ou mesmo do volume de operações de tratamento de dados pessoais por elas realizadas.

O Encarregado por ser uma função absolutamente nova em nosso mundo jurídico, deve ter uma dedicação para o estudo permanente, não somente na LGPD, mas de toda a legislação setorial nacional e internacional, precisando além disso, de todo o apoio disponível das organizações, quer seja no seu aspecto de estrutura física, ou ainda, de constituição de um grupo de apoio técnico que possa lhe ajudar no cumprimento de todas as suas atribuições.

Convém, aqui registrar o comentário de Rony Vainzof:

Para conseguir exercer esse papel, é fundamental que o DPO tenha um foco cirúrgico e inquebrantável em todos os dez princípios da LGPD, previstos no art. 6º. da Lei (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de

14. Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. [L13709 \(planalto.gov.br\)](https://www.planalto.gov.br/legis/2018/5/lei/l13709.htm) Acesso em 30.11.2021.

contas), avaliando e monitorando se todas as atividades de tratamento existentes estão de acordo com os referidos princípios (OPICE BLUM; VAINZOF; MORAES, 2020. p.35)

De todo o contexto de suas atividades, temos que a gestão do atendimento das solicitações apresentadas pelos titulares dos dados pessoais poderia ser classificada como umas das mais importantes funções por ele exercida nas organizações públicas e/ou privadas. Isso porque, a depender da falta de cumprimento de qualquer requisição apresentada pelo titular do dado pessoal, poderá gerar aplicação de qualquer uma das sanções constantes no artigo 52 e seus incisos da legislação protetiva.

Na gestão dessa atividade específica, caberá ao Encarregado e sua equipe a princípio, formatar um modelo adequado de formulário eletrônico (FRANCOSKI, 2021. p. 81-82) ou físico, para utilização dos titulares dos dados pessoais quando estiverem no exercício de seus direitos previstos na LGPD, sendo que, além disso, deverão elaborar todos os fluxos (FRANCOSKI, 2021. p.80-81) possíveis que este referido documento percorrerá dentro da estrutura da organização envolvida. Feito isto, será preciso analisar se o canal escolhido pela organização, para recebimento das requisições dos titulares dos dados, tenha condições de autenticá-las de forma segura, de maneira que as informações constantes nas respostas sejam entregues a quem verdadeiramente as requisitou, e não a terceira pessoa.

É neste aspecto, que o Encarregado e sua equipe deverão dedicar fundamental atenção, pois qualquer entrega indevida de informações a pessoa que não seja o titular do dado pessoal, pode ocasionar não somente aplicação de sanções, como já foi dito anteriormente, mas também porque, tal situação poderá ser capaz de abalar a imagem reputacional da instituição em evidência, valendo aqui citar a observação de Rony Vainzof quando menciona que: “A estrutura operacional para dar vazão ao atendimento dos requerimentos deverá ser proporcional ao porte da organização, às atividades de tratamento, à criticidade dos dados tratados e à sua atividade principal” (OPICE BLUM; VAINZOF; MORAES, 2020. p.49)

Por isso, será necessário que o Encarregado desde logo utilize uma metodologia adequada para classificação do nível de criticidade e complexidade de cada pedido, definindo de acordo com esta análise, se tais requisições deverão ser administradas por um ser humano, por meio automatizado, ou ainda, através de um meio híbrido (humano/automatizado), sendo importante destacar, que o Encarregado no momento que tiver que escolher qual o meio de

autenticação mais adequado à sua organização, deverá prestar atenção para não coletar no ato da autenticação, mais dados pessoais daqueles que já são tratados em seus diversos sistemas.

Considerando-se o porte da organização, o volume de dados pessoais nela existente, às espécies de tratamento imprimida e a criticidade dos dados tratados, é quase certo que o Encarregado precisará dispor de uma ferramenta tecnológica adequada para fazer todo o gerenciamento das requisições dos titulares dos dados pessoais, quando estiverem no exercício de seus direitos, exercendo aquele um papel central e fundamental para o bom e apropriado atendimento de todos esses pedidos, devendo está a temática ser analisada nos próximos itens desse estudo.

4. A necessidade de autenticação do titular do dado pessoal para o atendimento de suas solicitações

O significado da palavra autenticação, pode ser explicado pelo ato de confirmar, validar ou reconhecer que algo ou alguém é autêntico, ou seja, é uma garantia de que qualquer alegação sobre algum objeto, ou a respeito de uma determinada pessoa é essencialmente verdadeira.

De outro lado, a requisição dos direitos constantes no artigo 18 da LGPD, por parte dos titulares dos dados pessoais, pode ser definida como uma solicitação que uma pessoa natural faz a uma organização, visando saber quais dados sobre ela foi coletado, para qual finalidade ele será utilizado, dentre outras opções.

Este talvez seja um dos evidentes exemplos do empoderamento da pessoa do titular do dado pessoal concedidos na legislação protetiva, a ponto de causar um impacto muito grande nas mais diversas instituições do setor público ou privado, que terão necessariamente, e por consequência, que atuarem de forma proativa na criação de metodologias adequadas para atendimento desse novo canal de requisições concedido a cada um dos titulares de dados pessoais, além de efetivar a nomeação de um Encarregado, que será o gestor e garantidor da resposta adequada a cada uma dessas solicitações.

Muito embora, não esteja escrito expressamente, em nenhum dos sessenta e cinco artigos da Lei Geral de Proteção de Dados Pessoais, que a pessoa do titular do dado pessoal quando estiver no exercício de seus direitos, deve ser autenticada, por qualquer meio, já é possível neste instante mencionar que tal procedimento é absolutamente indispensável, não somente para que o Encarregado possa responder todos os pleitos com segurança, mais principal-

mente para que a organização, quer seja pública ou privada, não tenha uma exposição negativa a ponto de se tornar alvo de aplicação de qualquer tipo de sancionamento.

A boa prática aqui denominada de autenticação do titular do dado pessoal deve ser implementada pelas organizações de maneira imediata, logo após a definição do canal de recebimento das requisições e do desenho dos fluxos para tal atendimento.

Outra questão a ser aqui analisada, diz respeito ao momento em que se deve fazer a opção pela metodologia de autenticação do titular do dado pessoal, cabendo ao Encarregado examinar se tal método está de acordo com a principiologia do artigo 6º. da LGPD, especialmente, no que se refere aos princípios da necessidade e da adequação, bem como, deve ele manter atualizado o procedimento de autenticação de acordo com a evolução natural da tecnologia, se optar por uma de suas ferramentas.

Além disso, será preciso delimitar quando se deve iniciar a contagem dos prazos estipulados pela LGPD, para o atendimento das referidas requisições, no caso em que a organização tenha escolhido alguma metodologia específica de autenticação, a qual poderá ser feita por um ser humano ou até mesmo através de uma ferramenta de inteligência artificial. Nesses casos será mais garantido para a organização, que a resposta da requisição do titular somente deva ocorrer após a confirmação da real identidade do requerente, a fim de evitar desperdício de tempo e recursos com pedidos duvidosos ou inadequados.

A utilização pela organização, de qualquer outro canal de atendimento para as solicitações do titular do dado pessoal, que não siga os parâmetros de um procedimento de autenticação segura, poderá gerar facilmente um considerável número de incidentes de segurança, culminando conforme o caso, até em um grande vazamento de informações com pessoas estranhas ao titular.

Por isso, é absolutamente necessário que o Encarregado e sua equipe se preocupem com esta questão já no início do processo geral de implementação da LGPD, sensibilizando a toda administração *from de top*¹⁵, da importância de se fazer investimento em tecnologia atual e avançada, demonstrando que isso na realidade não será apenas mais um ônus, mas na verdade se constituirá em verdadeiro bônus/investimento em futuro bem próximo, pois somente

15. A expressão “*from the top*” se refere neste trabalho a alta direção, a alta cúpula e a alta administração. Nota da autora.

assim a instituição estará devidamente preparada para a implementação da lei de forma adequada, evitando desta forma também, exposição negativa de todos os seus membros

Outra questão pertinente a ser ressaltada, foi que em pesquisas realizadas pela Encarregada do TJSC e seu grupo em 2020, junto ao Clube de Dirigentes Lojista-CDL¹⁶ local, somente para exemplificar, foi detectado que no cardápio de assinaturas digitais à época, os preços encontrados para aquisição de assinatura digital, eram de valores elevados, concluindo-se portanto, que se tal opção fosse escolhida e viesse a ser adotada pelo referido Tribunal, certamente estaria deixando de fora, quanto ao exercício dos direitos da LGPD, um número considerável de pessoas pertencentes a camada de baixa renda, ou mesmo aqueles que vivem abaixo da linha da pobreza, e que não dispõem sequer de numerário suficiente para uma sobrevivência digna, quanto mais para aquisição de uma assinatura digital específica.

Seguindo todos os argumentos até aqui apresentados, iremos demonstrar no próximo item desse artigo, que o Tribunal de Justiça de Santa Catarina, através do Grupo de Trabalho Técnico e da Encarregada, compartilharam desde o momento inicial da formatação do Programa Geral de Implementação da LGPD, principalmente quando da escrita do seu *Road Map*¹⁷, intensa preocupação a respeito da autenticação do titular do dado pessoal no instante em que ele estivesse exercitando os seus direitos perante a Corte Catarinense, e por esse motivo foram em busca de uma ferramenta tecnológica, que tivesse como premissa indispensável à segurança e a inclusão para todos os titulares dos dados pessoais envolvidos.

5. O case do TJSC com o aplicativo LGPDjus

O desenvolvimento dos trabalhos de implementação da Lei Geral de Proteção de Dados Pessoais, junto ao Tribunal de Justiça do Estado de Santa Catarina, teve seu início no final do ano de 2018, através de um pequeno grupo, incluindo-se esta autora, que se propuseram a estudar a referida lei para posteriormente conseguir implementá-la junto a referida Corte de Justiça.

16. [Certificação Digital - Câmara de Dirigentes Lojistas de Florianópolis \(cdlflorianopolis.org.br\)](https://cdlflorianopolis.org.br) Acesso em 30.11.2021

17. *Road Map* ou plano de ação é um documento onde serão detalhadas todas as atividades constantes no Programa Geral de Implementação da LGPD em uma organização, quer seja de natureza pública ou privada. Nota da autora.

Desde aquela data, todas as atividades quanto a implementação da Lei Protetiva no TJSC, vêm evoluindo de maneira pioneira, através do desenvolvimento dos trabalhos realizados pelo Comitê Gestor de Proteção de Dados Pessoais, em parceria com o Grupo de Trabalho Técnico e com a Encarregada do Tratamento de Dados Pessoais, formando a estrutura necessária para o *start* do Programa Geral de Implementação da LGPD junto ao respectivo Tribunal de Justiça. A partir de então, vários entregáveis foram sendo apresentados, dentro do rol de tarefas e atividades que foram listadas no seu Plano de Ação (*Road Map*), o qual fora construído como referencial permanente a ser seguido pelos membros responsáveis pela referida implementação da lei.

De todas as ações referenciadas no *Road Map*, como já foram anteriormente citadas, uma delas de maneira especial, suscitou grandes debates e pesquisas, qual seja, de que forma seria poderia fazer a autenticação da pessoa do titular dos dados pessoais, quando estivesse em busca de seus direitos constantes no artigo 18 da LGPD, de maneira que ela fosse segura e adequada na entrega das informações, e ou respostas de suas requisições exatamente ao indivíduo que realmente as tivesse requisitado, e não a terceira pessoa de maneira indevida. Por isso se diz que não basta apenas fazer a criação de um canal de atendimento do titular do dado pessoal, é preciso que as instituições fiquem atentas no que se refere a sua autenticação.

Inicialmente, para o atendimento das referidas requisições, foi criado um formulário eletrônico (FRANCOSKI, 2021. p.81-82) junto ao canal da ouvidoria, acrescentando-se a necessidade do titular em informar o nome da mãe. Desenhou-se em seguida os fluxos para o recebimento dos pedidos da seguinte forma: primeiramente através do e-mail ou telefone da encarregada, em um segundo momento através do preenchimento do formulário eletrônico, já anteriormente citado, e por último foi criado um fluxo para atendimento de demandas originadas através dos respectivos órgãos regulatórios, ou seja, da Autoridade Nacional de Proteção de Dados-ANPD e do Conselho Nacional de Justiça, CNJ.

Quando da formatação do citado “Formulário Eletrônico”, junto à Ouvidoria, muitas dúvidas e incertezas surgiram, eis que apesar de todos os esforços do Grupo de Trabalho Técnico e da Encarregada, para oferecer aos titulares dos dados pessoais mecanismos apropriados para a recepção de seus pedi-

dos, mesmo com a opção de introdução em tal documento do nome da mãe, chegou-se à conclusão, que somente com este pequeno acréscimo não seria possível se efetivar de maneira segura a autenticação do titular requisitante.

Assim, e tomando como exemplo as autenticações dos usuários, junto aos *Mobile Banking*¹⁸, que são amplamente utilizados na atualidade por grande parte da população, a Encarregada e seu Grupo de Trabalho Técnico, tiveram a ideia da construção de um aplicativo, que fosse capaz de fazer a autenticação em camadas dos titulares, de acordo com a modalidade e criticidade do pedido, conferindo a eles segurança e certeza de que as informações seriam entregues a quem tivesse realmente solicitado, e não a qualquer outra pessoa.

Para este projeto foi firmado no ano de 2020, uma parceria inicial com o AMBLAB¹⁹, e com o ITS Rio²⁰, e mais recentemente um Acordo de Cooperação Técnica entre o TJSC e o ITS Rio, para construção do aplicativo LGPDjus, além do projeto, ter recebido apoio financeiro do governo da Inglaterra, tendo sido o mesmo lançado oficialmente em um evento²¹ virtual no dia 30 de junho do corrente ano.

O LGPDjus é uma solução tecnológica, que envolve um aplicativo para *smartphone* e um sistema administrativo, desenvolvido para viabilizar o atendimento de modo simples e seguro das solicitações dos cidadãos sobre questões ligadas à privacidade e à proteção de dados pessoais no âmbito do TJSC, em conformidade com a LGPD, funcionando o mesmo, tanto no sistema IOS quanto ANDROID.

Com o referido aplicativo, os titulares de dados pessoais podem requisitar serviços específicos junto ao TJSC, tais como:

1. Solicitar informações sobre o tratamento de seus dados pessoais;
2. Requerer a alteração de dados pessoais incorretos, desatualizados ou incompletos;
3. Requerer a exclusão ou a interrupção do tratamento de seus dados pessoais;

18. *Mobile Banking* pode ser definido como o acesso a serviços bancários pelo celular, normalmente feito através de um aplicativo.

19. [Laboratório AMB \(amblab.com\)](http://amblab.com) Acesso em 30.11.2021.

20. [Instituto de Tecnologia e Sociedade - por uma internet livre e aberta \(itsrio.org\)](http://itsrio.org) Acesso em 30.11.2021.

21. [Varanda ITS #105 LGPDJus e inovação no setor público \(itsrio.org\)](http://itsrio.org) Acesso em 30.11.2021.

4. E ainda, acompanhar o andamento de suas requisições.

O acesso aos serviços disponibilizados no LGPDjus é baseado em níveis de segurança de autenticação de usuários, conforme perfil de identificação e criticidade do serviço que está sendo acionado, nos termos da Lei 14.063/2020 (BRASIL, 2020) que dispõe sobre o uso de assinaturas eletrônicas.

Desta forma, ao utilizar o aplicativo, os usuários encontrarão três níveis de segurança:

1. Acesso Livre: espaço onde é possível obter informações sobre a LGPD em geral, os direitos dos titulares, *link* para o portal da LGPD no TJSC, e informações sobre a Encarregada;
2. Assinatura Simples: que requer um cadastro do usuário na plataforma, com o fornecimento de nome, CPF autodeclarado e a criação de identificador de acesso baseado em um e-mail e em uma senha;
3. Assinatura Qualificada: que ocorre por meio de verificação humana do cadastro. É obtida por meio de cadastro com contraprova (o usuário submete foto segurando o documento) validada pelo TJSC, sendo desta forma criada uma chave de acesso para as requisições de maior criticidade.

Todas as operações realizadas no aplicativo, incluindo a validação da conta do usuário para a criação de uma assinatura avançada, são autenticadas utilizando a tecnologia *blockchain*²², garantindo a autenticidade, a inviolabilidade, a integridade e o não repúdio das informações que trafegam por meio do aplicativo.

Além disso, todas as operações realizadas no *software* administrativo do LGPDjus, a partir dos serviços requisitados, são comunicadas aos usuários de forma objetiva, com prazo predefinido, por meio de notificações disponibilizadas em um botão específico na tela principal, sendo que cada notificação possui um número de protocolo, os detalhes da solicitação e a resposta do TJSC para o serviço acionado.

Caso haja necessidade de complementar as informações que instruíram o pedido, o usuário receberá uma notificação e poderá interagir com a equipe da Encarregada para apresentar os dados exigidos por meio da própria notificação. Para cada tipo de serviço, há informações objetivas sobre o que pode

22. De forma resumida, *blockchain* é um sistema que permite rastrear o envio e recebimento de alguns tipos de informação pela internet. São pedaços de código gerados *online* que carregam informações conectadas – como blocos de dados que formam uma corrente – daí o nome.

ser solicitado e as condições para que o TJSC possa processar a requisição. Especificamente no botão relacionado a LGPD, o cidadão tem acesso a informações resumidas sobre conceitos instituídos pela lei e sobre os direitos dos titulares dos dados pessoais, além de disponibilizar um *link* para a leitura do inteiro teor da referida legislação protetiva.

No menu lateral são apresentados o Termo de Uso e a Política de Privacidade do LGPDJus, estabelecendo uma relação transparente com o usuário sobre a operação do aplicativo, os seus direitos e deveres. A Política de Privacidade, em especial, traz informações sobre o tratamento de dados pessoais no âmbito do aplicativo, indicando os dados tratados, a finalidade e a forma do tratamento, os agentes de tratamento envolvidos, o tempo e conservação dos dados, além de aspectos de segurança da informação. No mesmo menu lateral, há os contatos da Encarregada do TJSC, em atenção ao disposto no artigo 41 d LGPD, bem como, o endereço do Portal da LGPD no referido Tribunal²³, oferecendo ao usuário do aplicativo canais alternativos para dirimir dúvidas e se informar sobre a conformidade do órgão à legislação protetiva. Em seguida, serão apresentados, os painéis internos do aplicativo LGPDjus, que ajudam a Encarregada e sua equipe a fazer o gerenciamento de todas as requisições oferecidas pelos titulares dos dados pessoais, desde o seu oferecimento até a sua resposta final, dentro dos prazos determinados pela Lei Geral de Proteção de Dados Pessoais.

6. A importância do Painel de Gerenciamento Interno do Encarregado no LGPDjus para o controle efetivo dos fluxos das requisições dos titulares

A referida ferramenta possui vários painéis, sendo que no primeiro deles, quando o sistema é iniciado, por padrão, é apresentada uma tela com a relação de todas as solicitações existentes, e aquelas que ainda estão pendentes de análise. Para cada solicitação apresentada na relação é informado o número do protocolo criado, o tipo de solicitação (consulta, modificação, exclusão ou validação da conta), a situação (pendente, aguardando informações, finalizado), o prazo para resposta, bem como, o nome do solicitante.

23. [Lei Geral de Proteção de Dados Pessoais - Ouvidoria - Poder Judiciário de Santa Catarina \(tjsc.jus.br\)](http://tjsc.jus.br) Acesso em 03.12.2021.

Ao lado de cada nome é exibido um *status* do cadastro do usuário, indicando se ele possui um registro simples no sistema o qual deve aparecer em um quadro de cor vermelha, tendo nesse caso um acesso restrito aos serviços. Se o processo de validação ainda não foi concluído, vai estar destacado em uma tarja amarela, e por fim, se o requisitante já tem uma assinatura verificada, isso estará na cor verde, sublinhando nessa última hipótese, que o requisitante já teria o direito de utilizar todos os serviços disponíveis no aplicativo, identificando de forma adequada o seu perfil.

Para filtrar os resultados da tela inicial, o sistema dispõe de alguns parâmetros, tais como:

1. Na caixa “Situação” é possível limitar a apresentação às solicitações conforme o seu *status*, selecionando-se somente aquelas que estão pendentes, as finalizadas, ou aquelas que estão aguardando informações, com prazo vencido ou simplesmente todas as solicitações armazenadas no sistema, sem distinção;
2. Na caixa “Tipo”, define-se quais os tipos de requisições oferecidas (consulta, modificação, exclusão, validação de conta) que serão exibidas na relação de solicitações, sendo que selecionando-se “Consultar”, por exemplo, serão exibidas somente as solicitações de consulta sobre o tratamento de dados pessoais;
3. O campo “Ordem” permite ordenar os dados apresentados na relação de pedidos, de modo crescente ou decrescente, por um número de protocolo ou por prazo.

Em seguida temos que, ao clicar sobre o número de protocolo do pedido apresentado na lista de requisições, o sistema abre a tela desse pedido, apresentando detalhes do cadastro do solicitante, como nome, CPF e apelido, ou ainda, informações da solicitação, como data, tipo, situação, e o prazo sobre os dados consultados. Nos pedidos de validação da conta, são também apresentadas as fotos enviadas pelos usuários para a autenticação da identidade do titular e fornecimento de credencial avançada. No quadro de “Ações Disponíveis” há um botão para “Analisar e concluir”, a partir do qual é possível responder à consulta sobre o tratamento de dados pessoais, informar sobre o atendimento de pedido de alteração ou exclusão desses dados, ou até mesmo repassar alguma informação ao requerente, finalizando dessa forma o atendimento.

De outro lado, para solicitações de validação de conta, ao concluir a análise, são apresentadas as opções de “Recusar”, nesta hipótese o usuário per-

manece com uma assinatura simples, ou poderá aparecer a opção “Aceitar”, onde o usuário recebe um certificado no sistema, passando a contar com uma assinatura avançada. Caso o pedido necessite ser complementado para ser processado, deve ser acionado o botão “Pedir informação adicional”, deixando o pedido pendente, identificado com o *status* de “Aguardando informações”. Há ainda possibilidade de prorrogar o prazo de um pedido, no caso de dificuldade técnica para apresentar resposta a solicitação, através do botão “Mudar Prazo”. O quadro “Histórico de Ações” exibe todas as operações realizadas e a comunicação gerada ao usuário, encaminhada ao aplicativo do *smartphone* por meio de notificações.

No item “Solicitantes”, do menu superior, é exibida uma tela com a lista de todos os usuários cadastrados no sistema, sendo que na relação é informado o número de solicitações efetuadas pelo usuário no aplicativo. Nesta tela também é possível aplicar alguns filtros de exibição, conforme a situação da conta do usuário, ou pesquisar um usuário específico, informando nome, e-mail ou CPF. Ao clicar sobre um usuário é exibida uma tela de informações adicionais sobre o solicitante, sendo que nessa tela há um botão para acionar o procedimento de remoção de uma conta caso o requerente pretenda eliminar completamente seus dados dos registros do aplicativo.

Na tela de “Detalhes do Solicitante”, além das informações de cadastro e utilização do aplicativo pelo usuário, são disponibilizados para conferência os arquivos registrados em *Blockchain*, no item denominado “Total de Registros”. Toda a troca de informações com o usuário via aplicativo gera um novo arquivo PDF que será registrado também em “*Blockchain*”, quando então, o requerente irá receber este arquivo por e-mail, junto com a notificação de operação realizada no sistema. Na relação dos arquivos associados a um usuário, pode ser visualizado o “*Hash*²⁴” gerado para a operação, bem como data e hora do registro, o qual garante a integridade dos dados fornecidos, informando que não houve modificações nos dados por ele enviado.

No menu “Notificações” é possível enviar, ou cadastrar um comunicado para ser enviado a todos os usuários simultaneamente, via notificação do aplicativo. De outro lado, no campo “Tipo” há opções para escolher o grupo de

24. A função *Hash* (Resumo) é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções *Hash* são conhecidas por resumirem o dado. <https://www.techtudo.com.br/> Acesso em 30.11.2021.

destinatários da mensagem, tais como os solicitantes ativos, aqueles com assinatura verificada, ou os solicitantes que possuem pendências, dentre outros. Em um outro menu chamado de “Indicadores”, é possível verificar dados gerais de utilização do aplicativo, estratificados por tipo de solicitação e perfil do usuário, com a apresentação também de dados estatísticos relacionados aos pedidos recepcionados e todos os atendimentos realizados.

Podemos ainda mencionar que o “Painel Interno do Aplicativo”, consegue fornecer a Encarregada, um gerenciamento detalhado e eficaz sobre os caminhos percorridos por todas as requisições iniciadas pelos titulares dos dados pessoais através do menu externo do aplicativo, sendo o mesmo absolutamente fundamental para que as respostas sejam dadas de forma segura e dentro dos prazos estipulados pela Lei Geral de Proteção de dados no artigo 19 e seus incisos I e II.

Por derradeiro, é conveniente aqui mencionar, que o segundo parâmetro do LGPDjus, seria o da inclusão, o qual ainda não foi possível ser efetivado na versão de teste que está funcionando desde o seu lançamento. Todavia, tal funcionalidade já está em construção, e será inserida na segunda versão do aplicativo, que deverá entrar em funcionamento ainda no primeiro semestre de 2022, proporcionando às pessoas que apresentem alguma deficiência física a utilização do LGPDjus de forma dinâmica e integral, cumprindo assim com os objetivos iniciais planejados na vertente de “Segurança” versus “Inclusão”.

Considerações finais

O atendimento dos titulares, quando estão no exercício de seus direitos decorrentes do art. 18 d LGPD é uma das tarefas mais desafiadoras para o Encarregado, dentro da dinâmica do programa geral de implementação da lei protetiva, devendo ele ter apoio integral da organização, especialmente no que refere as ferramentas tecnológicas, capazes de lhe ajudar a realizar tal atividade de forma ágil e segura.

O LGPDjus surgiu junto ao TJSC com o propósito de atender a demanda de requisições, com três premissas determinantes, ou seja, segurança quanto a autenticação da pessoa do titular, de inclusão de atendimento de todas as camadas da população, sem qualquer distinção, incluindo-se dentre elas, às pessoas com deficiência física e por último, com a utilização de um painel interno de gerenciamento das requisições para facilitar o trabalho do Encarregado.

O aprimoramento de tal aplicativo, caminhará no sentido de cada vez mais aperfeiçoar o atendimento dos titulares, junto ao TJSC, através do LGPDjus, colaborando assim de forma determinante para a criação de uma nova cultura de proteção de dados pessoais e privacidade, além de projetar que tal dispositivo possa vir a ser compartilhado e utilizado também por muitas outras instituições.

É o que se espera.

Referências

ANPD [Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf](http://www.gov.br/segunda-versao-do-guia-de-agentes-de-tratamento-retificada.pdf) (www.gov.br)

----- [guia-poder-publico-anpd-versao-final.pdf](http://www.gov.br/guia-poder-publico-anpd-versao-final.pdf) (www.gov.br)

----- [guia_lgpd_final.pdf](http://www.gov.br/guia_lgpd_final.pdf) (www.gov.br)

----- [guia-vf.pdf](http://www.gov.br/guia-vf.pdf) (www.gov.br)

----- [guia-do-consumidor_como-protoger-seus-dados-pessoais-final.pdf](http://www.gov.br/guia-do-consumidor-como-protoger-seus-dados-pessoais-final.pdf) (www.gov.br)

AMBLAB. *Laboratório AMB*. Dezembro, 2018. Disponível em: www.amblab.com. Acesso em: 30 de novembro de 2021.

AIQON. *As requisições de acesso aos dados do titular (DSAR) LGPD*. Aiqon Blog. Sem Data. Disponível em: [As requisições de acesso aos dados do titular \(DSAR\) LGPD](http://aiqon.com.br/as-requisicoes-de-acesso-aos-dados-do-titular-dsar-lgpd) (aiqon.com.br)

AIQON. *DSAR LGPD - Direitos dos titulares: Como lidar com as requisições*. Aiqon Blog. Sem Data. Disponível em: [DSAR LGPD - Direitos dos titulares: Como lidar com as requisições](http://aiqon.com.br/dsar-lgpd-direitos-dos-titulares-como- lidar-com-as-requisicoes) (aiqon.com.br)

ARCANJO, Juliana. *LGPD: Lei 14.010-20 prevê adiamento da aplicação de sanções administrativas, mas ainda depende da MP 959/20*. Portal Migalhas. 24 de junho de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/329476/lgpd-lei-14010-20-preve-adiamento-da-aplicacao-de-sancoes-administrativas-mas-ainda-depende-da-mp-959-20>.

AZEVEDO, Mônica Sofia Rei de. *Gestão de Projetos: Conheça os conceitos fundamentais*. Portal Gestão. <https://www.portal-gestao.com/artigos/7770-gest%C3%A3o-de-projetos-conhe%C3%A7a-os-conceitos-fundamentais.html>.

BATISTA, Alex Oliveira Abreu; DIAS, Emillie Rebecca Bastos; SILVA, Murilo Borges. *Identificação digital baseada em blockchain: Um conceito disruptivo no ciberespaço*. Anais do V Simpósio Internacional de Inovação em Mídias Interativas ROCHA, Cleomar (Org). Goiânia: Media Lab / UFG, 2018. p. 307-320. Disponível em: [Alex_Batista.pdf \(ufg.br\)](#)

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2ª. reimpressão. Rio de Janeiro: Forense, 2019, 314 p.

BLOCKCHAIN: uma explicação simples. *Fala, Nubank*. 18 de agosto de 2019. Disponível em: [Blockchain: uma explicação simples - Fala, Nubank](#)

BRASIL. Lei no 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados*. Brasília. Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

BRASIL. Medida Provisória no 959, de 29 de abril de 2020. *Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD*. Brasília, 2020. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm#:~:text=Estabelece%20a%20operacionaliza%C3%A7%C3%A3o%20do%20pagamento,Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de.

BRASIL. LEI Nº 13.853, DE 8 DE JULHO DE 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Brasília, 2019. Presidência da República. Disponível em: [Redação dada pela Lei nº 13.853, de 2019](#)

-----http://www.planalto.gov.br/ccivil_03/_ato2019_2022/2020/Mpv/mpv959.htm#:~:text=Estabelece%20a%20operacionaliza%C3%A7%C3%A3o%20do%20pagamento,Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de.

BRASIL. LEI Nº 14.063, DE 23 DE SETEMBRO DE 2020. *Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001*. Diário Oficial da União, Edição 184. Seção 1. p.4. Brasília, 2020. Disponível em: [LEI Nº 14.063, DE 23 DE SETEMBRO DE 2020 - LEI Nº 14.063, DE 23 DE SETEMBRO DE 2020 - DOU - Imprensa Nacional](#)

BRASIL. Lei no 14.010, de 10 de junho de 2020. *Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19)*. Brasília, 2020. Presidência da República. Disponível em: [http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm#:~:text=Disp%C3%B5e%20sobre%20o%20Regime%20Jur%C3%ADdico,coronav%C3%ADrus%20\(Covid%2D19\)](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm#:~:text=Disp%C3%B5e%20sobre%20o%20Regime%20Jur%C3%ADdico,coronav%C3%ADrus%20(Covid%2D19).).

BRASIL. LEI Nº 13.853, DE 8 DE JULHO DE 2019. *Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências*. Brasília, 2019. Presidência da República. Disponível em: [.http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm).

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, 1988. Disponível em: https://www.senado.leg.br/atividade/const/con1988/con1988_15.12.2016/art_5_.asp.

BRASIL. LEI Nº 8.666, DE 21 DE JUNHO DE 1993. *Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências*. Brasília, 1993. Presidência da República. Disponível em: <http://comprasnet.gov.br/legislacao/leis/lei8666.pdf>.

BRASIL. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. *Dispõe sobre a proteção do consumidor e dá outras providências*. Brasília, 1990. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm

-----[.http://www.planalto.gov.br/CCIVIL_03/_Ato20112014/2014/Lei/L12965.htm](http://www.planalto.gov.br/CCIVIL_03/_Ato20112014/2014/Lei/L12965.htm).

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. *Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências*. Brasília, 2011. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm.

BRASIL. *Perguntas Frequentes – ANPD*. Site. Última atualização em abril de 2022. Disponível em: [Perguntas Frequentes – ANPD – Português \(Brasil\) \(www.gov.br\)](http://www.gov.br/pt-br/assuntos/legislacao/legislacao-covid-19)

-----[.http://www4.planalto.gov.br/legislacao/portal-legis/legislacao-covid-19](http://www4.planalto.gov.br/legislacao/portal-legis/legislacao-covid-19).

-----[.http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709.htm#ementa](http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709.htm#ementa).

CABELLA, Daniela Monte Serrat; FERREIRA, Raíssa Moura. *Descomplicando: Agentes de Tratamento*. Portal Migalhas. 13 de maio de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/326741/descomplicando--agentes-de-tratamento>.

CARLO, Giovanni. *Como Compatibilizar os Direitos dos Titulares com a Autenticação*. 27 de setembro de 2021. Disponível em: dtibr.com. Acesso em: 30 de novembro de 2021.

CONSELHO NACIONAL DE JUSTIÇA. *Verbete Wikipedia*. Sem Data. Disponível em: https://pt.wikipedia.org/wiki/Conselho_Nacional_de_Justi%C3%A7a.

CDL. *Certificação Digital - Câmara de Dirigentes Lojistas de Florianópolis*. Florianópolis-SC. Sem Data. Disponível em: [Certificação Digital - Câmara de Dirigentes Lojistas de Florianópolis \(cdlflorianopolis.org.br\)](http://CertificacaoDigital-Camara.deDirigentesLojistas.deFlorianopolis.org.br)

CNJ. Recomendação N° 73 de 20/08/2020. *Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD. DJe/CNJ n° 272/2020, em 21/08/2020, p. 9-11*. Brasília, 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3432>.

----- <https://atos.cnj.jus.br/files/original202445202010165f8a018d31b02.pdf>.

CNJ. *LGPD: Norma define critérios mínimos para adequação pelos tribunais*. Site do CNJ. 15 de dezembro de 2020. Disponível em: <https://www.cnj.jus.br/lgpd-norma-define-criterios-minimos-para-adequacao-pelos-tribunais/>.

CUEVA, Ricardo Villas Boas. DONEDA, Danilo. MENDES, Laura Schertel. Coordenadores. *Lei geral de proteção de dados (Lei n° 13.709/2018: a caminho para a implementação da LGPD)*. São Paulo: Thomson Reuters Brasil, 2020, 255 p.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação a Lei geral de proteção de dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, 352 p.

DONEDA, Danilo; SARLET, Ingo Wolfgang. MENDES, Laura Schertel. JUNIOR, Otávio Luiz Rodrigues. Coordenadores. BIONI, Bruno Ricardo, Coordenador Executivo. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. 741 p.

EUROPA. <https://eurlex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679>.

EUROPA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. *Relativo à proteção das pessoas singulares no que*

diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 4/5/2016. L 119/1. Parlamento Europeu, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>.

EUROPA. *Regulamento Geral sobre a Proteção de Dados*. Consulta online. Sem data. Disponível em: gdprinfo.eu

FRANCOSKI, Denise de Souza Luiz. *O exercício dos direitos dos titulares dos dados pessoais sob a ótica do controlador e o encarregado das organizações públicas: expectativas e possibilidades*. Artigo contido na obra Estudos sobre privacidade e proteção de dados. Coordenador Felipe Palhares. -São Paulo: Thomson Reuters Brasil, 2021. p. 578-579.

FRANCOSKI, Denise de Souza Luiz. *Aspectos práticos para a implementação da Lei Geral de Proteção de Dados Pessoais-LGPD nos Órgãos Públicos: o case do Tribunal de Justiça de Santa Catarina-TJSC*. FRANCOSKI, Denise de Souza Luiz, TASSO, Fernando Antonio. Coordenadores. *A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos no setor público e privado*. p. 81-82. 1. ed. São Paulo :Thomson Reuters Brasil, 2021. p.81-82.

FRANCOSKI, Denise de Souza Luiz, TASSO, Fernando Antonio. Coordenadores. *A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos no setor público e privado*. p. 81-82. 1. ed. São Paulo :Thomson Reuters Brasil, 2021. 987 p.

FRANCOSKI, Denise de Souza Luiz. *“LGPD-JUS” os seus direitos em suas mãos: O case do TJ/SC*. Migalhas. 18 de junho de 2021. Disponível em: migalhas.com.br

FRASÃO, Ana, TEPEDINO, Gustavo, OLIVA, Milena Donato. Coordenadores. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters, 2019, 820 p.

FEIGELSON, Bruno; SIQUEIRA, Antônio Henrique Albani. *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/018*. São Paulo: Thomson Reuters Brasil, 2019, p. 126.

HASC. <https://www.techtudo.com.br/>

HARARI, Yuval Noah. *21 lições para o século 21*. Tradução Paulo Geiger. São Paulo: Companhia das Letras, 2018, 441 p.

ITSRIO. *Instituto de Tecnologia e Sociedade - por uma internet livre e aberta*. Site. Rio de Janeiro-RJ, sem data. Disponível em: [Instituto de Tecnologia e Sociedade - por uma internet livre e aberta \(itsrio.org\)](http://www.institutoitsrio.org)

ITSRIO. *Varanda ITS #105 LGPDJus e inovação no setor público* (itsrio.org). Rio de Janeiro-RJ, 30 de julho de 2021. Disponível em: [Varanda ITS #105 LGPDJus e inovação no setor público \(itsrio.org\)](#)

LIMA, Cintia Rosa Pereira. Coordenadora. *Comentários à lei geral de proteção de Dados: Lei n. 13.709/2018, com a alteração da lei n. 13.853/2019*. São Paulo: Almedina, 2020, 431 p.

LIMA, Cíntia Rosa Pereira de. *Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015)*. São Paulo: Almedina, 2020, 333 p.

LGPD: *A importância da autenticação do consumidor*. O Consumerista. 16 de dezembro de 2019. Disponível em [oconsumerista.com.br](#). Acesso em 30 de novembro de 2021.

MATOS, Renata Montez de. *Autenticação de usuários através da utilização de sistemas biométricos*. Dissertação de Mestrado. Programa de Pós-Graduação em Informática. Universidade Federal do Rio Grande do Sul. Porto Alegre-RS, 2000. Disponível em: [Autenticação de usuários através da utilização de sistemas biométricos \(ufrgs.br\)](#).

MALDONADO, Viviane Nóbrega. OPICE BLUM, Renato. Organizadores. *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. São Paulo: Thomson Reuters Brasil, 2018. 252 p.

MALDONADO, Viviane Nóbrega, OPICE BLUM, Renato. *Lei Geral de Proteção de Dados comentada*. Coordenadores. São Paulo: Thomson Reuters Brasil, 2019, 411 p.

MALDONADO, Viviane Nóbrega. *LGPD: Lei Geral de Proteção de Dados pessoais: manual de implementação*. Coordenação. São Paulo: Thomson Reuters Brasil, 2019.

MELO, Pedro Henrique Aparecido Damaso de. *Mecanismos de Autenticação e Controle de Acesso para uma Arquitetura de Internet do Futuro*. Dissertação de Mestrado. Programa de Pós-Graduação em Ciência da Computação. Universidade Federal de Uberlândia. Uberlândia-MG, 2017. Disponível em: [MecanismosAutenticacaoControle.pdf \(ufu.br\)](#)

OPICE BLUM, Renato. VAINZOF, Rony. MORAES, Henrique Fabretti. Coordenadores. *Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR*. São Paulo: Thomson Reuters Brasil, 2020, 558 p.

OPICE BLUM, Renato. Organizador. *Proteção de dados: desafios e soluções na adequação à lei*. Rio de Janeiro: Forense, 2020, 296 p.

PALHARES, Felipe. Coordenação. *Temas atuais de proteção de dados*. São Paulo: Thomson Reuters Brasil, 2019. 549 p.

PALHARES, Felipe. Coordenação. *Estudos sobre Privacidade e Proteção de Dados*. Thomson Reuters Brasil, 2021, 644 p.

POZZO, Augusto Neves Dal, MARTINS. Ricardo Marcondes Martins. Coordenadores. *LGPD e a Administração Pública: uma análise ampla dos impactos*. São Paulo: Thomson Reuters Brasil, 2020, 991 p.

-----[.SRC-RR-39.pdf](#)

-----[.Royal Society.pdf](#)

PINHÃO E KOIFFMAN. LGPD: *Proteger dados ou fornecer acesso? Eis a questão!* Site. 2020. Disponível em: [LGPD: Proteger dados ou fornecer acesso? Eis a questão! - PK Pinhão e Koiffman - Advogados \(direitoparatecnologia.com.br\)](#)

RODOTÁ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. 381 p.

SWISSCAM. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. 15 de setembro de 2021. Site. Disponível em: [33. Lei Geral de Proteção de Dados Pessoais \(LGPD\) | Swisscam Brasil](#)

TEIXEIRA, Tarcísio, ARMELIN. Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados: Comentado artigo por artigo*. 2. ed. Ver., atual., e ampl. Salvador: Editora JusPodivm, 2020, 224 p.

TJSC. <https://www.tjsc.jus.br/>.

TJSC. *Organograma*. Poder Judiciário de Santa Catarina. Florianópolis-SC. Sem Data. Disponível em: <https://www.tjsc.jus.br/organograma>.

TJSC. *Lei Geral de Proteção de Dados Pessoais*. Ouvidoria. Poder Judiciário de Santa Catarina. Florianópolis-SC. Sem Data. Disponível em: [Lei Geral de Proteção de Dados Pessoais - Ouvidoria - Poder Judiciário de Santa Catarina \(tjsc.jus.br\)](#)

TJSC. RESOLUÇÃO GP N. 28 DE 12 DE JUNHO DE 2019. *Institui o Comitê Gestor de Proteção de Dados no âmbito do Poder Judiciário do Estado de Santa Catarina*.

Florianópolis-SC. Cadernos Administrativo do Poder Judiciário, nº3080, p. 1-2. Disponível em: <http://busca.tjsc.jus.br/buscatextual/integra.do?cdSistema=1&cdDocumento=174510&cdCategoria=1&q=&frase=&excluir=&qualquer=&prox1=&prox2=&proxc=>.

----- . file:///C:/Users/delud/Downloads/Rsolucao-n10_-Institui-o-Comite-Gestor-de-Protecao-de-Dados.pdf.

----- . <https://www.tjsc.jus.br/web/ouvidoria/lei-geral-de-protecao-de-dados-pessoais/legislacao-relacionada>.

TJSC. *Publicações Sobre a LGPD*. Florianópolis-SC. Sem Data. Disponível em: <https://www.tjsc.jus.br/web/ouvidoria/lei-geral-de-protecao-de-dados-pessoais/publicacoes-sobre-o-tema>.

----- . [Sensibilização da LGPD nas Serventias Extrajudiciais https://www.tjsc.jus.br/web/ouvidoria/lei-geral-de-protecao-de-dados-pessoais/publicacoes-sobre-o-tema](https://www.tjsc.jus.br/web/ouvidoria/lei-geral-de-protecao-de-dados-pessoais/publicacoes-sobre-o-tema).

----- . <https://www.tjsc.jus.br/web/academia-judicial>.

Anexos

ANEXO I – TELAS DO APLICATIVO LGPDJUS

Figura 1 - Tela principal do LGPDjus



Figura 2 – Tela dos serviços relacionados aos dados pessoais do usuário, acessada no botão “Meus Dados Pessoais”



Figura 3 – Tela de consulta sobre o tratamento de dados pessoais pelo TJSC



Figura 4 – Tela de solicitação de exclusão de dados pessoais tratados pelo TJSC

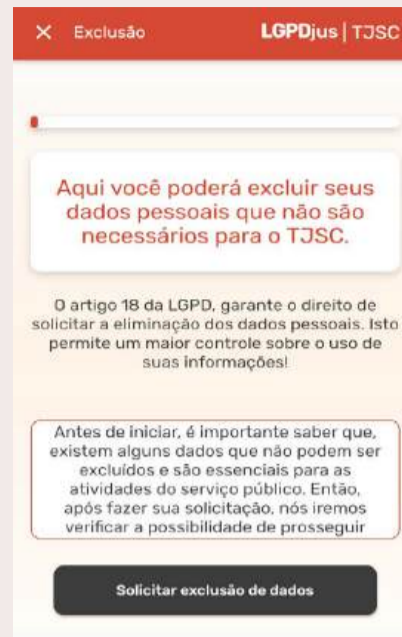


Figura 5 - Tela de informações gerais sobre a LGPD, acessada no botão “Conhecer mais sobre a LGPD”



Figura 6 – Tela de conceitos relacionados à LGPD, com acesso livre



Figura 7 – Tela para criação de conta do usuário (assinatura simples)

Cadastro LGPDjus | TJSC

Crie sua conta
Etapa 1

Nome completo

CPF

Como deseja ser chamado(a)?

Próximo

Figura 8 – Tela de confirmação de cadastro do usuário com assinatura simples

Validar conta LGPDjus | TJSC

Seu cadastro foi realizado com sucesso!

Para utilizar todas as funções do aplicativo LGPDjus você precisa verificar sua identidade. Para isso, será necessário enviar uma foto do seu documento e também, uma selfie sua segurando o documento.

Quando quiser, clique em continuar para realizar verificação.

Continuar

Fazer mais tarde

Figura 9 – Tela de criação de assinatura avançada para o usuário

Validação de conta LGPDjus | TJSC

Qual documento de identificação deseja enviar?

Carteira Nacional de Habilitação (CNH)

Carteira de Identidade (RG)

Continuar

Figura 10 – Tela de apresentação de foto para criação de assinatura avançada



Figura 11 – Tela de confirmação de processamento da assinatura avançada



Figura 12 – Menu lateral do aplicativo, com links para informações complementares

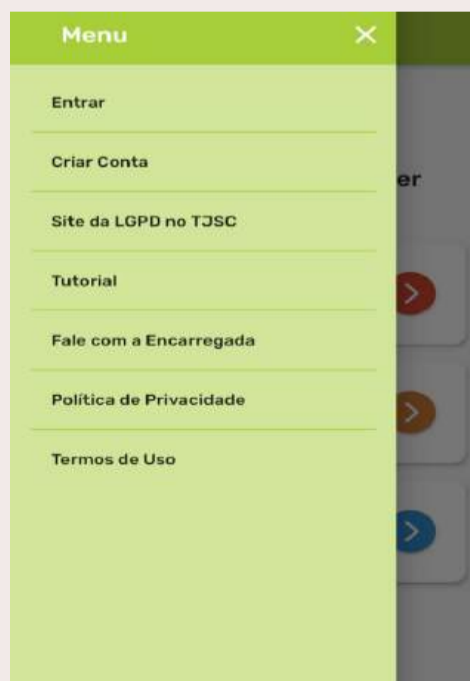
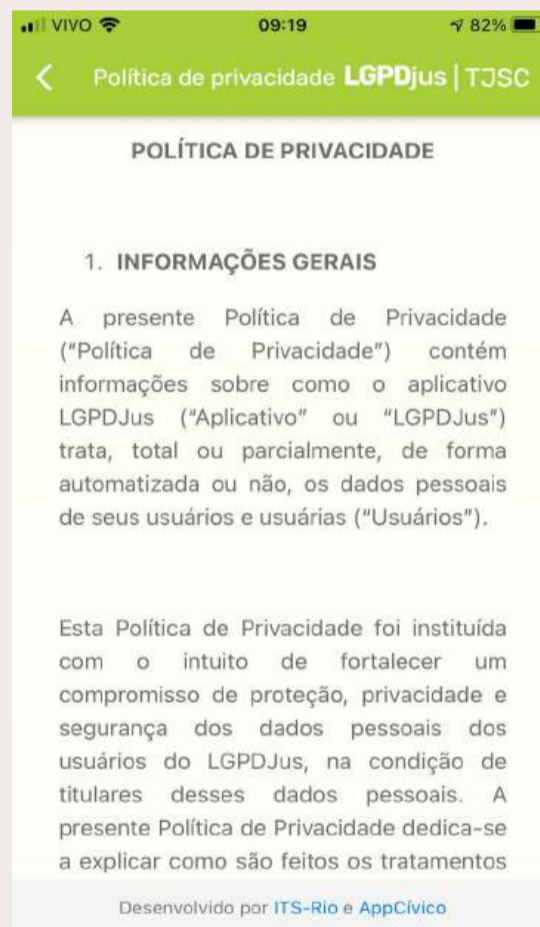


Figura 13 – Tela de informações de contato da Encarregada



Figura 14 – Tela de informações sobre a política de privacidade do aplicativo



ANEXO II – TELAS DO SISTEMA ADMINISTRATIVO

Figura 15 - Tela principal do sistema administrativo do LGPDjus, com a relação das solicitações pendentes

The screenshot shows the main interface of the LGPDjus administrative system. At the top, there is a navigation bar with the LGPDjus logo and menu items: Solicitações, Notificações, Solicitantes, Registros, Indicadores, and Giovanni. A search bar on the right allows searching by name or email. The main heading is 'Lista de solicitações', followed by a sub-heading: 'Nesta tela você pode visualizar todas as solicitações do sistema. [ver mais](#) ⓘ'. Below this is a 'Filtros:' section with three dropdown menus: 'Situação' (set to 'Solicitações pendentes'), 'Tipo da solicitação' (set to 'Todos os tipos'), and 'Ordem' (set to 'Padrão (protocolo decedente)'). An 'Aplicar' button is to the right. Below the filters, it says '5 resultados'. A table lists the requests with columns: Protocolo, Tipo da solicitação, Situação, Prazo, and Solicitante. The table contains five rows of data with status indicators like 'verificação pendente', 'não verificada', and 'verificada'. At the bottom left, it says 'Página 1 de 1'.

Protocolo	Tipo da solicitação	Situação	Prazo	Solicitante
21110400002	Consultar	Pendente	19/11/2021	[Redacted] verificação pendente
21110400001	Validação de conta	Pendente	19/11/2021	[Redacted] verificação pendente
21110300001	Consultar	Pendente	18/11/2021	[Redacted] não verificada
21102900001	Consultar	Pendente	13/11/2021	[Redacted] verificação pendente
21102300001	Consultar	Pendente	16/11/2021	[Redacted] verificada

Figura 16 – Filtros disponíveis na tela de solicitações do sistema administrativo

This screenshot shows the same interface as Figure 15, but with the filter dropdown menus open. The 'Situação' dropdown shows options: 'Solicitações pendentes' (selected), 'Solicitações finalizadas', 'Solicitações aguardando informações', 'Solicitações com prazo vencido', and 'Todas as solicitações'. The 'Tipo da solicitação' dropdown shows: 'Todos os tipos' (selected), 'Consultar', 'Modificação', 'Exclusão', and 'Validação de conta'. The 'Ordem' dropdown shows: 'Padrão (protocolo decedente)' (selected), 'Protocolo crescente', 'Prazo mais recente primeiro', and 'Prazo mais antigo primeiro'. The 'Aplicar' button remains visible.

Figura 17 – Tela de detalhamento de uma solicitação

The screenshot displays the detailed view of a request with ID '21102300001'. The top navigation bar is the same. The heading is 'Solicitação 21102300001' with a sub-heading: 'Nesta tela você interagir com o solicitante através das ações. [ver mais](#) ⓘ'. The page is divided into three main sections. The left section, 'Dados da solicitação', includes: 'Data de abertura: 23/10/2021 02:56:17', 'Categoria da solicitação: Consultar os dados', 'Situação: Pendente', and 'Prazo: 07/11/2021'. Below this is 'Detalhes da solicitação' with the question 'Quais os dados que você deseja consultar em nosso sistema?' and the answer 'CPF, Nome'. The bottom section is 'Histórico de ações:', showing a log entry: '25/10/2021 17:08:23 Conclusão de solicitação: Teste finalizado'. The right section, 'Dados do solicitante', includes: 'Nome completo: Usuário Teste verificada', 'CPF: [Redacted]', and 'Como deseja ser chamado: Usuário'. Below this is 'Ações disponíveis' with buttons for 'Pedir informação adicional', 'Mudar prazo', and a large blue 'Analisar e concluir' button.

Figura 18 – Tela com a relação de usuários cadastrados no LGPDjus e os filtros disponíveis para a exibição dos usuários

Lista de solicitantes

Nesta tela você pode visualizar todos os solicitantes que criaram uma conta no aplicativo. [ver mais](#) ⓘ

Filtros:

Tipo: Seleccione uma opção

Busca por nome, email ou CPF: usuário teste

Aplicar

Nome completo	E-mail	CPF	Nº de solicitações
Usuário Teste verificada	[Redacted]	[Redacted]	2 solicitações

Página 1 de 1

Figura 19 – Tela com informações detalhadas sobre um usuário

Detalhes do solicitante Usuário Teste

Nesta tela você pode ter uma visão geral da conta de um solicitante. [ver mais](#) ⓘ

- Status da conta: verificada
- Total de solicitações: 2 solicitações
- Total de registros: 6 arquivos
- Nome Completo: Usuário Teste
- Como deseja ser chamado: Usuário
- E-mail: [Redacted]
- CPF: [Redacted]
- Último uso do aplicativo: 04/11/2021 09:47:56

Remover conta

Clique no botão abaixo para iniciar a remoção da conta.

Agendar remoção

Figura 20 – Tela com os registros em *blockchain* efetuados para um usuário

Lista de registros em blockchain

Nesta tela você pode acompanhar os registros em blockchain. [ver mais](#) ⓘ

Filtrando por cliente: Nome: Usuário Teste, CPF: 887.715.639-20

Protocolo: Todos os registros

Aplicar

6 resultados

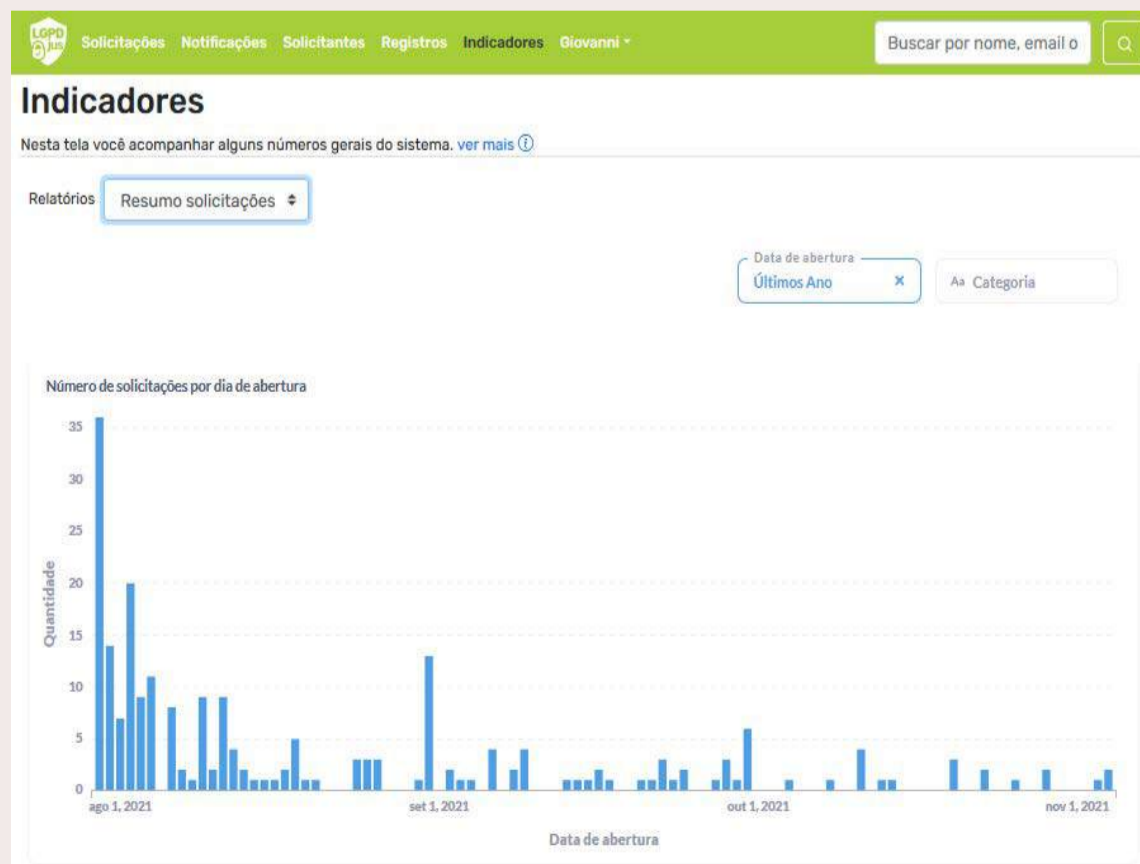
Horário de criação	Arquivo	Solicitante	Hash SHA-256	Horário do registro	Situação
hoje 23:00:00	Baixar solicitacao-21102300001.pdf Visualizar solicitação 21102300001	Usuário Teste	00cc5bc9d4d19f...	-	Pendente de r...
25/10/2021 17:00:00	Baixar solicitacao-21102300001.pdf Visualizar solicitação 21102300001	Usuário Teste	45df3b6e885a3...	25/10/2021 18:01:58 (São Paulo)	Registrado txid: 69fbc87e...
23/10/2021 02:00:00	Baixar solicitacao-21102300001.pdf Visualizar solicitação 21102300001	Usuário Teste	67a0d4317105ec...	23/10/2021 03:06:00 (São Paulo)	Registrado txid: 14988988...
22/10/2021 12:00:00	Baixar solicitacao-21102000001.pdf Visualizar solicitação 21102000001	Usuário Teste	33ffc212b378aa...	22/10/2021 13:04:06 (São Paulo)	Registrado txid: fb6f2eb31...

Figura 21 – Tela de envio de notificações para todos os usuários do aplicativo

Figura 22 – Tela de indicadores gerais das solicitações e usuários atendidos.



Figura 23 – Tela de indicadores detalhados das solicitações

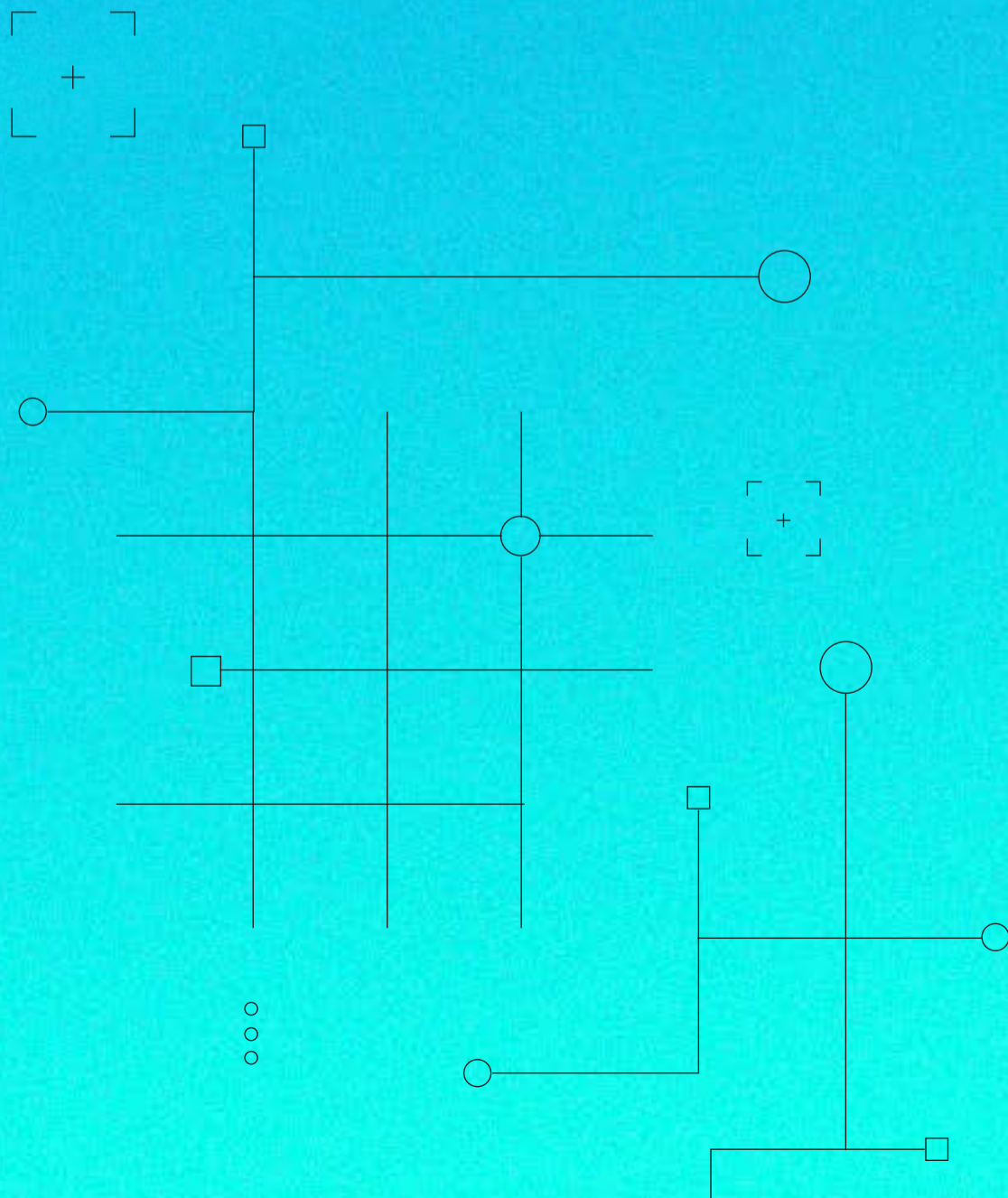


DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

6

Dark patterns nas contratações pela internet e o direito do consumidor

VIVIANE DE SOUZA RAMOS PEREIRA



Sumário: Introdução. 1. O que são *dark patterns*? 2. Implicações jurídicas. 2.1. Vulnerabilidade eletrônica. 2.2. Dever de informação. 2.3. Proteção contra práticas abusivas 2.4. Princípio da confiança. Considerações finais. Referências.

Introdução

Quem nunca fez uma compra *online* com apenas um clique e depois se arrependeu? Quem nunca forneceu dados bancários para testar gratuitamente um serviço, mas se deu conta, tempos depois, de que efetuava pagamentos mesmo sem utilizá-lo, simplesmente pelo fato de que havia esquecido de cancelá-lo após o período de teste? Quem nunca buscou algo gratuito na internet e acabou clicando inadvertidamente em algum anúncio que apareceu na sua tela? Quem nunca se confundiu num *website* e comprou sem querer o produto ou serviço mais caro dentre as opções ofertadas?

Esses são alguns exemplos das chamadas *dark patterns* ou padrões obscuros em livre tradução, uma prática que infelizmente ainda é bastante utilizada por alguns fornecedores no mercado de consumo.

O tema é tão relevante que a *European Data Protection Board* recentemente publicou o Guideline n° 3/2022 e uma consulta pública versando sobre como reconhecer e evitar as *dark patterns* nas plataformas de mídias sociais.

O uso de mecanismos de *dark patterns* ocorre tanto no ambiente físico como no virtual. Entretanto, este artigo restringe-se à análise desta prática nos meios virtuais e de seus impactos na esfera protetiva consumerista.

Preliminarmente deve-se atentar que as contratações pela internet tiveram crescimento recorde devido às medidas sanitárias de distanciamento social recomendadas para combater a pandemia da Covid-19. Alguns veículos de comunicação chegaram a anunciar que a “Pandemia faz triplicar número de brasileiros que compram produtos domésticos pela internet” apenas no ano de 2020 (SILVEIRA, 2020) e “No primeiro trimestre de 2021, as vendas [de *e-commerce* no Brasil] tiveram alta de 57,5% em relação ao mesmo período em 2020” (DADOS, 2021).

1. Graduada em Direito pela Universidade do Estado do Rio de Janeiro, pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro, empregada pública federal, advogada e consultora em Privacidade e Proteção de Dados Pessoais, Direito Civil e Direito do Consumidor.

Nesse cenário de crescimento nas contratações pela internet e de contratos de consumo que utilizam cada vez mais algoritmos², com códigos de programação cada vez mais precisos e eficazes para personalizar e customizar conteúdos e ofertas diversas ao usuário consumidor, o uso de *dark patterns* traz problemas ainda maiores como será abordado em seguida.

1. O que são *dark patterns*?

Primeiramente é preciso entender o que são *dark patterns* ou padrões obscuros em livre tradução, conceito criado por Harry Brignull (BRIGNULL, s.d.) em 2010 (A SPOTLIGHT, 2021).

Dentre os diversos conceitos encontrados destaco aquele encontrado em um site especializado em tecnologia segundo o qual “*Dark patterns* são direcionamentos intencionais, para que o usuário faça algo que não faria naturalmente” (UX, 2021).

Esses direcionamentos se dão no meio *online* por meio do *design* de uma interface, projetado para manipular o comportamento dos usuários consumidores a agirem de determinada forma não natural e, com isso, aumentar a taxa de conversão³ e as vendas daquele fornecedor.

Por isso é que as *dark patterns* também são chamadas de “UX do mal” pelos *designers*, pois, para alguns profissionais da área, trata-se de uma utilização possivelmente antiética e irresponsável do *UX Design* (UX, 2021).

UX Design (user experience design) significa desenvolver produtos e serviços colocando a experiência do usuário como seu principal objetivo, no centro do desenvolvimento. Nesse sentido, “*UX Design* é uma abordagem utilizada para resolver problemas de forma interdisciplinar, holística e direcionada a um profundo entendimento de comportamento, cognição, capacidades, desejos e contexto humano” (AGUIAR, 2021, p. 100).

Quando todo esse conhecimento sobre a experiência do usuário e o comportamento humano é utilizado com fins maliciosos, para induzir compras ou inscrições indesejadas pelos usuários consumidores, surge um problema que

2. Algoritmo “pode ser entendido como uma sequência de raciocínios, instruções ou operações para alcançar um objetivo, sendo necessário que os passos sejam finitos e operados sistematicamente”. (SAIBA, 2021).

3. Taxa de conversão pode ser entendida como uma métrica utilizada para mensurar a eficiência da comunicação de um *website* ou página específica e, assim, entender como é o retorno de tempo e dinheiro de cada investimento com relação às vendas. Exemplos de utilização dessa métrica: preenchimento de cadastro, solicitação de orçamento, inscrição em *newsletter* e venda de produtos ou serviços. (TAXA, 2020).

ultrapassa os debates éticos da área do *Design* e passa a ser também jurídico, como será especificado no próximo capítulo.

Alguns aplicativos e páginas de internet são muitas vezes propositalmente projetados para não serem plenamente compreendidos pelo usuário consumidor e, assim, levá-lo a tais comportamentos. Isso fica mais claro com os exemplos a seguir.

Segundo Ana Couto, os casos mais comuns de aplicação da prática de *dark patterns* são: (i) as opções pré-marcadas para consentir com o recebimento de *spam* de *marketing* e *download* de programas; (ii) ocultação de *links* de cancelamento; (iii) custos que apenas são listados na etapa final de conclusão de uma compra; e (iv) a realização de cobranças automáticas após o período de teste de determinado serviço (COUTO, 2021).

São igualmente apontadas como manifestações desses padrões obscuros: (i) o desvio deliberado, que faz com que o usuário adquira o produto ou serviço de maior valor por ocupar uma posição de destaque na tela em contrapartida com a posição discreta e por vezes apagada da opção mais barata; (ii) aplicativos que pedem acesso aos contatos dos usuários e utilizam tais dados para envio indevido de *spams* para seus conhecidos; (iii) condicionamento do período supostamente gratuito de teste de um serviço a uma continuidade forçada, com a mandatória contratação da assinatura após esse período; (iv) adição de itens no carrinho de compras sem solicitação do usuário; (v) dificuldades de cancelamento por obstrução visual; (vi) compra com apenas um clique, que favorece as compras por impulso (UX, 2021); (vii) anúncios disfarçados na página como se fizessem parte do conteúdo regular ou da navegação, o que leva a um aumento do número de cliques pelos usuários; e (viii) desvios de configuração para desviar a atenção do usuário para um lugar específico e, assim, ele não perceber algo mais que está acontecendo (KOVACS, s.d.).

Por fim, ainda temos: (i) banners disfarçados de interface; (ii) *checkbox* de *newsletter* já marcado por padrão em um cadastro ou que está escondido na página; (iii) *call to action*⁴ em grandes proporções na compra de poltronas mais espaçosas e conseqüentemente caras em passagens aéreas; (iv) solicitação de e-mail do usuário que acaba de acessar o site por meio de um *pop-up* (SOUZA, c2021); (v) erro simulado ao acessar um *site* utilizando um bloqueador de

4. Call to action é uma chamada para que o usuário realize determinada ação indicada pelo website, e-mail, anúncio etc. (SIQUEIRA, 2020).

publicidade; (vi) *nagging*, ou repetição de determinada funcionalidade até que o usuário autorize a ação solicitada e sem opção de parar a exibição (NICOLL, 2020); (vii) *interface interference* (INTERFACE, 2018), facilmente verificada por *pop-ups*⁵ grandes e seu minúsculo botão de “X” para seu fechamento; e até mesmo (viii) culpabilização e manipulação do usuário por determinada decisão através de um texto propositalmente redigido para envergonhar o usuário da sua decisão e tentar manipulá-lo a tomar a opção preferível para o *site* (VARGAS, 2021) (TARDELLI, 2020).

Algumas das corporações mundiais mais valiosas como Google e Facebook já foram sancionadas pela autoridade de proteção de dados francesa CNIL (*Commission Nationale Informatique & Libertés*) pela utilização de *dark patterns* no gerenciamento de *cookies*, violando, assim, a legislação nacional francesa de proteção de dados (DELIBERATION, 2021).

Essa decisão está em consonância com o estudo publicado em 2019 pelo LINC (*Le laboratoire d’innovation numérique de la CNIL*), laboratório de inovação do CNIL (SHAPING, 2019) e, segundo uma entrevistada do artigo de David Meyer (2022), passa a mensagem incisiva de que os usuários devem ter verdadeiras e justas possibilidades de escolha *online*, e não apenas escolhas do interesse das corporações (tradução nossa).

O órgão de proteção de dados do Reino Unido ICO (*Information Commissioner’s Office*) igualmente repudia o uso de *dark patterns* para obter o consentimento dos usuários na publicidade *online* (INFORMATION, 2021) (tradução nossa) e se encontra na mesma linha do entendimento do CNIL.

Fica claro, portanto, que as *dark patterns* podem se manifestar de diversas maneiras, das mais sutis às mais perceptíveis, no cotidiano dos usuários consumidores, o que traz repercussões jurídicas relevantes conforme será discutido abaixo.

2. Implicações jurídicas

Inicialmente, cabe pontuar que nem toda contratação realizada pela internet será de consumo. Será considerada relação de consumo a relação jurídica na qual um consumidor adquire produtos ou contrata serviços como destina-

5. *Pop-ups* são janelas que surgem na tela quando o usuário visita uma página web ou aplicativo sem que ele a solicite por nenhum comando ou clique. (POP-UP, c2003-2022).

tário final de um fornecedor (GOMES, 2016, p. 23-24)⁶.

Uma vez caracterizada a relação jurídica como consumerista, os diplomas normativos específicos mais relevantes para as contratações pela internet e conseqüentemente para esse artigo são o Código de Defesa do Consumidor – CDC (lei federal nº 8.078, de 11 de setembro de 1990) (BRASIL, 1990) e o Decreto nº 7.962, de 15 de março de 2013 (BRASIL, 2013), que regulamenta a Lei nº 8.078/1990 para dispor sobre a contratação no comércio eletrônico.

Corroborando esse entendimento, doutrina renomada aponta que o CDC, principal diploma legal na esfera protetiva consumerista, tem um campo de aplicação subjetivo ou *ratione personae*, ou seja, ele é aplicável a todas as relações contratuais e extracontratuais entre consumidores e fornecedores, alertando também que esses papéis são relacionais:

[...] a definição subjetiva neste novo direito privado solidário é relacional: assim um leigo, um civil frente a outro civil, será uma relação puramente de direito civil; o mesmo civil frente a um empresário, ou fornecedor, será uma relação de consumo; e este empresário ou profissional, talvez no mesmo tipo contratual de compra e venda, de transporte de coisas, de mandato, se frente a outro empresário ou profissional, será uma relação empresarial ou do antigo direito comercial [...] (BENJAMIN, 2009, p. 67-68).

Em resumo, em havendo uma relação jurídica entre pessoas que se enquadram no conceito de consumidor de um lado e de fornecedor de outro, resta caracterizada a relação de consumo e a incidência do CDC (BRASIL, 1990).

Quando essa relação é realizada eletronicamente, através da rede mundial de computadores⁷, aplica-se, ainda, o Decreto 7.962/2013 (BRASIL, 2013), que dispõe sobre a contratação no comércio eletrônico.

O referido decreto é, nos dizeres da doutrina, “um instrumento importantíssimo nas relações de consumo realizadas à distância”, tendo como pilares centrais a exigência de: (i) informações claras sobre o produto, serviço e do fornecedor; (ii) atendimento facilitado ao consumidor; e (iii) respeito ao direito

6. O CDC conceitua fornecedor como “toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços” no seu artigo 3º. (BRASIL, 1990).

7. Rede mundial de computadores ou *world wide web* (www), foi o protocolo que permitiu que navegadores conseguissem acessar informações em *websites*, tornando a internet acessível a pessoas comuns. (HELENA, 2019).

de arrependimento (LOSSIO, 2021, p. 138).

Este artigo discute como as *dark patterns* nas contratações eletrônicas são vistas pelo Direito do Consumidor e quais as suas repercussões. Nessa perspectiva, para alguns autores, “Um das principais discussões envolve o limite existente entre o desenvolvimento de um *design* persuasivo e a necessidade de transparência para que o consumidor consiga apresentar o seu consentimento de forma livre” (COUTO, 2021).

Isso acontece porque a dinâmica da informação, a maneira pela qual os produtos, serviços e até mesmo como os fornecedores se apresentam para os consumidores são fatores bastante importantes, especialmente sob a ótica do dever de informação e do princípio da transparência.

As *dark patterns* tentam justamente provocar um comportamento não natural no consumidor em prol do benefício de fornecedores, o que vai de encontro à esfera protetiva do consumidor sob vários aspectos que serão detalhados, em especial por potencializar uma situação de vulnerabilidade eletrônica e por violar o dever de informação e o princípio da confiança, além de caracterizar uma prática comercial abusiva.

2.1 Vulnerabilidade eletrônica

O artigo 4º inciso I do CDC prevê expressamente a vulnerabilidade do consumidor no mercado de consumo (BRASIL, 1990). Isso significa que há um reconhecido desequilíbrio entre consumidor e fornecedor, pois é este que detém os meios de produção, o que justifica uma tutela especial do consumidor, parte mais frágil e vulnerável nessa relação (GOMES, 2016, p. 40).

Tradicionalmente, a doutrina trata a vulnerabilidade do consumidor sob os seguintes aspectos: (i) técnico, pois o consumidor não possui conhecimento técnico do produto ou serviço que contrata; (ii) jurídico, uma vez que o consumidor não tem conhecimento jurídico para compreender os termos do contrato e suas repercussões, além de ter maiores dificuldades de defender seus interesses em juízo; (iii) fático ou socioeconômico, porque o consumidor não detém o mesmo poder econômico do fornecedor; e (iv) informacional, que significa que o consumidor não tem informações completas e suficientes sobre produtos e serviços ofertados no mercado de consumo (GOMES, 2016, p. 40).

No tocante à vulnerabilidade informacional, os autores defendem a importância da aparência, da comunicação e da informação no mercado de consumo que é cada vez mais visual, rápido e de risco (MARQUES, 2019, p. 325).

Contudo, é muito pertinente o alerta da professora Cláudia Lima Marques ao afirmar que “Hoje, porém, a informação não falta, ela é abundante, mani-

pulada, controlada e, quando fornecida, nos mais das vezes, desnecessária” (MARQUES, 2019, p. 325). Todo esse excesso de informação faz com que o consumidor não perceba muitas vezes as informações verdadeiramente úteis (MORAES, 1999, p. 116).

Alguns autores ainda elencam a chamada vulnerabilidade biológica ou psicológica, segundo a qual o consumidor muitas vezes é levado a consumir produtos e serviços que jamais desejou anteriormente devido à enorme quantidade de informações a que é exposto por meio dos seus sentidos (visão, olfato e paladar). Em suma, o consumidor pode ter sua vontade limitada pela massiva imposição de publicidade, um dos marcos do comércio eletrônico (LIMA, 2013), que utiliza dinâmicas de pressão e estratégias altamente eficazes para levar o consumidor a contratar por impulso e sem reflexão.

Ademais, segundo parcela da doutrina, as relações de consumo pela internet trazem outros desafios e adicionam um novo tipo de vulnerabilidade, qual seja a vulnerabilidade eletrônica.

Isso ocorre porque o comércio eletrônico ou *e-commerce* tem suas peculiaridades. Primeiramente, há uma relativização do elemento volitivo das partes causada pela massificação de contratos de adesão na celebração via internet. Presencia-se também uma desterritorialização ou falta de territorialidade definida dos contratos, uma despersonalização da relação jurídica (não há qualquer contato com quem se negocia ou muitas vezes o negócio é realizado por um dispositivo automático) e uma desmaterialização do meio de contratação (não existe um meio físico, material) (LIMA, 2013).

A produção passa a ser mundial, desterritorializando-se e despersonalizando-se as relações e o *marketing* e os mercados não possuem mais fronteiras. O meio virtual, conectado vinte e quatro horas por dia, permite o envio de mensagens e *e-mails* a qualquer momento, provocando alterações significativas nos hábitos de consumo com a agilidade na troca de informações e a expansão das possibilidades de publicidade (BENJAMIN, 2009, p. 39).

Nesse sentido, “Agora há apenas uma rede sem fim e sem fio de sujeitos intervenientes (portal, *website*, link, *provider* dentre outros) entre os contratantes, de maneira que o consumidor não tem como saber com quem está contratando” (LIMA, 2013).

Há, portanto, um substancial incremento nos riscos de contratos firmados via internet, pois em geral são contratos de adesão, com opção de apenas um clique para concordar com os termos, comumente do tipo “li e aceito”. Essa dinâmica normalmente não permite que o consumidor leia atentamente as cláusulas

sulas e condições, passando muito facilmente para a fase seguinte sem saber ao certo o conteúdo daquela contratação (LIMA, 2013).

Tanto é assim, que adveio o Decreto 7.962/2013 (BRASIL, 2013), que regulamenta o CDC e dispõe sobre a contratação no comércio eletrônico para tentar preencher essa lacuna.

Alguns autores defendem, inclusive, a necessidade de aprovação de uma norma legislativa que inclua no CDC uma nova sessão para dispor sobre o regime do comércio eletrônico (MARQUES, 2019, p. 1000).

Finalmente, vale ainda ressaltar que, além da vulnerabilidade “geral” ou standard prevista no inciso I do artigo 4º do CDC, a doutrina e a jurisprudência também trazem a hipervulnerabilidade ou vulnerabilidade agravada, que ocorre em situações sociais, fáticas e objetivas que aprofundam a vulnerabilidade do consumidor por circunstâncias pessoais aparentes ou conhecidas pelo fornecedor, tais como idade reduzida ou avançada, incapacidade, analfabetismo, doença etc (MARQUES, 2019, p. 350-352).

Nesse cenário, há pessoas que não distinguem claramente o que é um banner de publicidade e o que é uma compra, fazendo-as clicar em um botão comprar e contratando sem que tivessem a intenção de fazê-lo. Essas são, lamentavelmente, situações corriqueiras com idosos (BRASIL, 2003) e crianças (BRASIL, 1990), por exemplo, pessoas consideradas hipervulneráveis pela legislação pátria.

2.2 Dever de informação

O dever de informação decorre diretamente do princípio básico da transparência previsto no artigo 4º, *caput*, do CDC, pois a transparência pode ser entendida como o fornecimento de informação clara, correta e precisa acerca do produto a ser vendido ou do serviço a ser contratado e das cláusulas e condições do contrato a ser celebrado, além de lealdade e respeito na relação entre fornecedores e consumidores, seja na fase contratual seja na fase pré-contratual (MARQUES, 2019, p. 815).

Existe tanto um dever de informação para o fornecedor quanto um direito do consumidor de ser adequadamente informado (BENJAMIN, 2009, p. 58-59), pois “ao dever jurídico imposto a um indivíduo [...] corresponde um direito subjetivo assegurado a outro indivíduo ou ente” (MARQUES, 2019, p. 834).

Essa proteção na fase pré-contratual provoca uma regulação também da oferta ou da manifestação dos fornecedores para atrair o consumidor para a

relação contratual. É nesse momento que muitas vezes são adotadas as *dark patterns* como estratégias mercadológicas.

Esse entendimento fica claro no trecho:

Como nem todos os contatos entre fornecedor e consumidor levam ao estabelecimento de relações contratuais, a transparência deve ser uma nova e necessária característica de toda manifestação pré-contratual do fornecedor no mercado, desde a sua publicidade, vitrines, o seu marketing em geral, suas práticas comerciais, aos contratos ou às condições gerais contratuais que pré-redige, às informações que seus prepostos e representantes prestam etc. o que bem demonstra a abrangência do novo mandamento (MARQUES, 2019, p. 819).

Sob essa ótica, o CDC, no seu artigo 6º, inciso III, prevê o direito básico de o consumidor ter “a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem” (BRASIL, 1990).

Dizer que a informação deve ser adequada significa que ela deve ser completa. Já dizer que a informação deve ser clara é no sentido de que ela deve ser compreendida facilmente pelo consumidor (GOMES, 2016, p. 55). O uso de uma linguagem simples (A LINGUAGEM, s.d.), por exemplo, é um excelente recurso para que a informação prestada seja verdadeiramente clara.

Trata-se de direito de o consumidor ter todas as informações relevantes para aquela futura contratação, começando pelas informações sobre as características do produto ou do serviço e passando pelo conteúdo do próprio contrato (MARQUES, 2019, p. 815).

No tocante às informações sobre os preços de produtos e serviços, disciplinadas pelo Decreto 5.903/2006 (BRASIL, 2006), a necessidade de informações adequadas e claras significa que devem ser prestadas com correção, clareza, precisão, ostensividade e legibilidade. Aponto para o mandamento legal da clareza, que impõe que as informações devem ser compreendidas facilmente e de imediato pelo consumidor, sem que haja qualquer necessidade de interpretação ou cálculo nem abreviações ou termos que dificultem a sua compreensão (MAGRO, 2021, p. 4069).

O Decreto 7.962/2013 (BRASIL, 2013) igualmente dispõe sobre o dever de informação previsto no CDC, mas vai além e exige informação clara e adequada do fornecedor.

Tal medida merece aplausos, pois os *marketplaces* têm vários fornecedores diferentes, de locais distintos. O consumidor deve ser informado com quem é realizada aquela contratação, até mesmo porque a dinâmica de uma eventual devolução é diferente quando os fornecedores não são o próprio *website* acessado.

Seus objetivos são trazer uma transparência ainda maior ao consumidor (LOSSIO, 2021, p. 139), mitigar eventuais abusos por parte dos fornecedores e permitir que os consumidores exerçam seus direitos validamente, inclusive com a defesa em juízo se for preciso (MAGRO, 2021, p. 406).

É notório que o CDC previu uma série de novos deveres para o fornecedor que faz uso de publicidade no mercado como estratégia comercial e de incitação ao consumo. Dentre esses deveres está o dever de “veracidade especial” segundo a jurisprudência do Superior Tribunal de Justiça (STJ), que determina que, muito embora o fornecedor não seja obrigado a trazer nenhuma informação precisa na sua publicidade, caso o faça e traga alguma informação sobre o produto ou serviço ou sua qualidade ou preço, quantidade, riscos etc., essa informação deve ser verdadeira (MARQUES, 2019, p. 837).

Isso ocorre porque já existe vínculo entre as partes mesmo antes da celebração da relação obrigacional, ainda que esse dever de conduta seja apenas cooperar, informar, não inviabilizar o negócio. São os ditos deveres anexos à relação jurídica (MARQUES, 2019, p. 835).

Logo, fica clara o quão importante é a observância do dever de informação para as relações de consumo e como o uso das *dark patterns* retira a clareza das informações prestadas ao consumidor, inclusive induzindo-o a comportamentos que naturalmente não adotaria, violando, assim, seus direitos.

2.3 Proteção contra práticas abusivas

Vale lembrar que também há uma proteção expressa do consumidor contra práticas abusivas do mercado de consumo no art. 6º, inciso IV do CDC. Ela engloba práticas abusivas por meio da publicidade, de práticas comerciais ou de cláusulas contratuais (GOMES, 2016, p. 56).

Dispõe o CDC: “São direitos básicos do consumidor: [...]IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços” (BRASIL, 1990).

Segundo a doutrina as normas que vedam as cláusulas e práticas abusivas buscam restabelecer o equilíbrio da relação, da força da vontade e das expec-

tativas legítimas, o que igualmente compensaria a vulnerabilidade fática do consumidor (BENJAMIN, 2009, p. 59-60).

Para o eminente ministro Antônio Hermam V. Benjamim (2009, p. 216-217) a prática abusiva em sentido amplo pode ser compreendida como a “desconformidade com os padrões mercadológicos de boa conduta em relação ao consumidor”. Porém, “[...] prática abusiva no Código é apenas aquela que, de modo direto e no sentido vertical da relação de consumo (do fornecedor e do Consumidor), afeta o bem-estar do consumidor”.

Sendo assim, pelo conceito do próprio criador da expressão Harry Brignull, as *dark patterns* enquanto truques usados em sites e aplicativos que fazem o usuário fazer coisas que eles não tinham a intenção, tal como comprando ou se inscrevendo em algo (tradução livre) (BRIGNULL, s.d.), podem ser consideradas práticas abusivas do fornecedor.

Até mesmo porque vale lembrar que o rol de práticas abusivas trazido no CDC é meramente exemplificativo de acordo com a doutrina dominante, algo que não poderia ser diferente por conta das inúmeras mudanças no mercado de consumo e sua extrema rapidez (BENJAMIN, 2009, p. 218).

2.4 Princípio da confiança

Por último temos o princípio da confiança, que, apesar de não ser previsto expressamente no CDC, é considerado pela doutrina como um “princípio implícito” que permeia todo o ordenamento (SCHMIDT NETO, 2019, p. 195) ou “um dos mais importantes princípios do direito privado” (MIRAGEM, 2013, p. 229) ou, ainda, “uma irradiação normativa da boa-fé e [...] ligado diretamente ao princípio da transparência” (LIMA, 2014).

A ideia genérica de confiança enquanto convicção ou segurança em relação a alguma coisa ou crença na retidão moral, no caráter e na lealdade de uma outra pessoa (CONFIANÇA, 2021) pode ou não merecer proteção no nosso ordenamento jurídico. Isso porque se protege a confiança legítima, ou seja, a confiança justificada pelas circunstâncias e, ao fazê-lo, protege-se igualmente as legítimas expectativas (SCHMIDT NETO, 2019)⁸.

A confiança legítima também justifica a vinculabilidade das partes à relação jurídica porque é a confiança ou será a causa da contratação ou ao menos representará uma influência decisiva para ela (SCHMIDT NETO, 2019).

8. No direito comparado, a doutrina elenca alguns elementos que aferem a legitimidade da expectativa, tais como: (i) confiança ter sido despertada pela conduta alheia, (ii) ser justificada, (iii) ter ocorrido uma espécie de “investimento de confiança”, e (iv) ter sido frustrada a expectativa criada. (SCHMIDT NETO, 2019, p 203).

O problema é que vivemos uma crise de legitimação ou de confiança cuja origem seria a terceira revolução industrial e a globalização da economia, pois estas trouxeram uma nova forma de consumir, mais rápida, mais impessoal, sem barreiras territoriais a partir de uma produção mundial, sem fronteiras e de um meio virtual sempre conectado (BENJAMIN, 2009, p. 39).

Há um aprofundamento ainda maior da crise de confiança quando se trata de comércio eletrônico, uma vez que:

Como toda contratação a distância, o comércio eletrônico causa certo receio diante da impossibilidade de tocar ou visualizar o objeto da relação negocial, A impessoalidade dessa forma de contratação projeta a relevância da confiança para um nível ainda maior do que nos contratos tradicionais. Não se pode mais imaginar uma relação interpessoal no mundo virtual 'sem que haja um mínimo de colaboração entre as partes' (SCHMIDT NETO, 2019, p. 211).

Por isso a doutrina aponta para uma tendência de se mitigar a importância do princípio da autonomia da vontade em prol do princípio da confiança, principalmente nesse contexto de massificação das relações, de despersonalização e de anonimato (SCHMIDT NETO, 2019, p. 199).

Como o princípio da proteção da confiança legítima vai além e valora o resultado prático, se abusivo ou não, e não mais apenas a conduta das partes, ao privilegiá-lo mitigar-se-ia o aprofundamento da posição de vulnerabilidade do consumidor, ao menos parcialmente (BENJAMIN, 2009, p. 39).

Diante do exposto, a utilização de padrões obscuros em aplicações *online* igualmente viola o princípio da confiança, pois frustra as legítimas expectativas do consumidor ao induzi-lo a um comportamento não natural e que beneficia, mormente, o fornecedor.

Considerações finais

A utilização de padrões obscuros ou *dark patterns* no *design* de *websites* e aplicativos é, portanto, uma questão que transpassa os debates sobre a ética e o mau uso pelo *designer* responsável pela aplicação. Trata-se de uma prática com repercussões jurídicas, especialmente em se tratando de contratações pela internet envolvendo, de um lado, o consumidor e, de outro, o fornecedor.

Dentre as implicações jurídicas trazidas pelas *dark patterns*, abordamos especificamente as questões acerca da vulnerabilidade eletrônica, do dever de informação por parte do fornecedor, do direito básico do consumidor contra práticas comerciais abusivas e, em derradeiro, do princípio da confiança.

Conclui-se que as *dark patterns* agravam o quadro de vulnerabilidade (a eletrônica segundo parcela da doutrina) do consumidor, ferem o direito de informação do consumidor e o princípio da confiança e se enquadram como uma prática comercial abusiva, conduta esta rechaçada pelo nosso ordenamento jurídico.

Dessa forma, entende-se como melhor caminho a necessária conscientização dos consumidores sobre essa prática, bem como a devida punição dos fornecedores que insistem em utilizá-la. Somente com esse trabalho conjunto de promoção à cidadania digital dos usuários consumidores e de penalização para os fornecedores que descumprirem os mandamentos legais consumeristas que haverá uma relação jurídica mais equilibrada e transparente entre os sujeitos do mercado de consumo.

Referências

AGUIAR, Karelina Staut de. *Visual Law: como a experiência do Direito pode ser aprimorada*. In: SOUZA, Bernardo de Azevedo e; OLIVEIRA, Ingrid Barbosa. *Visual Law: como os elementos visuais podem transformar o direito*. 1 Edição. São Paulo: Thomson Reuters Brasil, 2021.

A LINGUAGEM SIMPLES. Comunica Simples, 2021. Disponível em: <<https://comunicasimples.com.br/a-linguagem-simples/>>. Acesso em 7 de janeiro de 2022.

A SPOTLIGHT ON DARK PATTERNS. Testimonium, 2021. Disponível em: <<https://testimonium.co/>>. Acesso em 5 de janeiro de 2022.

BENJAMIN, Antônio Herman; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. *Manual de Direito do Consumidor*. 2 ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2009.

BRIGNULL, Harry. *Dark Patterns: inside the interfaces designed to trick you*. Disponível em: <<https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you>>. Acesso em 30 de dezembro de 2021.

_____. *What are dark patterns?* Disponível em: <https://www.darkpatterns.org/>. Acesso em 5 de janeiro de 2022.

CONFIANÇA. Dicio Dicionário Online de Português, 2021. Disponível em: <<https://www.dicio.com.br/confianca/>>. Acesso em 3 de janeiro de 2022

COUTO, Ana. *Dark Patterns em UX: uma interface entre o design e a proteção de dados*. Sem Processo, 2021. Disponível em: <<https://www.semprocesso.com.br/post/dark-patterns-ux-design-e-protacao-de-dados>>. Acesso em 30 de dezembro de 2021.

DADOS DE ECOMMERCE NO BRASIL: CONFIRA OS PRINCIPAIS NÚMEROS DO COMÉRCIO ELETRÔNICO. Resultados Digitais, 2021. Disponível em: <<https://resultadosdigitais.com.br/blog/dados-de-ecommerce-no-brasil/>>. Acesso em 30 de dezembro de 2021.

DELIBERATION OF THE RESTRICTED COMMITTEE NO. SAN-2021-023 OF 31 DECEMBER 2021 CONCERNING GOOGLE LLC AND GOOGLE IRELAND LIMITED. CNIL, 2021. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf>. Acesso em 13 de abril de 2022.

GUIDELINES 3/2022 ON DARK PATTERNS IN SOCIAL MEDIA PLATFORM INTERFACES: HOW TO RECOGNISE AND AVOID THEM. EDPB, 2022. Disponível em: <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en>. Acesso em 13 de abril de 2022.

GOMES, Nathália Stivalle. *Direito do Consumidor*. 1 ed. Salvador: Editora JusPodivm, 2016.

HELENA, Ligia. *Rede mundial de computadores (o www!) completa 30 anos e ganha homenagens*. Claudia, 2019. Disponível em: <<https://claudia.abril.com.br/sua-vida/rede-mundial-de-computadores/>>. Acesso em 1º de janeiro de 2022.

INFORMATION COMMISSIONER'S OPINION: DATA PROTECTION AND PRIVACY EXPECTATIONS FOR ONLINE ADVERTISING PROPOSALS. ICO, 2021. Disponível em: <<https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf>>. Acesso em 13 de abril de 2022.

INTERFACE INTERFERENCE. UXP Dark Patterns, 2018. UXP Dark Patterns, c2022. Disponível em: <<https://darkpatterns.uxp2.com/patterns-2/interface-interference/>>. Acesso em 30 de dezembro de 2021.

KOVACS, Leandro. *O que é dark pattern em aplicativos e sites? 5 exemplos*. Tecnoblog, s.d. Disponível em: <<https://tecnoblog.net/responde/o-que-e-dark-pattern-em-aplicativos-e-sites-5-exemplos/>>. Acesso em 30 de dezembro de 2021.

LIMA, Maria Renata Barros de. *A vulnerabilidade do consumidor no e-commerce*. Jus, 2013. Disponível em: <<https://jus.com.br/artigos/24601/a-vulnerabilidade-do-consumidor-no-e-commerce>>. Acesso em 2 de janeiro de 2021.

LIMA, Rafaela Silva. *A Relação Jurídica de consumo em consonância com o Princípio da Confiança*. Jus, 2014. Disponível em: <<https://jus.com.br/artigos/33939/a-relacao-juridica-de-consumo-em-consonancia-com-o-principio-da-confianca>>. Acesso em 3 de janeiro de 2021.

LÓSSIO, Claudio Joel Brito. *Manual Descomplicado de Direito Digital: Guia para Profissionais do Direito e da Tecnologia*. 2 ed. rev., atual. e ampl. São Paulo: Editora JusPodivm, 2021.

MAGRO, Américo Ribeiro; SOUZA, Landolfo Andrade de. *Manual de Direito Digital*. 1 ed. Salvador: Editora JusPodivm, 2021.

MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 9. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2019.

MEYER, David. *France cracks down on dark patterns, fining Google and Facebook nearly \$240 million for manipulative cookie tricks*. Fortune, 2022. Disponível em: <<https://fortune.com/2022/01/06/france-cookie-law-facebook-google/>>. Acesso em 13 de abril de 2022.

MIRAGEM, Bruno Nubens Barbosa. *Curso de Direito do Consumidor*. 4 ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2013.

MORAES, Paulo Valério Dal Pai. *Código de Defesa do Consumidor O princípio da vulnerabilidade*-. Porto Alegre: Síntese, 1999.

NICOLL, Alyssa. *Dark Patterns in UX*. Progress Telerik, 2020. Disponível em: <<https://www.telerik.com/blogs/dark-patterns-ux>>. Acesso em 30 de dezembro de 2021.

O QUE É DARK PATTERN UX E PORQUÊ EVITÁ-LO. Homem Máquina, 2020. Disponível em: <<https://www.homemmaquina.com.br/o-que-e-dark-pattern-ux-e-porque-evita-lo/>>. Acesso em 30 de dezembro de 2021.

POP-UP. Infopédia Dicionários Porto Editora, c2003-2022. Disponível em: <<https://www.infopedia.pt/dicionarios/lingua-portuguesa/pop-up>>. Acesso em 7 de janeiro de 2022.

SAIBA COMO FUNCIONA UM ALGORITMO E CONHEÇA OS PRINCIPAIS EXEMPLOS EXISTENTES NO MERCADO. Rockcontent, 2021. Disponível em: <<https://rockcontent.com/br/blog/algoritmo/>>. Acesso em 30 de dezembro de 2021.

SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2 ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2019

SHAPING CHOICES IN THE DIGITAL WORLD FROM DARK PATTERNS TO DATA PROTECTION: THE INFLUENCE OF UX/UI DESIGN ON USER EMPOWERMENT. IP REPORTS INNOVATION AND FORESIGHT N°06. LINC.CNIL, 2019. Disponível em: <https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf>. Acesso em 13 de abril de 2022.

SILVEIRA, Daniel. *Pandemia faz triplicar número de brasileiros que compram produtos domésticos pela internet, diz Serasa*. G1, 2020. Disponível em: <<https://g1.globo.com/economia/noticia/2020/10/20/pandemia-faz-mais-brasileiros-comprarem-produtos-domesticos-pela-internet-aponta-serasa.ghtml>>. Acesso em 30 de dezembro de 2021.

SIQUEIRA, André. *Call to Action: tudo o que você precisa saber sobre CTA*. Resultados Digitais, 2020. Disponível em: <<https://resultadosdigitais.com.br/blog/tudo-sobre-call-to-action/>>. Acesso em 9 de janeiro de 2022.

SOUZA, Natan. *O que é Dark Pattern UX e até onde deveríamos ir*. Dicas UX, s.d. Disponível em: <<https://www.dicasux.com.br/ux/o-que-e-dark-patterns-ux/>>. Acesso em 30 de dezembro de 2021.

TARDELLI, Andre. *Dark Patterns em UX: Conhecendo os padrões obscuros das interfaces*. Alura, 2020. Disponível em: <<https://www.alura.com.br/artigos/dark-patterns-em-ux>>. Acesso em 30 de dezembro de 2021.

TAXA DE CONVERSÃO: O QUE É E COMO CALCULAR? Resultados Digitais, 2020. Disponível em: <<https://resultadosdigitais.com.br/blog/o-que-taxa-de-conversao/>>. Acesso em 5 de janeiro de 2022.

UX DO MAL: 5 EXEMPLOS DE DARK PATTERNS PARA FICAR DE OLHO. Digital House, 2021. Disponível em: <<https://www.digitalhouse.com/br/blog/dark-patterns>>. Acesso em 30 de dezembro de 2021.

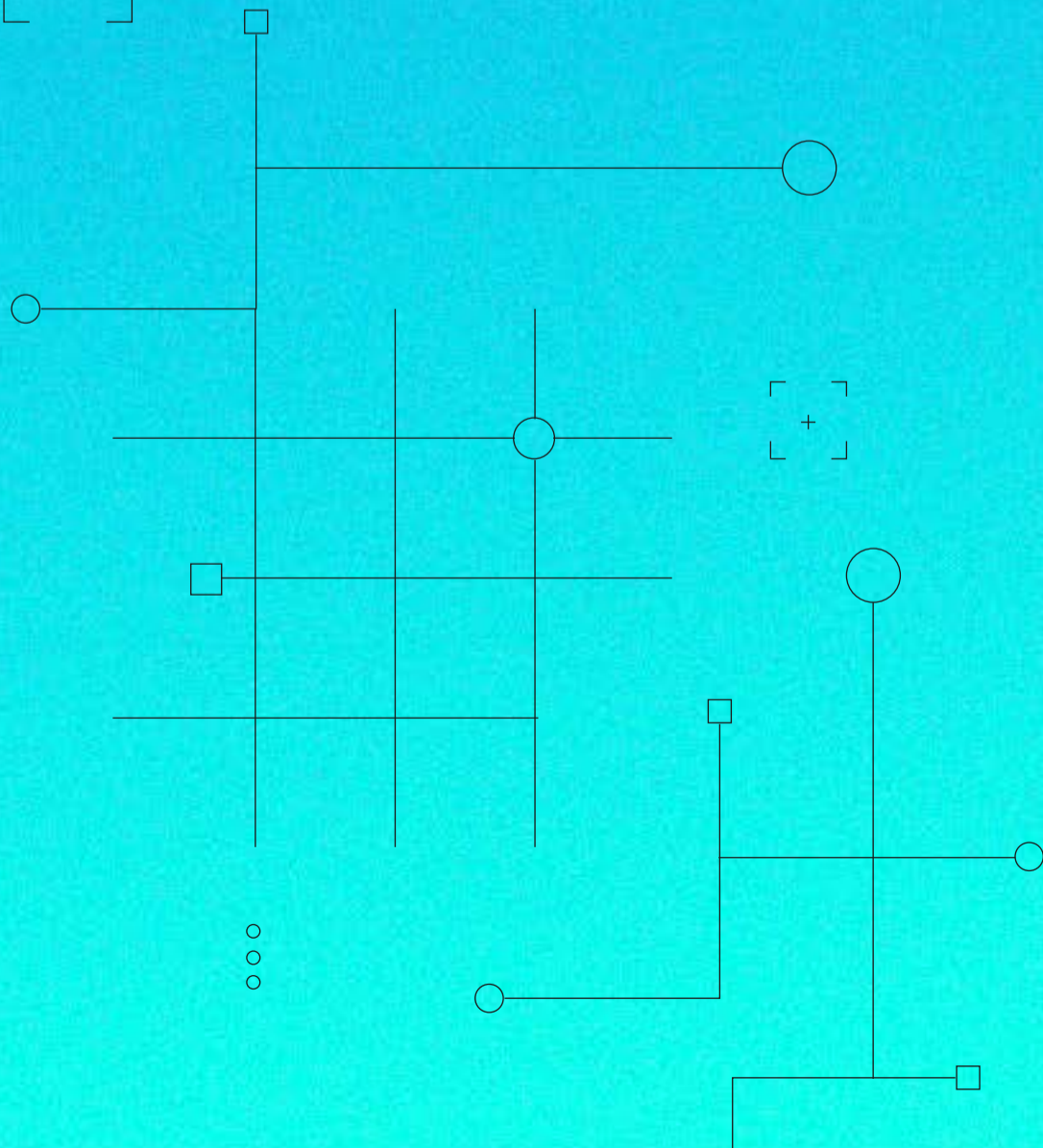
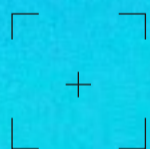
VARGAS, Mariana. *Dark Patterns nas aplicações que usamos todos os dias*. UX Collective BR, 2021. Disponível em: <<https://brasil.uxdesign.cc/dark-patterns-nas-aplicacoes-que-usamos-todos-os-dias-f7a17f3afd85>>. Acesso em 30 de dezembro de 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

7

Riscos a direitos e liberdades fundamentais como baliza da proteção de dados pessoais

RAFAEL ROCHA PESSOA



Sumário: Introdução. 1. O risco como um elemento inerente ao tratamento de dados pessoais. 1.1. Visão prática sobre o conceito de risco em proteção de dados. 1.2. A regulação do instrumento para a avaliação do risco em proteção de dados. 2. A tutela dos direitos e liberdades fundamentais. 2.1. A baliza da proteção de dados baseada na aferição de risco a direitos e liberdades fundamentais. 2.2. O direito à proteção de dados pessoais como um direito fundamental autônomo. Considerações finais. Referências.

Introdução

O surgimento de diferentes normas relacionadas à privacidade e à proteção de dados pessoais nas últimas décadas trouxe consigo uma crescente noção na sociedade sobre a relevância da adequada proteção e uso de informações sobre pessoas naturais. Em uma camada mais superficial, tal noção faz com que as pessoas tenham cada vez mais expectativa de que seus dados sejam mantidos em segurança, com a promessa de confidencialidade, e sejam acessados apenas por pessoas e organizações que efetivamente precisem acessá-los.

Embora a segurança da informação seja um pilar de fundamental relevância para a efetiva proteção de dados pessoais, a inobservância de outras questões aparentemente menos tangíveis aos titulares – e que vão além da organização da segurança implementada pelos agentes de tratamento – podem, em situações específicas, expor titulares de dados a riscos e danos relevantes, independentemente do uso dos mais avançados padrões de segurança, sobretudo em uma realidade cada vez mais movida a dados. É nesse sentido que, no bojo dos mais avançados textos normativos relacionados ao tema, a tutela adequada dos direitos e liberdades fundamentais se mostra tão relevante.

A forma como o conjunto de normas relacionadas à proteção de dados encapsula a proteção dos direitos e liberdades fundamentais está atrelada à noção de que tais direitos e liberdades podem estar expostos a riscos relevantes

1. Advogado com dez anos de experiência em temas na intersecção entre direito e tecnologia, graduado em Direito pela Universidade Presbiteriana Mackenzie, pós-graduando em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro, candidato a LLM em Direito e Tecnologia na Tilburg University, especialista em Privacidade e Proteção de Dados pelo Data Privacy Brasil, bem como em Propriedade Industrial, Gestão de Propriedade Intelectual e Direitos Autorais pela Organização Mundial da Propriedade Intelectual (OMPI) e pela Harvard Law School. Membro da International Association of Privacy Professionals (IAPP), designado como Fellow of Information Privacy (FIP) e certificado como um profissional especialista na legislação de proteção de dados da União Europeia (CIPP/E) e como um gestor de programas de privacidade (CIPM).

no contexto do tratamento de dados pessoais. Ocorre que o conceito de risco aplicado à proteção de direitos e liberdades fundamentais invariavelmente exige do intérprete da norma um exercício complexo de reflexão sobre as mais variadas possibilidades de ameaça aos direitos e liberdades das pessoas.

Evidentemente, tal reflexão depende da compreensão do intérprete sobre *quais são* os direitos e as liberdades garantidas às pessoas no ordenamento jurídico aplicável ao tratamento de dados realizado e *como o uso de dados pessoais pode ameaçar* tais direitos e liberdades. É justamente essa complexidade que pode dificultar que agentes de tratamento realizem avaliações precisas e efetivamente alinhadas à legislação vigente, notadamente quando tais agentes estiverem primariamente comprometidos com a mitigação de riscos à sua própria atividade.

Na prática, essa complexa avaliação deve servir para produzir efeitos diretos na tomada de decisão de uma organização sobre o que ela pode ou não fazer com dados pessoais, haja vista que, à luz da legislação brasileira, a efetiva existência de riscos aos direitos e liberdades fundamentais pode, em determinados casos, acabar por tornar uma atividade de tratamento de dados pessoais ilegítima. Como então tomar as medidas necessárias ao efetivo cumprimento das obrigações relacionadas à proteção de dados pessoais, garantindo que, para além da verificação de requisitos de segurança e conformidade, direitos e liberdades individuais sejam compreendidos e adequadamente respeitados?

1. O risco como um elemento inerente ao tratamento de dados pessoais

O conceito de risco pode guardar diferentes significados em diferentes contextos. Para os propósitos do presente estudo, interessa particularmente o entendimento do significado do risco no âmbito da proteção de dados pessoais, risco este que pode se relacionar com diferentes resultados como consequência do tratamento de dados pessoais, dentre os quais se destacam, de um lado, o *risco regulatório* – tomado pelo agente de tratamento ao determinar como deve se dar o tratamento, visando à não violação de suas obrigações neste contexto – e, de outro, o *risco aos direitos e liberdades fundamentais*, assumido pela pessoa natural ao ter seus dados pessoais tratados pelos agentes de tratamento.

Na prática organizacional de empresas, é comum ver – especialmente em momentos de transformação normativa e cultural, como o atual momento do

Brasil em vista da recente vigência plena da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) – um enfoque quase que exclusivo com relação à mitigação do *risco regulatório*. Tal abordagem privilegia o estabelecimento de medidas técnicas e administrativas para evitar que a organização viole as obrigações legais e regulatórias a ela aplicáveis, sobretudo com o objetivo de evitar a sua responsabilização.

Embora compreensível através das lentes de autopreservação do agente de tratamento, tal abordagem predominantemente voltada à mitigação do risco regulatório tem grande potencial de gerar um verdadeiro conflito com a natureza das leis de proteção de dados. Isso porque referida abordagem, ao invés de centralizar os esforços da organização na avaliação dos impactos de suas atividades aos direitos dos titulares, privilegia tão somente uma aferição do risco a que a organização está exposta – e que está disposta a assumir – em vista da sua própria necessidade de cumprir e demonstrar cumprimento das obrigações a ela impostas pela regulamentação.²

A contemplação quanto ao risco regulatório está, portanto, ligada ao interesse da organização em cumprir deveres formais que a auxiliem na demonstração – seja proativa, com o estabelecimento de evidência de seus esforços, seja reativa, em caso de questionamento sobre sua conduta – de tal cumprimento. Trata-se de abordagem que deriva de expresse requisito legal previsto na LGPD,³ mas que abarca apenas uma fração – mais formal do que material – da efetiva responsabilidade assumida pelo agente de tratamento.

É exatamente neste sentido que Gomes (2020, p. 259) tece sua crítica:

Avaliar riscos se transformou numa tarefa pura e simples de checar conformidade com a Lei, avaliando se as operações de tratamento de dados possuem base legal, se elas atendem aos princípios, se os dados estão sendo eliminados ao final do tratamento, tudo isso, para mitigar o risco de sanções e para demonstrar *accountability*. Ou seja, uma empreitada muito mais voltada ao risco (regulatório) da organização que trata dados pessoais, do que um exercício de mensuração dos possíveis efeitos adversos para o titular dos dados.

2. Neste sentido, ver GOMES (2020, p. 246).

3. LGPD, artigo 6º, X: “responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.”

No entanto, embora a contemplação do risco regulatório inerente à atividade de tratamento de dados pessoais seja uma realidade que invariavelmente modula a tomada de medidas dentro de uma organização, é certo que o propósito de se garantir direitos sobre dados pessoais está muito mais intrinsecamente relacionado à *proteção da pessoa natural* – titular dos dados – e não dos interesses organizacionais do agente de tratamento.⁴ Isso porque, ao fim e ao cabo, o próprio risco regulatório assumido pelo agente de tratamento só existe em razão da existência do próprio risco que suas atividades podem causar aos titulares dos dados tratados. Assim, tem-se que, pela ótica da proteção de dados, caso não houvesse risco aos titulares, tampouco haveria risco ao agente de tratamento.

Feita esta necessária distinção quanto à natureza do risco mais relevante à disciplina da proteção de dados pessoais, resta entender o que os agentes de tratamento devem, de fato, considerar ao avaliar os potenciais impactos de suas atividades de tratamento de dados. Para fazê-lo, é necessário primeiro entender do que se tratam os riscos aos titulares no âmbito da proteção de dados e como estes riscos podem ser avaliados.

1.1 Visão prática sobre o conceito de risco em proteção de dados

Como muito bem sintetizado por Gellert (2017, p. 2), pode-se afirmar, para os propósitos do presente estudo, que o risco tem dois significados – um de ordem vernacular e outro de ordem técnica. No sentido vernacular, o risco se refere a um possível perigo futuro; já no técnico, o risco assume uma noção dupla vinculada à previsão de eventos futuros e à tomada de decisões baseada nos resultados de tal previsão. Partindo dessa premissa, conclui-se que o agente de tratamento deve ser capaz de não só tomar decisões sobre o tratamento de dados que realizará – consequência lógica do próprio ato de tratar dados –, como também ser capaz de, *previamente* à tomada dessas decisões, prever possíveis eventos futuros decorrentes do tratamento que realizará.

Evidencia-se, nesse contexto, um dever que vai muito além de examinar a norma vigente e avaliar se as práticas adotadas pelo agente de tratamento a ela se adequam do ponto de vista formal – razão pela qual a crítica à visão

4. O aparente conflito entre os dois objetivos de um agente de tratamento com relação à aferição de riscos (regulatórios e aos titulares) também foi objeto de crítica no trabalho de QUELLE (2015).

organizacional que se limita a antever e prevenir riscos regulatórios se faz necessária. O dever maior do agente está, portanto, centralizado na necessidade de diligenciar para (i) prever eventos futuros que exponham o titular de dados a situações que impliquem ameaça aos seus direitos e liberdades fundamentais; e (ii) tomar decisões com relação a tais situações, sobretudo com vistas à minimização das eventuais ameaças identificadas.

Naturalmente, a diligência demandada do agente de tratamento será invariavelmente subjetiva, na medida em que caberá ao próprio agente fazer as avaliações de risco necessárias para satisfazer de forma adequada os requisitos legais aplicáveis. No entanto, apesar de natural, a subjetividade de tais análises pode trazer consequências desconhecidas aos direitos e liberdades que as leis de proteção de dados visam tutelar, sobretudo se o agente de tratamento aplicar metodologia de avaliação de riscos que se mostre incompatível com a necessária tutela de tais direitos e liberdades fundamentais – desfecho provável caso o agente de tratamento centralize seus esforços *apenas* na aferição do risco regulatório.

A complexidade deste conflito é potencializada em virtude do amplamente disseminado modelo de *metarregulação* observado na normatização da proteção de dados pessoais.⁵ Referido modelo surge em razão da impossibilidade de se estabelecer regulamentação efetiva *ex ante* a todo e qualquer cenário onde possa vir a existir ameaça ao direito tutelado, assim permitindo que autoridades reguladoras e entes regulados *colaborem* para a construção do cenário regulatório, exercendo forças dentro de suas respectivas competências outorgadas pelo próprio ordenamento.⁶ Como consequência, tem-se que quanto mais os agentes de tratamento tenderem a subverter o verdadeiro conceito de avaliação de riscos em proteção de dados – tão somente sob o viés do risco regulatório, por exemplo –, mais difícil será para desconstruir a normalidade dessa subversão, o que certamente ocorrerá em detrimento dos próprios direitos e liberdades cuja tutela se buscava com a regulação.

Parece, então, que o caminho a ser percorrido para garantir que os verdadeiros objetivos da regulamentação da proteção de dados pessoais sejam alcançados depende do consenso dos agentes reguladores e dos agentes regulados quanto à forma adequada de avaliação do risco em proteção de dados.

5. Sobre o tema da metarregulação no âmbito da proteção de dados, ver BINNS (2017, p. 19-31).

6. Sobre o tema, ver ZANATTA (2017).

Felizmente, as mais modernas leis existentes sobre o tema – dentre as quais está a LGPD – fornecem os contornos básicos para que a chegada a um consenso nesse sentido se torne uma tarefa um pouco mais factível.

1.2 A regulação do instrumento para a avaliação do risco em proteção de dados

Assumindo o papel de instrumento de maior relevância para a presente análise,⁷ o relatório de impacto à proteção de dados pessoais (RIPD) é definido na LGPD como a “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.⁸ Em tese, tal instrumento deve possibilitar que agentes de tratamento possam realizar avaliações documentadas e concretamente aprofundadas sobre contextos específicos de tratamento de dados pessoais com o objetivo de (i) mapear eventuais riscos aos direitos e liberdades dos titulares; e (ii) encontrar formas de mitigar tais riscos.

Embora as técnicas e metodologias para a elaboração de RIPDs ainda não estejam completamente claras no cenário regulatório brasileiro,⁹ já existem uma série de referenciais possíveis para a sua construção em linha com os fundamentos e princípios da legislação brasileira. Talvez o melhor exemplo neste sentido para o presente estudo seja o observado no contexto da União Europeia, onde o conceito de relatório de impacto à proteção de dados já foi – e continua sendo – objeto de ampla discussão e regulação.

O Regulamento (UE) 2016/679 – Regulamento Geral de Proteção de Dados da União Europeia (GDPR, no acrônimo em inglês) foi, em sua origem, muito mais prescritivo do que a LGPD na temática da avaliação de riscos decorrentes do tratamento de dados pessoais. O *Data Protection Impact Assessment* (DPIA), é o instrumento designado pelo regulamento para ser usado quando

7. Uma apertada, porém, detalhada síntese sobre o racional dos instrumentos relevantes ao tema pode ser vista em BINNS (2017, p. 5-8).

8. LGPD, artigo 5º, XVII.

9. A edição de regulamentos e procedimentos relacionados ao RIPD é de competência da Autoridade Nacional de Proteção de Dados (ANPD), de acordo com o artigo 55-J, XIII da LGPD. Por meio da Portaria nº 11 de 2021 (acessível em <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>), a ANPD publicou a sua agenda regulatória para o biênio 2021/2022 e inseriu a regulamentação do RIPD como uma das atividades a ser desenvolvida neste período. Até o momento da elaboração deste artigo, foram realizadas reuniões técnicas para a discussão do tema (disponíveis em <https://www.youtube.com/watch?v=DZH8Vgk6jJU&list=PLWiiz1AbXMPbDyyswWaSNWwlekfuQIBv>), mas não houve outros avanços em termos de discussão acerca do conteúdo do instrumento normativo que será editado.

“um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares”.¹⁰

O próprio artigo 35 do GDPR antecipa situações concretas em que o tratamento de dados pode, em regra, gerar riscos relevantes aos titulares, tal como o tratamento realizado no âmbito de uma avaliação de aspectos pessoais de pessoas naturais para a tomada de decisões que produzam efeitos jurídicos sobre a pessoa avaliada ou que a afetem significativamente de forma similar.¹¹ Tal situação se apresenta como hipótese em que o regulador reconheceu *de forma prévia* o risco inerente aos direitos e liberdades das pessoas, a exemplo de situações em que uma pessoa poderia ter o seu acesso a determinada oportunidade de trabalho ou concessão de crédito injustamente prejudicado em razão do tratamento automatizado de dados e registros diversos sobre si, como, por exemplo, informações sobre seus hábitos e comportamento de consumo.¹²

Em qualquer caso, é particularmente relevante à presente análise reforçar que, seja na legislação brasileira, seja na europeia, não existe obrigação que sugira que agentes de tratamento devam elaborar RIPDs para toda e qualquer atividade que depende de dados pessoais. Ao menos no contexto europeu, a linha da necessidade de tal instrumento é traçada na *probabilidade* de que determinado tratamento tem de causar alto risco aos direitos e liberdades de pessoas naturais.¹³

Diferentemente da lógica construída até o momento na legislação brasileira, o GDPR ainda foi além e estabeleceu que, uma vez elaborado o RIPD, caso o agente de tratamento verifique que, mesmo após tomadas as medidas disponíveis para mitigar os riscos identificados, ainda existam altos riscos aos direitos e liberdades fundamentais, a autoridade supervisora competente deve ser previamente *consultada* quanto à realização do tratamento almejado.¹⁴

10. GDPR, artigo 35.

11. GDPR, artigo 35.3(a).

12. A exemplo das situações examinadas em MONTEIRO (2018).

13. Nesse sentido, o Article 29 Working Party reforçou em suas diretrizes sobre o tema, ainda anteriormente à vigência do GDPR, que tal característica dos RIPDs estaria relacionada à abordagem baseada em riscos (*risk-based approach*) prevista no GDPR. Ver *Article 29 Working Party Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, revisada em 4 de outubro de 2017.

14. GDPR, Consideranda nº 84.

Embora no Brasil ainda não exista diretriz similar quanto aos gatilhos que podem tornar necessária a elaboração de um RIPD, é possível extrair do texto legal nacional a mesma intenção do texto europeu: proteger direitos e liberdades fundamentais.¹⁵ Assim, para além da complexidade referente ao desenvolvimento de uma metodologia para a avaliação de riscos relacionados ao seu tratamento de dados pessoais, tal constatação invariavelmente remete o intérprete da norma brasileira à necessidade de, no caso concreto, refletir sobre os possíveis impactos aos direitos e liberdades fundamentais das pessoas impactadas por suas atividades.

Assim, considerando que o entendimento – sobre quais são e qual a relevância – dos direitos e liberdades fundamentais pode estar, em muitos contextos, *desconectado* dos propósitos de conformidade almejados por uma organização sujeita a obrigações relacionadas à proteção de dados pessoais, faz-se necessário revisitar o significado de tais direitos, contextualizando-os à luz do direito à proteção de dados pessoais.

2. A tutela dos direitos e liberdades fundamentais

Reflexões sobre direitos e liberdades fundamentais evocam a ideia da existência de uma hierarquia entre direitos, estipulada sobretudo em vista dos diferentes valores de uma sociedade, subscritos em seus principais instrumentos normativos. No âmbito da União Europeia, é possível ver a sistematização dos direitos fundamentais na Carta de Direitos Fundamentais da União Europeia.¹⁶ No Brasil, observa-se a Constituição Federal de 1988¹⁷ (em maior destaque em seu artigo 5º) trazendo uma longa relação de direitos e garantias que refletem os valores aparentemente mais caros à sociedade, pavimentando o caminho para o estabelecimento do ordenamento jurídico a partir do racional definido por tais direitos e garantias.

A discussão concreta sobre os direitos e liberdades fundamentais é necessária para uma compreensão constitucionalmente adequada do regime de proteção de dados brasileiro. Como anteriormente discutido, o foco das

15. É o que se extrai da própria definição do RIPD, segundo o artigo 5º, XVII da LGPD.

16. Carta dos Direitos Fundamentais da União Europeia, acessível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf - acesso em 9 de janeiro de 2022.

17. Constituição Federal da República Federativa do Brasil de 1988, acessível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

avaliações de risco do agente de tratamento de dados deve ser identificar (e mitigar, conforme possível) eventuais ameaças aos direitos e liberdades das pessoas impactadas pela atividade de tratamento a ser realizada. Assim, uma análise de natureza constitucional deve ser realizada quando do planejamento de uma atividade de tratamento de dados.

Na prática, isso significa dizer que devem ser previstos – e medidos – os possíveis cenários em que uma pessoa possa vir a ter algum de seus direitos indevidamente prejudicado como resultado do tratamento de dados pessoais. Casos comuns neste sentido podem envolver situações como as que seguem:

Discriminação: determinada organização pode decidir consultar registros sobre as atividades de uma pessoa em uma rede social para inferir questões relacionadas ao seu posicionamento político e, com base em tal inferência, tomar decisão que afete substancialmente os interesses da pessoa, tal como desqualificá-la em um processo seletivo;¹⁸

Supressão da liberdade de expressão: uma organização responsável por operar determinada aplicação de internet baseada em interações sociais da sua comunidade de usuários pode decidir implementar procedimento automatizado para detectar certos padrões de linguagem utilizados nas mensagens dos usuários e, verificada a incidência em determinada regra pré-determinada na plataforma, realizar a eliminação sumária do conteúdo publicado;¹⁹

Óbice ao livre desenvolvimento da personalidade: uma plataforma de compartilhamento de conteúdo audiovisual que implementar técnicas para identificar os padrões de uso da aplicação por seus usuários com a intenção de lhes apresentar conteúdo direcionado que, além de servir ao propósito de fazer com que os usuários interajam mais com a plataforma, também permitam um nível relevante de entendimento (e exploração) de gatilhos psicológicos e emocionais com base na interpretação da forma como os usuários utilizam a plataforma e seu conteúdo, situação que pode abrir espaço para que seja possível antecipar e influenciar sentimentos e desejos com relação à percepção que seus usuários podem

18. Neste caso, a atividade teria o potencial não só de violar o princípio da não-discriminação previsto na LGPD (artigo 6º, IX), como também o direito fundamental à igualdade previsto no *caput* do artigo 5º da Constituição Federal. Além disso, a medida também pode ter reflexos indevidos sobre o direito ao livre exercício do trabalho (Constituição Federal, artigo 5º, XIII) e ao próprio direito social ao trabalho (artigo 6º, *caput*, Constituição Federal).

19. Tal medida é capaz de trazer evidentes riscos ao livre exercício da liberdade de expressão, direito fundamental consagrado no artigo 5º, IV da Constituição Federal.

ter de si mesmos e do mundo à sua volta, sobretudo quando os usuários da plataforma forem indivíduos mais suscetíveis a tal tipo de influência, como crianças, adolescentes e outros grupos vulneráveis.²⁰

Os casos exemplificados acima não têm qualquer pretensão de esgotar as complexas avaliações sobre os riscos a direitos e liberdades fundamentais que podem se mostrar necessárias na prática de uma organização, a depender do contexto em que dados podem ser usados. Tais casos apenas ilustram a constatação de que a preocupação do legislador não foi apenas no sentido de fazer com que os agentes de tratamento tivessem que garantir a *segurança* dos dados sob o seu controle, mas sobretudo que os agentes fossem compelidos a avaliar que tipo de consequência o *próprio tratamento* dos dados poderia trazer ao titular, ainda em uma situação em sequer exista risco relacionado à segurança.

Ademais, cumpre notar que o próprio texto constitucional pátrio reconhece a não taxatividade do rol de direitos contido no seu artigo 5º, apontando assim para a possibilidade da soma de outros direitos decorrentes do regime e dos princípios constitucionais – bem como constantes de tratados internacionais de direitos humanos ratificados pelo Brasil – ao status conferido por referido dispositivo da Constituição.²¹

A conclusão que se pode extrair da dinâmica brevemente ilustrada acima, é a de que o racional da proteção de dados está intrinsecamente relacionado à tutela de direitos e liberdades fundamentais, sendo arguível que o pleno exercício do direito à proteção de dados assume a função de *meio* para se garantir a efetividade dos direitos fundamentais nas situações em que tais direitos possam se ver ameaçados pelo uso de dados sobre uma pessoa. É justamente nessa linha que argumenta Sarlet (2021, p. 29) ao dizer que “o direito à proteção dos dados pessoais é inequivocamente fundamental também no sentido material, pois – mesmo que se o considere como de natureza instrumental – ele serve justamente à proteção de tais valores, princípios e direitos.”

Referida conclusão abre espaço, inclusive, para que o direito à proteção de dados pessoais seja reconhecido pelo ordenamento como um direito funda-

20. O risco ao livre desenvolvimento da personalidade neste caso é capaz de atingir aspectos íntimos da personalidade da pessoa de forma deliberada e com o objetivo de potencializar o uso da plataforma em detrimento das emoções exploradas e que, além de potencialmente inviabilizar o livre desenvolvimento da personalidade dos usuários da aplicação (um dos fundamentos da LGPD – artigo 2º, VII), também pode esbarrar na própria dignidade da pessoa humana, um dos fundamentos da Constituição Federal (artigo 1º, III).

21. Constituição Federal, artigo 5º, §2º.

mental. É nesse sentido que caminharam a União Europeia²² e o Brasil, como verificaremos adiante neste estudo. Antes disso, porém, cabe adentrar no cerne da presente discussão: superadas as questões instrumentais sobre a avaliação de risco e, mais importante, compreendido o principal conceito de risco em proteção de dados, qual deve ser a implicação prática da verificação da efetiva existência de riscos aos direitos e liberdades fundamentais dos titulares dos dados por um agente de tratamento e, em que medida tal verificação deve modular o tratamento por ele almejado?

2.1 A baliza da proteção de dados baseada na aferição de risco a direitos e liberdades fundamentais

Analisando as disposições da LGPD, podem ser vistas menções esparsas ao tema do RIPD, menções essas que não oferecem ao agente de tratamento uma conclusão sobre o que fazer – ou deixar de fazer – com relação à atividade de tratamento avaliada. Depreende-se, contudo, que ante à responsabilidade assumida pelos agentes de tratamento com relação à garantia do direito à proteção de dados, as conclusões a que um RIPD permitir que o agente de tratamento chegue devem subsidiar suas decisões sobre (i) manter o tratamento de dados da forma como planejado; (ii) implementar medidas técnicas e administrativas para mitigar os riscos aos titulares de modo a viabilizar a realização do tratamento planejado; ou (iii) deixar de realizar a atividade de tratamento caso os riscos identificados não possam ser adequadamente mitigados.

Neste tema, como já brevemente comentado neste artigo, o GDPR *obriga* os agentes de tratamento a ele sujeitos a consultar a autoridade supervisora caso uma avaliação de riscos realizada por meio de um RIPD tenha como resultado, após a tomada das medidas mitigatórias adequadas, um risco alto aos direitos e liberdades dos titulares.²³ Mesmo assim, apesar de tal obrigação não encontrar paralelo na legislação brasileira, é certo que cabe ao agente de tratamento *decidir* sobre o tratamento que pode implicar riscos aos titulares.

22. Carta dos Direitos Fundamentais da União Europeia, artigo 8º: 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Acessível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf - acesso em 9 de janeiro de 2022.

23. GDPR, Considerando nº 84.

Assim, a tomada de decisão sobre o que fazer posteriormente à elaboração do RIPD deve iniciar com uma reflexão sobre *o que* exatamente legitima as atividades de tratamento analisadas, de modo a permitir que um exercício de balanceamento entre a necessidade do tratamento e o risco ao titular seja realizado. Pela perspectiva do agente de tratamento, isso significa garantir que o tratamento almejado seja amparado por uma *autorização legal* adequada – as chamadas bases legais para tratamento de dados pessoais, previstas nos artigos 7º e 11 da LGPD.

Tem-se, portanto, que, caso determinado tratamento de dados implique risco aos direitos e às liberdades dos titulares, porém seja necessário ao cumprimento de uma obrigação imposta por uma disposição legal vigente,²⁴ o agente de tratamento se verá compelido a realizar o tratamento de igual forma, em que pese existirem riscos aos direitos e liberdades fundamentais do titular. Pode-se dizer, nesses casos, que o *próprio legislador determinou previamente* que o tratamento de dados imposto pela lei não implica, no âmbito do ordenamento jurídico pátrio, risco *desproporcional* aos direitos e liberdades fundamentais do titular. Tal situação, contudo, sequer exigiria do agente de tratamento qualquer avaliação de riscos mais aprofundada, haja vista que o agente está obrigado a cumprir as leis a ele aplicáveis.

Por outro lado, situação distinta seria observada caso o agente de tratamento chegasse à conclusão de que o tratamento de dados almejado é legitimado em razão da necessidade de se atender a um interesse legítimo. O cuidado do legislador neste aspecto foi tamanho que referida hipótese autorizativa do tratamento de dados pessoais foi expressamente *limitada* pelos direitos e liberdades fundamentais dos titulares,²⁵ havendo inclusive previsão específica na lei quanto à possibilidade de a ANPD solicitar do controlador um RIPD quando o tratamento tiver como fundamento seu interesse legítimo.²⁶ Deparado com esse tipo de conflito – entre os interesses legítimos do agente e os direitos e liberdades do titular –, o agente de tratamento tem uma decisão-chave a ser tomada: definir se o tratamento poderá ou não ser realizado, e como.

24. LGPD, artigo 7º, II e artigo 11, II, 'a'.

25. LGPD, Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, **exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.**

26. LGPD, artigo 10, §3º.

É diante deste conflito entre interesses e direitos que o agente de tratamento precisará, por conta própria, definir se os direitos e liberdades fundamentais dos titulares *prevalecem* sobre seus interesses. Nesse sentido, o Data Privacy Brasil desenvolveu um robusto estudo sobre o exercício de balanceamento necessário à verificação da existência de um interesse legítimo em uma série de casos concretos exemplificativos, em vista dos direitos e liberdades dos titulares impactados em cada situação.²⁷

Novamente trazendo o presente debate para a prática da operação de um agente de tratamento, a título exemplificativo, pode-se dizer que, caso uma empresa de locação de automóveis decida implementar processo para verificar registros de ações judiciais nos quais seus pretensos clientes estejam ou estiveram envolvidos com o objetivo de *negar* a prestação de seus serviços a pessoas que tenham, segundo critérios exclusivos da empresa, histórico tido como *inaceitável* pensando na manutenção da segurança da propriedade e integridade de seus veículos, o tratamento dos dados relacionados às ações judiciais teria grandes chances de ser *ilegítimo* para o contexto, por provavelmente prevalecerem os direitos e liberdades dos titulares.

No caso ilustrado, verificado o interesse da empresa em coletar dados sobre seus pretensos clientes com o pretexto de conferir suposta *segurança material* à sua operação, tal interesse pode se mostrar como altamente questionável em vista dos direitos e liberdades fundamentais de tais pessoas, à luz dos princípios da isonomia e não discriminação previstos na Constituição Federal, bem como em vista dos contornos legais aplicáveis à atividade econômica da empresa.²⁸

A situação hipotética narrada apenas cuida de exemplificar a necessidade de exercícios de balanceamento entre interesses supostamente legítimos de uma organização e os direitos e liberdades garantidas às pessoas impactadas pelas suas atividades. Como desfecho, tem-se que, será apenas mediante a realização de análises efetivamente comprometidas com a identificação dos riscos *aos titulares* no contexto do tratamento de dados pessoais é que o agente de tratamento estará mais próximo de cumprir suas obrigações legais e regulatórias em proteção de dados.

27. BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Acessível em <https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse>. Acesso em 9 de janeiro de 2022.

28. Artigos 4º, III, 6º, IV e 39, IX da Lei nº 8.078/90 (Código de Defesa do Consumidor) e artigo 36, §3º, X e XI da Lei nº 12.529/2011.

3. O direito à proteção de dados pessoais como um direito fundamental autônomo

Constatada a complexidade do necessário balanceamento entre as atividades de tratamento de dados pessoais de uma organização e os direitos e liberdades dos titulares, para além de requisitos meramente formais, contribui para o fortalecimento da perspectiva protetiva em relação ao titular dos dados o avanço normativo com relação à elevação do status do direito à proteção de dados ao patamar de um direito fundamental.

Após diversos movimentos nesse sentido no país, desde a existência de teses que argumentavam sobre a existência de um direito fundamental à proteção de dados pessoais implícito no texto constitucional (SARLET, 2021, p. 35-39), até a decisão do plenário do Supremo Tribunal Federal em que se reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais,²⁹ em acréscimo ao já expressamente previsto direito à privacidade,³⁰ enfim chegou-se, em fevereiro de 2022, na emenda à constituição que cuidou de inserir o direito à proteção de dados pessoais como um direito fundamental de forma expressa.³¹

Nesse contexto de evidente – e crescente – robustez do ordenamento em benefício da proteção de direitos e liberdades fundamentais de forma associada à proteção de dados pessoais, as avaliações de risco debatidas no presente artigo só se tornarão cada vez mais relevantes e necessárias. Parece então que caberá à ANPD tomar as medidas que entender cabíveis para elucidar os objetivos e parâmetros verdadeiramente esperados dos agentes de tratamento quando da elaboração de RIPDs para viabilizar a realização deste tipo de exercício de balanceamento.

Tal avanço regulatório se mostra, portanto, absolutamente essencial à garantia da proteção dos direitos de todas as pessoas naturais no ordenamento jurídico brasileiro, contribuindo para a efetivação dos propósitos da legislação sobre proteção de dados por meio de uma atuação educativa da ANPD, tanto perante os agentes de tratamento, quanto perante a sociedade como um todo.

29. Decisão do plenário do Supremo Tribunal Federal que confirmou a decisão monocrática de 17 de abril de 2020 da Ministra Rosa Weber na ADIn nº 6387. Disponível em <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em 6 de janeiro de 2022.

30. Constituição Federal, artigo 5º, X.

31. Emenda Constitucional nº 115 de 10 de fevereiro de 2022. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 16 de abril de 2022.

Considerações finais

Não há dúvidas de que, nos últimos anos, o direito à proteção de dados pessoais alcançou posição de bastante destaque para a manutenção do Estado Democrático de Direito. Aos operadores do direito, faz-se necessário ter efetivo comprometimento com a interpretação das normas vigentes em vista de seus princípios e fundamentos, não sendo aceitável que a noção quanto à proteção de dados seja limitada à verificação de padrões de segurança e *checklists* de conformidade tão somente para garantir o atendimento de requisitos formais.

É justamente diante dessa complexidade que o intérprete das normas deve entender que a proteção de dados pessoais só pode ser garantida com uma abordagem multidisciplinar – dentro e fora do Direito –, de modo que a lei seja aplicada em sua integralidade.

Com isso, a conclusão lógica em relação ao tema examinado no presente artigo deve ser a de que avaliar riscos em proteção de dados pode assumir, na prática, diversas formas. Embora a diversidade de formas não seja necessariamente prejudicial à tutela do direito à proteção de dados, é crucial que o agente de tratamento esteja equipado com o conhecimento necessário para saber *distinguir* referidas formas de avaliação de risco e direcionar seus esforços de forma estratégica – de um lado, para não expor titulares a riscos com relação a seus direitos e liberdades fundamentais, e, de outro, para levar à frente suas iniciativas de governança em privacidade, com foco em conformidade, e conduzindo os diálogos necessários à organização sobre o risco regulatório inerente à sua operação.

Referências

BINNS, Reuben. *Data Protection Impact Assessments: A Meta-Regulatory Approach in International Data Privacy Law*, Vol. 7(1), 28 de abril de 2017. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964242. Acesso em 8 de janeiro de 2022.

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Acessível em <https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse>. Acesso em 9 de Janeiro de 2022.

GELLERT, Raphaël. *Understanding the notion of risk in the General Data Protection Regulation*, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017).

GOMES, Maria Cecília Oliveira. *Entre o Método e a Complexidade: Compreendendo a Noção de Risco na LGPD in Temas Atuais de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2020. Coordenação Felipe Palhares.

MONTEIRO, Renato Leite. *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?* Artigo estratégico #39 do Instituto Igarapé, dezembro de 2018. Acessível em <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em 8 de janeiro de 2022.

QUELLE, Claudia. *Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level?* Tilburg Law School Research Paper. 15 de dezembro de 2015. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726073. Acesso em 8 de janeiro de 2022.

SARLET, Ingo Wolfgang. *Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados in Tratado de Proteção de Dados Pessoais*. Coordenadores: Danilo Doneda [et al.]. Rio de Janeiro: Forense, 2021.

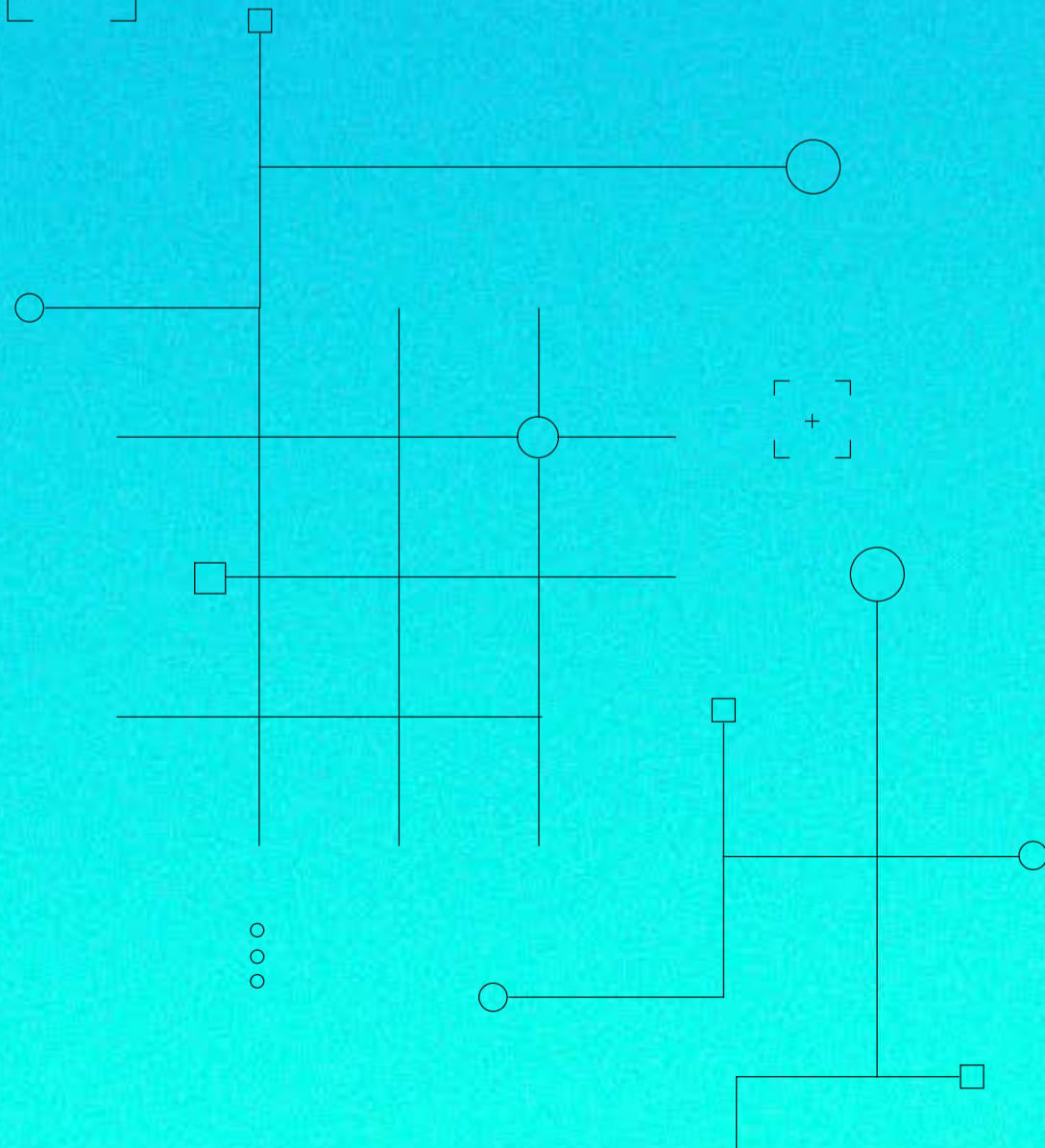
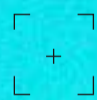
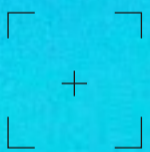
ZANATTA, Rafael. *Proteção de dados pessoais como regulação do risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet, 14 de novembro de 2017. Disponível em http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em 7 de janeiro de 2022.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

8

O consumidor e a publicidade direcionada *on-line*: uma análise segundo a Lei Geral de Proteção de Dados Pessoais

GABRIELA BRUM DAVOLI



Sumário: Introdução. 1. Uma análise principiológica do tratamento dos dados pessoais para envio de publicidade direcionada. 1.1. Finalidade, adequação, transparência e livre acesso. 1.2. Necessidade, qualidade dos dados e não discriminação. 1.3. Segurança, prevenção, responsabilização e prestação de contas. 2. As bases legais aplicáveis ao tratamento de dados para publicidade direcionada. 2.1. O fornecimento do consentimento pelo titular. 2.2. O atendimento aos legítimos interesses do controlador ou de terceiros e a aplicação da privacidade contextual. Considerações finais. Referências.

Introdução

É cada vez mais comum nos depararmos com anúncios publicitários personalizados na internet. Isso é possível em função da (não mais tão) recente implementação de ferramentas tecnológicas no ambiente *on-line* que auxiliam no rastreamento dos usuários e na consequente inferência dos seus interesses e entrega de publicidade precisa. Um dos principais exemplos dessas ferramentas são os *cookies*, que permitem saber com precisão, por exemplo, por onde o mouse do usuário passou, em quais links ele clicou e quanto tempo ficou em uma determinada página.

Essa entrega de mídia altamente personalizada necessariamente demanda o tratamento de um alto volume de dados pessoais e, considerando a granularidade das informações sobre os padrões de navegação dos usuários, bem como a correlação cirúrgica entre o produto anunciado e os interesses do usuário impactado, é um tipo de publicidade que pode ser definida como publicidade comportamental (BIONI, 2020, p. 17). Isso apenas é possível em função do envolvimento de plataformas de mídia responsáveis pela cadeia de tratamento dos dados, tais como Ad Networks, AdServers, Demand-Side Platforms (DSPs), Exchange, Private Marketplace (PMP) e Sell-Side Platform (SSPs) (RAMOS, 2021, p. 84 e 85). Essas plataformas trabalham em conjunto para que ocorra uma espécie de leilão em tempo real (IAB Brasil, 2016, p. 92) e

1. Advogada com mais de dois anos de experiência em direito digital, mídia, privacidade e proteção de dados pessoais. Formada em ciências jurídicas e sociais pela Universidade Federal do Rio Grande do Sul, pós-graduanda em direito digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro, candidata a LLM em Direito e Tecnologia na Tilburg University, especialista em Privacidade e Proteção de Dados pelo Data Privacy Brasil e em direito digital pela Fundação Getúlio Vargas. Certificada pelo IAB Brasil em Digital Fundamentals em 2020.

seja entregue para o usuário –em torno de 10 milissegundos²–o conteúdo mais relevante possível.

Tudo isso acontece no universo da chamada mídia programática (SILVEIRA, MORISSO, 2018, p. 72), uma das grandes responsáveis pela redução de custos em ações publicitárias (EVANS, 2009, p. 42) e consequentemente pelo crescimento das vendas *on-line*³. Diversos são os materiais disponibilizados *on-line* sobre o tema⁴, tendo em vista a sua relevância e alta complexidade.

Diante desse cenário, alguns são os desafios sob o aspecto de proteção de dados pessoais, quando o assunto é a entrega de publicidade direcionada comportamental: **(i)** seja o cumprimento pelos agentes de tratamento de dados⁵ com os deveres decorrentes dos princípios da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou LGPD) perante o titular dos dados⁶, tendo em vista, por exemplo, que até mesmo especialistas que trabalham com a matéria encontram problemas em rastrear todos os atores que atuam no processo de entrega de conteúdo (OLIVEIRA, 2019, p. 59), **(ii)** seja a definição de qual é a base legal adequada⁷ -e se há uma -para o tratamento dos dados pessoais que possibilitam que os usuários sejam impactados com tamanha assertividade.

Dessa maneira, este artigo tem como objetivo fazer uma análise principiológica do uso de dados pessoais, segundo a LGPD, para entrega de publicidade direcionada comportamental. Nesse sentido, será feita uma avaliação da atividade de tratamento de dados pessoais considerando cada um dos princípios previstos no art. 6º da LGPD.

Por fim, será estudada a legitimidade da aplicação das possíveis bases legais disponíveis para o tratamento de dados pessoais para entrega de publicidade direcionada comportamental. Assim, serão discutidos os prós e os contras decorrentes das hipóteses capazes de fundamentar o tratamento de

2. Conforme demonstra “O que é e como funciona o Real Time Bidding (RTB) em mídia programática?”. 2020. (3m58s). Publicado pelo canal IAB Brasil. Disponível em <<https://www.youtube.com/watch?v=dRNd5SjCjCov>>

3. Segundo o Digital AdSpend 2021 da IAB, investimentos em publicidade digital movimentaram R\$ 36,9 bilhões no Brasil, em 18 meses. Disponível em <<https://iabbrasil.com.br/pesquisa-digital-adspend-2020-2021/>>

4. Pela busca do termo “mídia programática” no Google Acadêmico (<https://scholar.google.com.br/?hl=pt>), foram encontrados cerca de 24.400 resultados.

5. Pessoas naturais ou jurídicas, de direito público ou privado, que tratam dados pessoais, seja em nome próprio (controlador) seja em nome de terceiro (operador), na linha do que define o art. 5º, IX da LGPD.

6. Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, conforme art. 5º, V da LGPD.

7. Hipótese legal que autoriza o tratamento de dados pessoais, conforme indica o art. 7º da LGPD.

dados pessoais para mídia programática, bem como serão avaliadas as possíveis salvaguardas que podem ser adotadas para mitigar os riscos de violação às liberdades e aos direitos fundamentais dos titulares.

1. Uma análise principiológica do tratamento dos dados pessoais para envio de publicidade direcionada

O art. 6º da LGPD traz uma série de princípios que devem ser observados, ao lado da boa-fé⁸, pelos agentes de tratamento do desempenho das suas atividades de tratamento de dados pessoais. Os princípios são norteadores para a interpretação dos dispositivos da legislação, pois auxiliam na compreensão dos demais artigos da LGPD (FRAZÃO, 2018, p. 4), bem como “no exame da disciplina da proteção de dados pessoais e dos seus usos permitidos segundo os critérios definidos na legislação” (MIRAGEM, 2019, p. 5).

Para a matéria de mídia programática, a avaliação detalhada desses princípios se torna relevante para o entendimento dos limites que devem ser observados no tratamento de um alto volume de dados pessoais por diversos agentes de tratamento na cadeia de entrega de publicidade direcionada. Nessa linha, decidiu-se pela análise dos princípios previstos na legislação de acordo com as semelhanças das medidas que devem ser adotadas para o seu cumprimento, o que pode coincidir – em alguns casos - com a ordem em que estão dispostos nos incisos do art. 6º da LGPD.

1.1 Finalidade, adequação, transparência e livre acesso

O primeiro princípio trazido pelo art. 6º é o princípio da finalidade (inciso I), que indica que os dados pessoais deverão ser tratados para “propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. Esse princípio pode ser analisado em conjunto com o princípio da adequação (inciso II), uma vez que este também aborda a necessidade de que o tratamento dos dados seja compatível “com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.

Tais princípios, invariavelmente, abordam o princípio da transparência (inciso VI), que dispõe sobre a “garantia, aos titulares, de informações claras,

8. Limitaremos a análise do presente artigo aos incisos do art. 6º da LGPD, tendo em vista a delimitação do escopo da análise pretendida. Contudo, vale a leitura da análise do princípio da boa-fé no tratamento de dados pessoais nas relações de consumo em MIRAGEM, 2019.

precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento”, pois indicam a necessidade de que os propósitos do tratamento dos dados sejam informados aos titulares. Este último está diretamente ligado ao princípio do livre acesso (inciso IV), uma vez este que garante ao titular o direito de poder consultar fácil e gratuitamente informações sobre a forma e a duração do tratamento dos dados pessoais, excetuando o segredo de negócio, o que pode trazer dúvidas sobre como compatibilizar os princípios em análise (FRAZÃO, 2018, p. 6).

Seguindo essa lógica, quando analisada a finalidade de tratamento de dados pessoais para entrega de publicidade de direcionada comportamental, é possível afirmar que se trata de um propósito legítimo, uma vez que, na legislação brasileira, não há qualquer proibição expressa em relação a esta prática⁹. Quanto à especificidade do propósito, se considerarmos que os dados serão utilizados para potencializar a assertividade da entrega de conteúdo, pode-se dizer que está de acordo com a exigência legal da finalidade ser específica.

Parece que um dos grandes desafios em relação ao tema está diretamente relacionado ao fornecimento de informações explícitas, claras, precisas e gratuitas para o consumidor sobre a atividade que será desenvolvida com os seus dados. Isso decorre tanto da complexidade do fluxo informacional e das limitações cognitivas dos usuários para entendimento do tema (BIONI, 2020, p. 138) quanto do mecanismo hoje utilizado no mercado para dar transparência aos titulares, as políticas de privacidade, que tem se mostrado falho por inúmeras razões.¹⁰

A situação se torna ainda mais difícil quando se fala no cumprimento dos requisitos do art. 9º da LGPD¹¹, especialmente em função da necessidade de indicação do uso compartilhado dos dados pessoais pelo controlador e a finalidade. É claro que menções mais amplas e genéricas nas políticas de privacidade sobre o assunto podem mitigar os riscos relacionados à potencial viola-

9. Para a presente análise, considerou-se que o envio de publicidade está de acordo com as limitações previstas no Código de Defesa do Consumidor (Lei nº 8.078/90 – CDC), a exemplo do art. 36 e seguintes do CDC.

10. Bruno Bioni afirma que as políticas de privacidade têm se mostrado falhas, pois reforçam a aventada assimetria do mercado informacional e são ferramentas que não capacitam, efetivamente, o cidadão para exercer o controle sobre suas informações pessoais em BIONI, 2020, p. 162.

11. Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

ção da legislação pelo controlador dos dados sob o aspecto da transparência. Contudo, o mercado precisa olhar criticamente para esse método considerado ultrapassado e, conforme indicado por Bruno Bioni (2020, p. 166), estudar se “há novas formas de concretizar a prometida esfera de controle sobre os dados pessoais”, especialmente, para o cumprimento com o dever informacional perante o consumidor em decorrência do tratamento de dados para entrega de publicidade comportamental.

1.2 Necessidade, qualidade dos dados e não discriminação

O tratamento dos dados pessoais deve ser feito de acordo com o mínimo necessário para atingir as finalidades pretendidas, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação aos propósitos do tratamento de dados, conforme indica o inciso III do art. 6º da LGPD. Além disso, deve ser garantido ao titular “exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (art. 6º, V da LGPD), bem como que os dados não sejam usados para fins discriminatórios, ilícitos ou abusivos (inciso IX).

É evidente a essencialidade do tratamento de um alto volume de dados pessoais para a publicidade moderna (RAMOS, 2021, p. 96). Para que sejam entregues anúncios personalizados, além do envolvimento dos agentes da mídia programática¹², se faz necessário o cruzamento de dados pessoais advindos de diversas fontes, tais como *first-party* e *third-party data*, bem como *data providers* (RAMOS, 2021, p. 98). Dessa forma, quanto mais se compreende das informações e do fluxo que elas percorrem para impactar os usuários com publicidade direcionada, fica mais clara a dificuldade de definir quais dados pessoais são tratados, os papéis dos envolvidos no tratamento dos dados e a quais dados pessoais eles têm acesso.

Nessa linha, figura como desafiador o cumprimento com os princípios da necessidade e da qualidade, pois pode ser difícil garantir que todos os dados utilizados têm um propósito específico, são relevantes, exatos, claros e pertinentes para a atividade de tratamento¹³. Somam-se a esse fator os riscos dis-

12. Conforme abordado na introdução do presente artigo.

13. Nesse sentido, Bruno Miragem fala do equilíbrio entre a pretensão de maior precisão na análise dos dados e a limitação do seu uso em face do princípio da necessidade em MIRAGEM, 2019, p. 173-222.

criminatorios decorrentes das atividades de *Big Data* (MENDES, MATTIUZO, 2019, p. 39), de modo que até mesmo a observância ao princípio da não-discriminação pode vir a ser questionada.

Como pontuado por Bruno Miragem (2019, p. 183), é difícil chegar a um equilíbrio entre a limitação dos usos dos dados e a pretensão de maior precisão na sua análise:

Em especial frente às várias possibilidades de correlações que podem ser realizadas em termos estatísticos entre dados que aparentemente não tenham uma vinculação direta entre si. A precisão do que se deva considerar o mínimo necessário para a realização das finalidades do tratamento de dados tensiona com o volume ou qualidade dos dados necessários para a melhor consecução destas finalidades.

É claro que os controladores dos dados podem adotar algumas medidas técnicas para garantir que os dados sejam usados de forma mais segura e eficiente e, por consequência, mais estruturada, como pela centralização das informações em um *data lake*. Contudo, isso não significa que somente dados estritamente necessários serão utilizados, mas apenas que será possível gerenciar perfis de audiência de forma mais organizada.¹⁴

1.3 Segurança, prevenção, responsabilização e prestação de contas (*accountability*).

Os três últimos princípios analisados estão relacionados ao dever geral de qualidade da prestação de serviço do fornecedor¹⁵. A legislação exige que sejam utilizadas medidas técnicas e administrativas aptas para a proteção dos dados pessoais contra o tratamento indevido (art. 6º, VII da LGPD), o que, em certa medida, está conectado com a prevenção de potenciais danos decorrentes do tratamento de dados pessoais (inciso VIII).

Além de trazer obrigações para a proteção dos dados tratados, a LGPD dispõe que os agentes de tratamento devem ser capazes de demonstrar que adotaram medidas eficazes para o cumprimento da legislação (inciso IX). Dessa maneira, aqueles que utilizam dados pessoais na consecução das suas ati-

14. Nesse sentido, RAMOS, 2021, p. 102.

15. Nesse sentido, MIRAGEM, 2019, p. 185.

vidades ficam obrigados a implementar regras de boas práticas e governança que, entre outras medidas, estabeleçam procedimentos internos de supervisão e de mitigação de riscos relacionados ao tratamento de dados pessoais.¹⁶

Seguindo essa lógica, todos os participantes envolvidos na entrega de publicidade direcionada devem adaptar as suas respectivas atividades¹⁷, conforme os propósitos para os quais utilizam os dados pessoais, para garantir o cumprimento da legislação, bem como para serem capazes de comprovar essa garantia. Nesse sentido, a avaliação criteriosa dos riscos decorrentes do tratamento dos dados no fluxo da mídia programática e a sua documentação, tais como pela elaboração de análises *privacy by design* (HUSTINX, 2010, p. 254) e de relatórios de impacto à proteção de dados pessoais¹⁸ somada à implementação de medidas técnicas¹⁹ podem ser uma boa forma de cumprir com os princípios da segurança, prevenção e *accountability*.

2. As bases legais aplicáveis à publicidade direcionada

Superada a análise da entrega de publicidade comportamental sob o viés dos princípios que regem o tratamento dos dados pessoais, é relevante avaliar – caso o agente de tratamento dos dados pessoais seja capaz de cumprir com os princípios da legislação – qual é a base legal adequada para o tratamento dos dados pessoais para essa finalidade. Quando abordada a relação entre o consumidor e o fornecedor, algumas são as hipóteses previstas na legislação que autorizam o tratamento dos dados.²⁰ Assim, a definição da hipótese que legitima o tratamento deve sempre partir da definição de quais serão os dados pessoais tratados²¹ e da finalidade para a qual o dado pessoal será utilizado,

16. O Art. 50 da LGPD define que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

17. Considerando que são agentes de tratamento de dados pessoais.

18. *Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco*, conforme definido pelo inciso XVII do art. 5º da LGPD.

19. As quais não serão aprofundadas no presente artigo em função do escopo jurídico da análise.

20. *Nas relações de consumo, tem relevância o exame, sobretudo, dos incisos I, II, VI, VIII, IX e X do art. 7º da LGPD*, conforme MIRAGEM, 2019, p. 179.

21. A definição de quais dados pessoais serão tratados é relevante em função das diferentes hipóteses legais aplicáveis

pois, no sentido do que foi pontuado por Bruno Miragem (2019, p. 179), a finalidade é um dos elementos centrais na disciplina da proteção de dados pessoais.

A partir da definição da finalidade de tratamento dos dados pessoais para direcionamento de publicidade comportamental, é possível seguir para avaliação de quais são as bases legais passíveis de autorizar a utilização dos dados para esse propósito. Geralmente, a doutrina²² estuda duas principais bases legais que podem legitimar o tratamento das informações dos usuários para campanhas de marketing: o consentimento (art. 7º, I da LGPD), e o atendimento aos legítimos interesses do controlador ou de terceiro (inciso IX). Vale ressaltar ainda que, em quaisquer das hipóteses, é necessário que o controlador dos dados pessoais garanta, mediante requisição²³, o atendimento aos direitos dos titulares.

2.1 O fornecimento do consentimento pelo titular

No que tange ao consentimento do titular para o tratamento dos seus dados pessoais, importa referir que está intrinsecamente ligado à autodeterminação do indivíduo (DONEDA, 2019, p. 302), que expressa estar de acordo com algo que lhe é apresentado (MIRAGEM, 2019, p. 179). Para que esse consentimento seja considerado válido, é necessário que a manifestação do titular seja livre, informada e inequívoca (art. 5º, XII da LGPD). Nesse sentido, o usuário deve **(i)** ter liberdade de optar por não ter seus dados tratados para uma determinada finalidade, **(ii)** ter acesso a informações claras e precisas em relação à atividade que será desempenhada com as suas informações e **(iii)** manifestar-se de modo que fique evidente a sua vontade²⁴, por meio de uma ação afirmativa, por exemplo.

Apesar de alguns países já terem se posicionado no sentido de fornecimento de consentimento do titular para entrega de publicidade compor-

ao tratamento de dados pessoais (constantes no art. 7º da LGPD) e dados pessoais sensíveis (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme dispõe o art. 5º, II da LGPD), em relação aos quais as bases legais estão previstas no art. 11 da LGPD.

22. Nesse sentido, RAMOS, 2021, p. 125 a 145; e BIONI, 2020, p. 225 e 232.

23. Conforme indica o art.18 da LGPD.

24. O art. 8º da LGPD indica que o consentimento previsto no inciso I do art. 7º deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

tamental²⁵, a coleta desse consentimento pode encontrar alguns entraves. Considerando a necessária observância ao princípio da necessidade (conforme abordado no item **1.2.** acima), o fornecimento do consentimento para uma finalidade específica autoriza o controlador dos dados a tratá-los apenas para esta finalidade, de modo que a utilização dos dados para outro propósito demandaria um novo consentimento (BIONI, 2020, p. 222). Isso pode acabar sendo incompatível com a dinâmica da tecnologia do *Big Data*, visto que a sua intenção é justamente alargar as possibilidades de utilização dos dados pessoais (MILOSLAVSKAYA, 2016, p. 303), de modo que a coleta de um novo consentimento a cada nova finalidade de tratamento de dados poderia burocratizar o sistema de entrega de publicidade e não seria efetivo, também em função da limitação cognitiva do usuário.²⁶

Soma-se a esse fator a impossibilidade de coleta de consentimento por alguns intermediários na relação de mídia programática, que podem acabar tratando os dados para finalidades próprias, tendo em vista que não há qualquer contato direto com o titular dos dados pessoais.²⁷ Assim, diante dos desafios técnicos da coleta de um consentimento válido do titular para entrega de publicidade direcionada, caso fosse exigida legalmente esta coleta, é provável que as grandes empresas do setor de tecnologia tivessem vantagem sobre as demais empresas, como indicado por Pedro Ramos (2021, p. 145), “teríamos um cenário provavelmente pouco competitivo, de maior concentração entre os grandes atores do mercado e com baixa atratividade para o usuário.”

Dessa maneira, fala-se na aplicação da privacidade (consentimento) contextual²⁸, que não seria limitada a uma finalidade única, mas sim a propósitos de tratamento de dados pessoais que poderiam ser perquiridos dentro do contexto de determinada relação e conseqüentemente ter seu tratamento embasado em outra hipótese legal. Como pontuado por Bruno Bioni (2020, p. 226), esse tipo de privacidade se mostra “útil, já que ela é elástica o suficiente para

25. Nesse sentido, ARTICLE 29, Opinion 02/2010 on online behavioural advertising. No mesmo sentido, ver a reportagem “China cria lei para limitar poder de algoritmos de influenciar nossas vidas”. Disponível em <<https://www.uol.com.br/tilt/colunas/felipe-zmoginski/2022/01/10/china-cria-lei-para-limitar-poder-de-algoritmos-de-influenciar-nossas-vidas.htm>>

26. No mesmo sentido BIONI, 2020, p. 223.

27. Nessa linha, Pedro Ramos indica que esses intermediários precisariam se valer apenas da boa-fé dos seus parceiros comerciais e de obrigações contratuais para exigir que coletassem o consentimento em seu nome em RAMOS, 2021, p. 144.

28. Sobre o tema, Bruno Bioni indica que a *teoria da privacidade contextual estrutura-se sob a premissa de que o fluxo informacional deve ser apropriado de acordo com as suas respectivas esferas sociais [...] de modo que retoma-se em parte o discurso normativo da autodeterminação informacional* em BIONI, 2020, p. 225.

governar o uso secundário de dados pessoais que não podem ser previamente especificados e controlados de maneira rígida.”

2.2 O atendimento aos legítimos interesses do controlador ou de terceiros e a aplicação da privacidade contextual

Em relação à base legal do legítimo interesse, a legislação evidencia o fato de que o tratamento deve observar os direitos e as liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Além disso, são definidos como requisitos para fundamentação de uma determinada atividade no legítimo interesse (i) a utilização dos dados para finalidades legítimas e (ii) a definição de uma situação concreta; o que inclui, mas não se limita a dois exemplos (iii) atividades de apoio e promoção de atividades do controlador e (iv) garantia do exercício regular dos direitos pelos titulares, desde que (v) respeitadas as suas legítimas expectativas (art. 10, I e II da LGPD).

Ainda que não haja uma exigência expressa na legislação brasileira sobre a necessidade de elaboração de um teste de balanceamento ou de legítimo interesse²⁹, com base nas recomendações de outros países sobre o tema³⁰, a realização e documentação desse teste (conhecido em inglês como *legitimate interests assessment*, ou simplesmente LIA) para avaliação da aplicabilidade dessa base legal tem sido implementada, como medida de governança e *accountability* (JOELSONS, 2020, p. 2). Por ser essa uma base legal interpretativa, o LIA “é capaz de fornecer algumas pistas sobre quais são os principais pontos de atenção para mitigação dos riscos de eventual não conformidade acerca do uso do legítimo interesse” (BIONI, 2020, p. 249).

Nesse sentido, partindo para uma análise prática da atividade de tratamento de dados pessoais para entrega de publicidade direcionada comportamental, pode-se dizer que a utilização dos dados se dá de forma legítima, visto que, como abordado no item 1.1., não há proibição legal relacionada a este propósito. Ainda, considerando que a avaliação deve ser feita em relação

29. A legislação fala na possível solicitação pela Autoridade Nacional de Proteção de Dados (ANPD) de relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento interesse legítimo do controlador, conforme art. 10, §3º.

30. Nesse sentido, ARTICLE 29. Opinion on 06/24 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. >

a uma situação concreta de uso dos dados para mídia programática, é possível justificar a adequação do tratamento à LGPD (RAMOS, 2021, p. 128).

De modo geral, a finalidade de entrega de publicidade pode ser considerada uma atividade de apoio e promoção das atividades do controlador³¹ e, para que possa se justificar no seu legítimo interesse, deverá ser ponderada com os direitos e liberdades fundamentais do usuário. Dessa maneira, uma das principais salvaguardas para garantir esses direitos nesses casos é a implementação de mecanismos que possibilitem a oposição (*opt-out*) pelo titular dos dados em relação ao tratamento dos seus dados pessoais e, “quanto mais visível for tal prática e mais fácil for o exercício do *opt-out*, maiores são as chances de a aplicação do legítimo interesse ser considerada como uma base legal válida” (BIONI, 2020, p. 253).

Quanto à legítima expectativa do usuário em relação ao recebimento de publicidade comportamental, diante da dificuldade relacionada à transparência em relação ao tema³², a saída para os controladores dos dados pessoais parece ser valer-se na privacidade contextual³³, com atenção aos riscos relacionados ao abuso de direito nesses casos (BIONI, 2020, p. 230). A **(i)** implementação de algumas salvaguardas³⁴ para o direcionamento de publicidade e a **(ii)** garantia da legítima expectativa do titular, por exemplo, **(ii.a)** pelo impacto de usuários com os quais o controlador já tenha uma relação preestabelecida, bem como **(ii.b)** pela elaboração de um LIA, podem, portanto, ser um caminho para garantir que os titulares exerçam o domínio sobre seus dados (BIONI, 2020, p. 255) e consequentemente o tratamento para mídia programática ocorra em conformidade com a LGPD.

Considerações finais

É evidente a complexidade do tratamento de dados pessoais para entrega de publicidade direcionada comportamental no ambiente *on-line*. Conforme visto, o envolvimento de diversas fontes de dados pessoais, atores intermediá-

31. Conforme abordado na introdução do presente artigo, quando feita a referência da movimentação de R\$ 36,9 bilhões no Brasil, em 18 meses, em decorrência da publicidade.

32. Conforme abordado no item 1.1. e 2.1.

33. Conforme abordado no final do item 2.1.

34. Tais como transparência, minimização e possibilidade de *opt-out*, conforme abordado por Bruno Bioni em BIONI, 2020, p. 238.

rios que participam do fluxo da mídia programática e a ausência de mecanismos eficazes de transparência, tornam difícil a garantia do domínio dos dados pessoais pelos titulares.

Considerando o aumento exponencial desse tipo de publicidade no mercado e os benefícios que ela pode trazer tanto para fornecedores (que conseguem promover seu negócio), quanto para os consumidores (que são impactados por produtos e serviços de seu interesse), é fundamental encontrar formas eficazes de equilibrar os interesses dos controladores e os princípios previstos na legislação para resguardar os titulares. Diante dos desafios pontuados para que essa atividade possa se pautar nas bases legais previstas na legislação, a cooperação entre a academia e o mercado publicitário deve ser basilar para que sejam encontradas soluções realistas para endereçar o tema.

Desse modo, algumas medidas têm sido tomadas por agentes relevantes da regulamentação publicitária para promoção de debates sobre como é possível alcançar esse equilíbrio. Enquanto não se chega a um consenso sobre a questão, de forma paralela, é importante que os agentes de tratamento de dados pessoais trabalhem de forma conjunta, por meio da imposição de obrigações contratuais de proteção de dados aos seus parceiros, e de forma individual, a partir da avaliação das suas atividades de tratamento e adoção de estratégias de governança e *accountability*, para garantir que o fluxo informacional de entrega de publicidade comportamental se dê conforme a legislação de proteção de dados pessoais.

Referências

ARTICLE 29, Data Protection Working Party. *Opinion 02/2010 on online behavioral advertising*. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf>

ARTICLE 29, Data Protection Working Party. *Opinion on 06/24 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Disponível em < <https://www.dataprotection.ro/servlet/ViewDocument?id=1086>>

BIONI, Bruno Ricardo. *Proteção de dados pessoais e os limites do consentimento*. 2ª edição. Rio de Janeiro: Editora Forense, 2020.

DONEDA, Danilo. *Da privacidade e da proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 2ª edição. São Paulo: Thomson Reuters Brasil, 2019.

EVANS, David D. The economics of the online advertising industry. *Journal of Economic Perspectives*, Apr. 2009. Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1086473>

FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados Pessoais: principais repercussões para a atividade empresarial*. 2018. Disponível em <http://www.professoraanafraza.com.br/files/publicacoes/2018-08-30-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_Parte_I.pdf>

HUSTINX, Peter. Privacy by design: delivering the promises. *Identity in the Information Society*, v. 3, n. 2, p. 253-255, 2010. Disponível em <<https://link.springer.com/content/pdf/10.1007/s12394-010-0061-z.pdf>>

INTERACTIVE ADVERTISING BUREAU BRASIL. *Mídia programática*. São Paulo: IAB Brasil, 2016. Disponível em <<https://iabbrasil.com.br/wp-content/uploads/2012/09/E-BOOK-IAB-BRASIL-M%C3%8DDIA-PROGRAM%C3%81TICA.pdf>>

JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. *Revista de Direito e as Novas Tecnologias. Revista dos Tribunais*. vol. 8/2020, julho-setembro 2020.

MENDES, Laura; MATTIUZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. *Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias*. RDU, Porto Alegre, Volume 16, n. 90, 2019, 39-64, nov-dez 2019. Disponível em <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019>>

MILOSLAVSKAYA, Natalia; TOLSTOY, Alexander. Big data, fast data and data lake concepts. *Procedia Computer Science*, v. 88, p. 300-305, 2016. Disponível em <<https://www.sciencedirect.com/science/article/pii/S1877050916316957>>

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *Revista dos Tribunais*, vol. 1009, ano 108, p. 173-222. São Paulo: Ed. RT, novembro 2019. Disponível em <<https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf>>

O que é e como funciona o Real Time Bidding (RTB) em mídia programática?. 2020. Publicado pelo canal IAB Brasil. Disponível em <<https://www.youtube.com/watch?v=dRNd5SjCjCov>>

OLIVEIRA, Caio Marcelo Bizerril de. *Mídia programática: identificação e ranqueamento dos principais problemas e desafios para sua utilização*. Dissertação (Mestrado em Administração de Empresas) - Programa de Pósgraduação em Administração de Empresas, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2019. Disponível em <<https://www.maxwell.vrac.puc-rio.br/45847/45847.PDF>>

PALHARES, Felipe (coord.). Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen Almeida; DE FREITAS, Jussara Maria Leal. Vício do consentimento através do neuromarketing nos contratos da era digital. *Revista de Direito do Consumidor*, 2020.

RAMOS, Pedro Henrique. Direito e mídia digital: melhores práticas. Belo Horizonte: Editora Dialética, 2021.

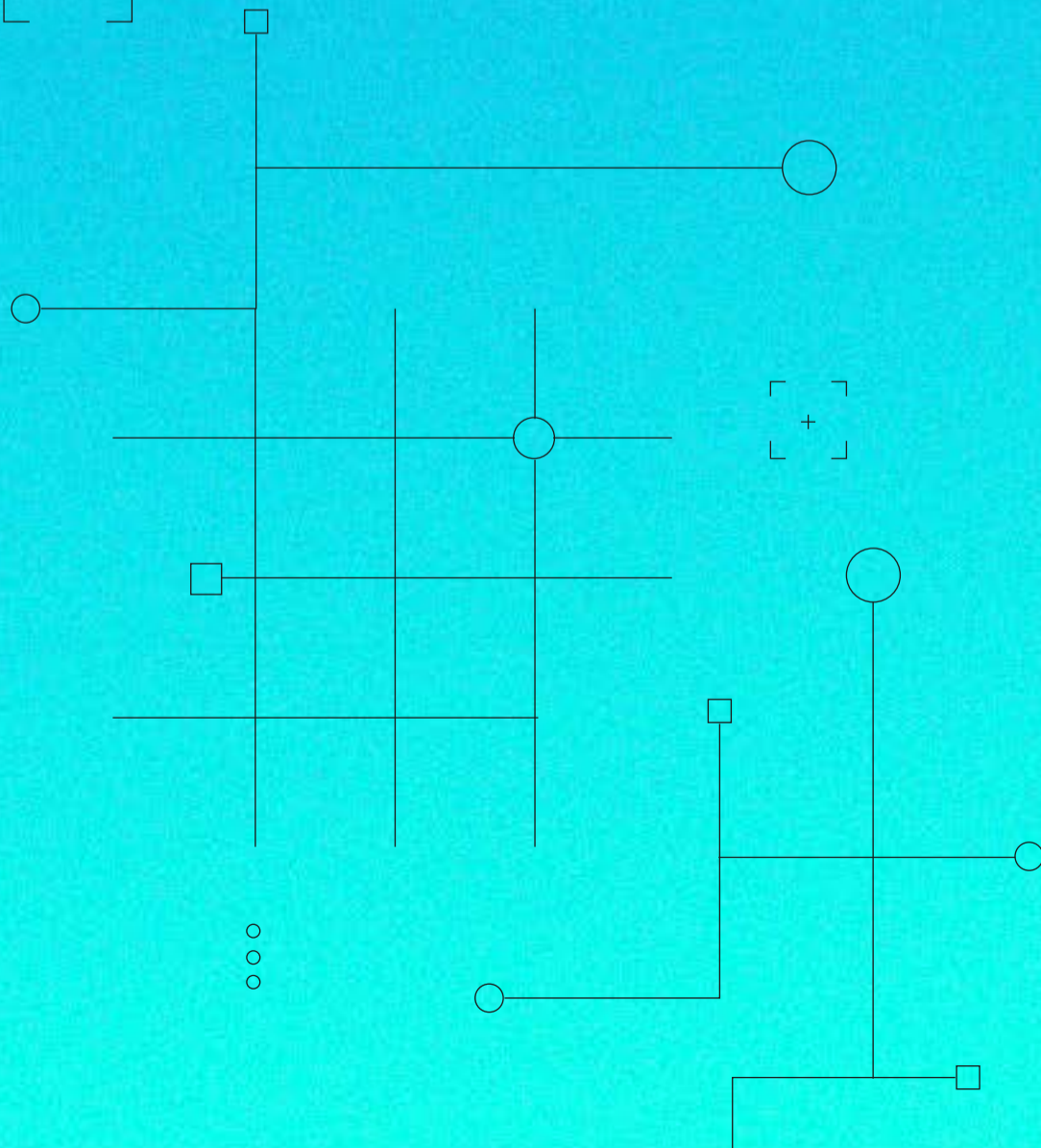
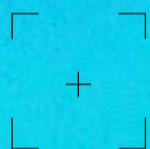
SILVEIRA, Stefanie; MORISSO, João Gabriel. *O uso de algoritmos na mídia programática*. *Parágrafo*, v. 6, n. 1, p. 71-82, 2018. Disponível em < https://www.researchgate.net/profile/Stefanie-Silveira/publication/330857309_Algorithm_use_in_the_programmatic_media_O_uso_de_algoritmos_na_midia_programatica/links/5c589fd-292851c22a3a92044/Algorithm-use-in-the-programmatic-media-O-uso-de-algoritmos-na-midia-programatica.pdf >

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9

Aplicação da Gamificação nas Interfaces de Trabalho e seus Reflexos no Direito ao Não-Trabalho

TAMARA DA SILVA



Sumário: Introdução. 1. Gamificação. 2. Aplicativos de entrega e a interface do trabalho. 3. Reflexo social e legislação 4. Limites da otimização do trabalho, precarização e direito à desconexão. Considerações finais. Referências.

Introdução

Com o desenvolvimento da Sociedade da Informação e o advento das tecnologias vinculadas à internet, o trabalho vem adquirindo novos contornos. A expansão da comunicação, propiciada pelas novas mídias digitais, vem revelando a necessidade de se remodelar os conceitos existentes, cunhados sob uma perspectiva analógica. Nesse contexto, o conceito da gamificação vem sendo explorado por interfaces de trabalho que, num primeiro momento, pretendem estimular o desempenho e tornar mais amigável a interface laboral.

Entretanto, lançando olhar sobre as consequências da aplicação desmedida, é possível estabelecer que as técnicas da gamificação – que exploram uma sensação de satisfação, através do estímulo e da recompensa, sem que, de fato, ocorram - induz a permanência da conexão ao trabalho, estimulando a autoexploração da mão-de-obra.

Por isso, faz-se necessário discutir limites entre o incentivo à produtividade e o exaurimento do trabalhador, por meio de estímulos contínuos que dificultam a desconexão. Da mesma forma, deve-se analisar o direito ao não-trabalho e a desconexão à luz da tendência da gamificação dentro das relações de trabalho da era digital.

1. Gamificação

É notória a transformação tecnológica que vem ocorrendo nas últimas décadas. Nunca se esteve tão conectado. Essa revolução digital do século XXI impactou a troca de dados e informações, trazendo um novo aspecto para as interações sociais. Acompanhando todo esse movimento, as relações de trabalho e consumo também se modificaram.

Já existe uma geração integrada à realidade das redes online desde a infância, que não reconhecem outro cenário que não a linguagem e metáfora

1. Graduada em direito pela Universidade do Estado do Rio de Janeiro – UERJ. Advogada.

dos jogos (Fabrício Fava, 2018). A geração Z² reforça o fato de que tudo está cada vez mais virtual e integrado. O tempo livre e o trabalho podem ter a distância entre o sofá e a mesa, lazer e responsabilidade conversam na mesma tela de celular, o filho e o chefe são separados por abas diferentes, expondo uma simbiose nas relações atuais.

As gerações passadas já conheciam os videogames, os quais já foram tidos como algo inovador e moderno. Esses games evoluíram e passaram por transformações que vão além do design gráfico visto por seus usuários, passando por linguagens algorítmicas e psicológicas.

Essa estrutura da gamificação (*gamification*), por meio do estímulo e recompensa, não é uma novidade, mas seu uso vem se expandindo para diversos setores sociais e econômicos, afetando, inclusive, a dinâmica de trabalho.

O que é a gamificação³? Trata-se de utilizar os mecanismos e conceitos dos jogos para resolver problemas da vida real. Busca-se aplicar técnicas de jogos em funções que não são jogos, trazendo ludificação e engajamento no que é realizado.

A gamificação é um conceito que vai além dos jogos, abrangendo mecanismos de estímulo, objetivo e recompensa. Quando uma interface oferece um sistema de pontos, de fases, de qualificações por etapas, superioridade e outros engajamentos atrelados a uma meta específica, ela estimula seu usuário por meio do reconhecimento.

É possível ver aplicação do conceito em diversos setores. Na área da educação, as escolas utilizam para melhorar os processos de aprendizagem e treinar professores para que adotem determinados comportamentos. Outro exemplo do cotidiano é a gamificação no aplicativo Waze⁴, em que os usuários

2. “A geração Z é composta por quem nasceu na primeira década do século XXI (...) O mais marcante dessa geração é a sua íntima relação com a tecnologia e com o meio digital, considerando que ela nasceu no momento de maior expansão tecnológica proporcionada pela popularização da internet.” PORFÍRIO, Francisco. “Geração Z”; Brasil Escola. Disponível em: <<https://brasilecola.uol.com.br/sociologia/geracao-z.htm>> Acesso em 03 de nov. de 2020.

3. “A gamificação (ou *gamification*, em inglês) é o termo utilizado para falar da lógica e dos mecanismos presentes nos jogos, principalmente com o uso de novas tecnologias, para estimular o aprendizado, motivar comportamentos e fornecer a sensação de recompensa. Em qualquer tipo de jogo existe um objetivo a ser cumprido e obstáculos que levam o protagonista em busca da realização. A psicologia por trás dos jogos revela algo muito profundo: a conquista e a superação movem o ser humano.” Bruna Giroldo. “Gamificação e mercado de trabalho: qual a relação entre os termos?”, BlogDigital PUC/PR, 16/11/2020. Disponível em <<https://posdigital.pucpr.br/blog/gamificacao-e-mercado-de-trabalho>>, Acesso em 03 de Jan. de 2022.

4. Aplicativo de navegação alimentado pelos usuários. “O Waze é alimentado e usado por motoristas em todo o mundo. Eles se conectam uns com os outros e trabalham juntos para melhorar a experiência de todos. Como um aplicativo de trânsito e navegação que se baseia na comunidade, o Waze foi criado como uma ferramenta de navegação social para carros particulares.” Google Suporte, “Como o Waze funciona?” Disponível em <<https://support.google.com/waze/answer/6078702?hl=pt-BR>>, Acesso em 28 de Dez. de 2021.

fornecem informações sobre o trânsito em tempo real e com isso ganham pontos em seus avatares⁵, que são ranqueados, ganhando destaque.

No mercado de consumo, foi desenvolvida uma escova de dentes pela marca Oral-B⁶, em que o produto fornece um *feedback* quanto à escovação de quem a estiver usando. Por meio de um pequeno painel, há uma carinha que pode ficar feliz ou triste de acordo com a escovação feita, fazendo com que o consumidor se sinta motivado a buscar aprovação.

Dentro da relação de trabalho, a gamificação pode envolver uma contrapartida direta, como uma premiação em forma de dinheiro ou benefícios⁷. De forma indireta, pode oferecer apenas reconhecimento meritório, como por exemplo, um ranking que demonstre a posição dos funcionários com as melhores avaliações dadas por seus colegas. Assim, se mantém uma atmosfera de competição e expectativa, em que as pessoas querem experimentar a sensação de recompensa.

2. Aplicativos de entrega e a interface do trabalho

A inteligência artificial é uma realidade que ganha espaço e afeta trabalhadores, sejam empregados, sejam autônomos. A aplicação da gamificação pelas empresas pode melhorar a interação e o ambiente organizacional, entretanto, a utilização distorcida e excessiva evidencia o conceito de explorador e explorado no contexto trabalhista.

Assim, por meio da gamificação, explora-se a ideia de que não basta cumprir seu trabalho, mas também é preciso estar disponível, alcançar novas metas e, ainda, ser melhor que os demais para se manter em um topo fictício.

A princípio, gamificar estimula o alcance de mais metas por meio de bônus, prêmios, lanches e outras recompensas rápidas, para que trabalhadores não

5. “Sabe a foto de perfil que você usa em redes sociais, tais como Facebook, Instagram e Twitter? Ela é chamada de avatar. Ou seja, o termo significa a representação de uma pessoa na internet. O avatar faz parte da identidade e presença de alguém no universo digital. Também pode ser usada para se referir aos personagens escolhidos pelas pessoas em jogos online, por exemplo.” Fernando Souza. “Glossário de Marketing Digital”, publicado em 18 abril de 2019. Disponível em < <https://fernandosouza.com.br/glossario/avatar/>>. Acesso em 28 de Dez. de 2021.

6. Site da marca Oral-B, Disponível em < <https://oralb.com.br/pt-br/artigos-cuidado-bucal/perguntas-e-respostas-sobre-os-produtos>> Acessado em 03 de Jan. de 2022.

7. Art. 457 da CLT – “Compreendem-se na remuneração do empregado, para todos os efeitos legais, além do salário devido e pago diretamente pelo empregador, como contraprestação do serviço, as gorjetas que receber. (Redação dada pela Lei nº 1.999, de 1.10.1953) (...) § 4º Consideram-se prêmios as liberalidades concedidas pelo empregador em forma de **bens, serviços ou valor em dinheiro** a empregado ou a grupo de empregados, em razão de desempenho superior ao ordinariamente esperado no exercício de suas atividades. (Redação dada pela Lei nº 13.467, de 2017).” [grifo do autor]

se desconectem e ganhem um pouco mais. No entanto, o que se verifica, na prática, são autônomos, tidos por empreendedores, que se arriscam e prolongam suas atividades para além da fadiga física pela experiência do “jogo”. É a indução de uma rotina intensa, altamente competitiva por conta da grande oferta, que demanda duras jornadas e requer rapidez e habilidade.

Uma aplicação clara do conceito pode ser vista nas plataformas de entrega de comidas e transporte de passageiros, que estimulam o ambiente virtual de competição e pontos, Rui Maciel aponta que, “segundo queixas, as plataformas, com destaque para o *Rappi*, tendem a privilegiar os entregadores por sua pontuação nos *apps* e não necessariamente por sua localização. Além disso, eles afirmam que há penalização para quem fica desconectado dos *apps* por muito tempo ou recusam corridas.”⁸

Dentro da concepção gráfica e dos mecanismos da gamificação, a inteligência artificial, por meio de algoritmos, consegue manter as pessoas conectadas às metas que despertam o anseio por um prêmio. Trata-se de gatilhos psicológicos, por meio dos quais, quando o trabalhador está próximo de bater uma meta, outra surge com uma gratificação melhor, gerando uma motivação com rápida recompensa.

Segundo Delmar Rodrigues (ano 2018, p. 12), “ao ‘acreditar’ no que está sendo narrado ou exposto, o público se coloca em um estado de imersão, absorto que está naquele universo ficcional. De modo semelhante, Huizinga (ano 2001, p. 23) expressou o conceito de ‘círculo mágico’, que descreve a área em que o jogador se entrega voluntariamente para jogar, sem notar o que está ao seu redor.”

O estímulo excessivo, a vontade de alcançar mais objetivos e, no caso dos entregadores de aplicativo (*app*), a precarização por ausência de vínculo empregatício fazem com que não haja limitação das jornadas, não ocorra um descanso remunerado, entre outras garantias, como a manutenção da saúde. Quando ocorre um acidente, esse trabalhador-empendedor também arca com todos os riscos do negócio.

Este cenário não se aplica somente aos autônomos do setor de entregas. Eles ganharam evidência pela rápida projeção da precarização da mão-de-obra, mas, não muito longe, os empregados de carteira assinada – que tam-

8. Maciel, Rui. Deputados criam projetos de lei que preveem direitos aos entregadores de apps. Site: Canal Tech, 07 de Julho de 2020. Disponível em <<https://canaltech.com.br/legislacao/deputados-criam-projetos-de-lei-que-preveem-direitos-aos-entregadores-de-apps-167618/>> Acessado em 05 Jan. 2022.

bém sofrem os impactos da pouca oferta e grande demanda – igualmente se veem incitados a estar ao dispor em qualquer momento do dia. Veem, também, seu desempenho sempre medido e comparado com os demais, alimentando algum sistema de *feedback* positivo.

Muitas plataformas não são usadas para melhorarem a vida de seus trabalhadores, mas para alterar a percepção da condição em que se encontram. A gamificação tem todo um aparato para dar uma sensação de ganho. Ela fantasia o labor para ser recompensador, em vez de recompensar⁹.

3. Reflexo Social e Legislação

Na visão do filósofo contemporâneo Byung –Chul Han (2017, p.69), o capitalismo da emoção “gamifica o mundo do trabalho e da vida. O jogo emocionaliza e até dramatiza o trabalho, criando assim mais motivação. Através da rápida sensação de realização e do sistema de recompensas, as interfaces de trabalho exploram a sensação de jogo para gerar mais desempenho e rendimento.”. A mão-de-obra, “jogador”, fica muito mais entregue e absorto em suas metas que um trabalhador funcional que atua no nível emocional, batendo ponto e cumprindo sua jornada de 8 horas diárias e 44 horas semanais.

O capitalismo sempre busca meios de inovar e perpetuar sua lógica exploratória. Aproveita-se dos parâmetros da sociedade atual, que não aceita a exposição da negatividade, romantizando o trabalho como forma de status positivo, trazendo ao ápice a visão de ser empreendedor de si mesmo.

Byung–Chul Han traz em suas obras um pensamento que espelha esse sistema de trabalho e reforça a concepção de que “tão destrutiva quanto a violência da negatividade é a violência da positividade. (...) O sujeito do regime neoliberal perece com o imperativo da otimização de si, ou seja, ele morre da obrigação de produzir cada vez mais desempenho.”

Embora os elementos dessa discussão ganhem uma roupagem atual, ela repousa sobre normas e garantias que datam de antes da Constituição Federal de 1988. A saúde do trabalhador é um direito constitucionalmente assegurado e de interesse público e coletivo, uma vez que o financiamento da saúde pública é suportado por toda população¹⁰.

9. No sentido de trazer apenas a sensação de ganho, sem, de fato, trazer um retorno monetariamente mensurável.

10. “Parte do dinheiro utilizado para financiar o SUS vem de contribuições sociais de patrões e empregados, como o INSS (Instituto Nacional do Seguro Social). Outra parte vem do pagamento de impostos embutidos no preço de produtos e serviços

O cuidado com a saúde já era uma preocupação do constituinte de 1988, garantindo, ao longo da Carta Magna, alguns dispositivos que asseveram este direito. Dentro dos direitos sociais, o artigo 6º¹¹ garante saúde a todos, independentemente do exercício de um labor. O artigo 7º, caput e XXII traz direitos aos “trabalhadores urbanos e rurais, além de outros”¹² de forma a garantir um ambiente de trabalho seguro sem distinção. Além do artigo 7º, o artigo 225 garante um meio ambiente equilibrado, nele abrangido o meio ambiente do trabalho (artigo 200, VIII), cabendo ao “Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações”¹³.

O trabalhador é um espelho das suas condições de trabalho e a falta de descanso adequado entre suas jornadas resulta em um esgotamento físico e mental. É necessário assegurar que todos possam ser remunerados a ponto de poder usufruir de um descanso satisfatório.

A CF assegura em seu artigo 7º, inciso XV¹⁴, que o repouso semanal deve ser preferencialmente aos domingos. Já a Consolidação das Leis do Trabalho (CLT) em seus artigos 66 e 67¹⁵, além do artigo 1º da Lei 605/49¹⁶, também garante um descanso de no mínimo 11 horas entre jornadas e um repouso semanal remunerado de 24 horas consecutivas.

(Imposto sobre Circulação de Mercadorias e Prestação de Serviços – ICMS), IPI (Imposto de Produtos Industrializados), impostos sobre o lucro (Cofins), sobre os automóveis (IPVA) e sobre a moradia (IPTU). Ou seja, você também é responsável pela manutenção do sistema.” Disponível em <<https://drauziovarella.uol.com.br/saude-publica/como-funciona-o-sus/>>, acessado em 13 de Abr. de 2022;

11. “Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição. (Redação dada pela Emenda Constitucional nº 90, de 2015)”;

12. “Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social: XXII -redução dos riscos inerentes ao trabalho, por meio de normas de saúde, higiene e segurança;”

13. “Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.”

14. “Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social: XV -repouso semanal remunerado, preferencialmente aos domingos;”

15. “Art. 66 -Entre 2 (duas) jornadas de trabalho haverá um período mínimo de 11 (onze) horas consecutivas para descanso.”
“Art. 67 - Será assegurado a todo empregado um descanso semanal de 24 (vinte e quatro) horas consecutivas, o qual, salvo motivo de conveniência pública ou necessidade imperiosa do serviço, deverá coincidir com o domingo, no todo ou em parte.”

16. “Art. 1º da Lei 605/49: Todo empregado tem direito ao repouso semanal remunerado de vinte e quatro horas consecutivas, preferentemente aos domingos e, nos limites das exigências técnicas das empresas, nos feriados civis e religiosos, de acordo com a tradição local”.

O próprio ordenamento jurídico reconhece que aqueles que laboram¹⁷ devem ter propiciada a manutenção de seu bem-estar e proteção da saúde.

Além da dignidade humana, deve-se evitar o colapso de uma sociedade fadigada, autoexplorada, sem tempo para o ócio restaurador e que vive o auge dos índices de transtorno mental entre os brasileiros¹⁸. O trabalhador sem descanso remunerado tem que se manter à disposição para a próxima atividade que assegure sua renda. Ademais, há uma pressão por produção que impossibilita usufruir do descanso de maneira plena, desconectada e livre.

4. Limites da otimização do trabalho, precarização e direito à desconexão

A mesma tecnologia que permite um mundo de possibilidades ao homem é a mesma que o escraviza. Nas palavras de Jorge Luiz Souto Maior, “como se tem dito por aí à boca pequena, é o avanço tecnológico que está roubando o trabalho do homem, mas, por outro lado, como se verá, é a tecnologia que tem escravizado o homem ao trabalho”¹⁹.

Otimizar o trabalho, torná-lo mais agradável de ser realizado e motivar as pessoas a desempenharem melhor suas funções não são técnicas condenáveis, desde que respeitados os limites legais e a saúde do trabalhador. A tecnologia trouxe uma nova contradição para as relações empregatícias, uma vez que tanta facilidade e conexão permitiu ao trabalhador maior liberdade para decidir onde e como realizar suas tarefas, mas, também, o tornou dependente de estar disponível.

Em um país com altos índices de desemprego²⁰, a motivação externa, por meio de prêmios e status sociais, é um elemento extra. Existe uma massa que busca apenas manter o emprego, satisfazendo um sistema criado para iludi-

17. Tendo ele carteira assinada ou não. A intenção é abranger todo trabalhador, mesmo que travestido de empreendedor, é um trabalhador, muitas vezes, explorado pelo mesmo sistema.

18. Fonte: Pesquisa mostra que 86% dos brasileiros têm algum transtorno mental, Por Letícia Passos - Atualizado em 31 jul 2019, 17h58 - Publicado em 31 jul. 2019, 15h48, Leia mais em: <https://veja.abril.com.br/saude/pesquisa-indica-que-86-dos-brasileiros-tem-algum-transtorno-mental/> acessado em 04 de dez. de 2021;

19. SOUTO MAIOR, Jorge Luiz. Do Direito à Desconexão do Trabalho. São Paulo, 2003, p.01. Disponível em <https://www.jorgesoutomaior.com/uploads/5/3/9/1/53916439/do_direito_%C3%A0_desconex%C3%A3o_do_trabalho..pdf> Acessado em 03 de nov. 2021.

20. Fonte: Desemprego fica em 14,1% no trimestre encerrado em novembro, Editoria: Estatísticas Sociais | Uberlândia - Atualizado em 30/01/2021 17h02 - Publicado em 28/01/2021 09h00, Disponível em: <<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/29935-desemprego-fica-em-14-1-no-trimestre-encerrado-em-novembro>> Acessado em 03 de nov. 2021.

-los com uma sensação de realização, uma recompensa que lhes traz um êxito precário e passageiro, diminuindo seus direitos e os tornando exploradores de si mesmos.

Existe uma grande reflexão sobre o tema em que “a autoexploração é muito mais eficiente que a exploração estranha, pois caminha de mãos dadas com o sentimento de liberdade. Paradoxalmente, o primeiro sintoma de burnout é a euforia. Lançamo-nos eufóricos ao trabalho. Por fim acabamos quebrando.” (HAN, 2017, p.115).

Os conceitos abordados aplicam-se para trabalhadores informais, empregados e autônomos. Cada um, em um nível, está sob a influência desse moderno modo de viver neoliberal. De maneira geral, são estimulados a acreditar que o sucesso só depende deles mesmos.

Obviamente, todos desejam ter sucesso em sua área, um bom emprego, ou a realização de um sonho. Mas a modernidade tecnológica transforma o trabalho em status, conecta lazer e responsabilidades em um mesmo ambiente. O algoritmo é um chefe objetivo, que reconhece estrelas e não percebe a subjetividade da sua relação com seus “usuários”²¹.

A tecnologia não veio para libertar o homem, mas para aprisioná-lo, torná-lo mais dependente de trabalho. Nas palavras de Jorge Luiz Souto (2003), “esta preocupação é em si mesma um paradoxo, revelando, como dito, as contradições que marcam o nosso ‘mundo do trabalho’. A primeira contradição está, exatamente, na preocupação com o não-trabalho em um mundo que tem como traço marcante a inquietação com o desemprego.”

O panorama da autoexploração, baseada em mecanismos que estimulam a competitividade e a imersão no trabalho - gamificação - ganhou um amplo terreno e destaque por meio das plataformas de intermediação de trabalho, principalmente com relação aos entregadores e motoristas de aplicativo.

Essa mão-de-obra ganha por produção (entregas) pode decidir o quanto quer trabalhar, podendo começar, pausar e encerrar, quando quiser, seguindo sua própria programação. No entanto, o que se passou a ver foi um cenário diferente, marcado por um trabalho de baixa remuneração por entregas, necessárias longas jornadas, enorme temor de avaliações ruins, busca por elevar pontos e níveis dentro das interfaces e um trabalhador permanentemente conectado.

21. Referindo-se aos empregados ou trabalhadores que são submetidos às interfaces de trabalho gamificado.

Desconectar, usufruir de descanso satisfatório e aproveitar momentos de lazer, para quem trabalha sob demanda dos aplicativos, tornou-se um privilégio. De um direito a um privilégio, considerando a ótica de que o tempo de descanso não é remunerado e mais tempo à disposição para o trabalho, significa uma renda mais adequada.

A exploração do homem pelo capital é uma relação antiga, que sempre exigiu barreiras para conter sua ferocidade. Normas asseguradoras de condições mínimas às partes mais fracas, em regra, são reflexos de lutas por melhores condições. A legislação deve acompanhar o debate público e continuar assegurando direito ao trabalho seguro e digno.

No momento em que a sociedade desperta para as novas conjunturas de exploração, é necessário colocar as normas em debate. Neste sentido, foram propostos diferentes Projetos de Lei (PL) no Brasil, estimulando o debate e expondo o interesse em legislar acerca do tema. Sempre propondo adequações que perpassam aos pontos mais sensíveis, há projeto que requer o reconhecimento de vínculo de emprego com os entregadores de *app*, seguro de vida e danos ao veículo. Além de almejar essas garantias mínimas, trazem a questão do oferecimento de um espaço adequado e seguro para o descanso, alimentação, entre os serviços²².

A questão da proibição da aplicação do sistema de pontos para o recebimento de entregas dentro dos aplicativos²³ e limitações de jornada²⁴ também são pontos relevantes encontrados nessas propostas legislativas. Muitas, ainda aguardando tramitação, mas em sua maioria, já prejudicadas em decorrência da nova legislação, Lei nº 14.297, de 5 de janeiro de 2022, que traz inovações legislativas que visam garantir mais proteção aos trabalhadores de plataformas de entrega.

A plataforma UBER já utiliza uma ferramenta que limita o tempo online do motorista dirigindo usando o aplicativo, desconectando automaticamente o

22. Projeto de Lei 3577/20, deputado federal Márcio Jerry (PCdoB-MA), “Art. 350-B. §1º Caberá à empresa operadora de aplicativo de entrega assegurar ao entregador: a) alimentação e água potável; b) espaço seguro para descanso entre as entregas.” Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909106&filename=PL+3577/2020> Acessado em 12 abr. 2022.

23. Projeto de Lei 3597/20, deputado Bira do Pindaré (PSB/MA). Disponível em <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256636>> Acessado 12 abr.2022.

24. Art. 7º O horário de trabalho do ciclista não será superior a 10 (dez) horas diárias, cabendo à empresa de plataforma digital o controle dessa jornada por intermédio do sistema de aplicativo.” Projeto de Lei 3599/20. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909567&filename=PL+3599/2020> Acessado em 05 nov. 2021.

motorista que alcançar 12 horas de uso contínuo. A plataforma argumenta ter adotado a medida pensando em uma maior segurança no trânsito, não afastando que o excesso de jornada é prejudicial à saúde do parceiro da plataforma e impacta toda sociedade. Sob este aspecto, a plataforma notificou o que se segue:

A nova ferramenta vai fornecer notificações ao motorista quando ele se aproximar do limite de 12 horas online conduzindo o veículo em um único dia. Atingido esse limite, ele será automaticamente desconectado e não poderá utilizar o aplicativo pelas seis horas seguintes. Passado esse período, o motorista pode ficar online novamente para receber solicitações de viagem. A ferramenta mostra o tempo online erodando, facilitando que o motorista tenha visibilidade do período de tempo que está dirigindo usando a plataforma da Uber.²⁵

Não obstante muitos desses projetos de lei também sejam passíveis de críticas por continuarem a proteger mais as plataformas do que a vida daqueles que se arriscam na prestação do serviço, é notório o crescimento em torno de novas formas de proteger os trabalhadores.

Internacionalmente, também há inúmeras discussões e algumas cidades já começaram estabelecer direitos mínimos. Na cidade de Nova York, Estados Unidos, no dia 23 de setembro de 2021, aprovou-se uma nova legislação que busca estabelecer condições mínimas para trabalhadores de aplicativo, bem como, firmar o compromisso das autoridades públicas em realizarem um estudo de mercado para compreender melhor o negócio de delivery. Entre as garantias da nova legislação nova-iorquina, destaca-se o dever de informação aos entregadores quanto à distância da corrida, tempo de viagem, endereço de retirada e entrega do produto, cláusulas contratuais que asseguram utilizar o banheiro do local da prestação de serviço e maior transparência nas compensações e informações das gorjetas²⁶.

Já em Washington, outro estado norte-americano, foi sancionada a lei que garante um pagamento mínimo para motoristas das empresas de transporte

25. “Uber lança ferramenta que limita o tempo online do motorista dirigindo usando o aplicativo para promover segurança viária”, UberNewsroom, publicado em 04/03/2020; Disponível em: <<https://www.uber.com/pt-BR/newsroom/uber-lanca-ferramenta-que-limita-o-tempo-online-do-motorista-dirigindo-usando-o-aplicativo-para-promover-seguranca-viaria/>> Acessado em 08 de Jan. 2022.

26. “Nova York aprova lei que prevê direitos para entregadores de delivery” Thiago Lavado – Revista Eletrônica Exame, 24/09/2021. Disponível em <<https://exame.com/tecnologia/nova-york-aprova-lei-que-preve-direitos-para-entregadores-de-delivery/>> Acesso em 13 de Abr. 2022.

por aplicativo, a princípio Uber e Lyft. Os motoristas passam a receber um valor mínimo de 1,17 dólar por milha (1,6 quilômetro) percorrida, garantindo também um pagamento mínimo de 3 dólares por viagem. Além de prever licença médica remunerada e poderem questionar caso tenham seus cadastros removidos dos aplicativos.

A própria sociedade empresária Uber esteve envolvida na negociação e tramitação deste projeto de lei, o qual estabelece que os direitos vão ser gradualmente aplicados e assegura a manutenção da autonomia, afastando o reconhecimento de qualquer vínculo empregatício²⁷.

No Brasil, a mais recente norma nesse sentido foi a lei nº 14.297, de 5 de janeiro de 2022²⁸, sancionada pelo Presidente da República, a qual prevê, entre outras disposições, que as empresas que se utilizam dos aplicativos de entrega deverão fornecer aos entregadores itens como água potável, álcool em gel e máscaras, além de acesso aos banheiros das empresas. Já as plataformas devem contratar um seguro contra acidentes, sem franquia, que deverá ser fornecido em nome do entregador.

O artigo 8º da lei nº 14.297/22²⁹ estabelece que as hipóteses de bloqueio, de suspensão ou de exclusão da conta do entregador da plataforma eletrônica devem ser fundamentadas, trazendo mais uma maior segurança e transparência para os parceiros.

Embora, lentamente, essa nova dinâmica de relação de trabalho vá ganhando amparo legal e garantias mínimas, ainda há muito o que discutir quanto ao tema. A recente lei em nada trata de limites à jornada de trabalho ou a um descanso remunerado que permita a desconexão.

Mesmo que para muitos a visão empreendedora de flexibilidade e “ausência de patrão” soem como conquistas, trata-se apenas de uma ilusão da sociedade do desempenho, que explora o trabalho “*enquanto joga*” (B. C. Han, 2018).

27. “Motoristas de Washington ganham garantia e benefícios históricos de novos ganhos” – Uber Blog, 01/03/2022. Disponível em <<https://www.uber.com/blog/washington-driver-flexibility-law/>> Acesso em 13 de abr. 2021.

28. BRASIL. Lei nº14.297, de 5 de janeiro de 2022. Disponível em <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Lei/L14297.htm> Acessado em 07 jan. 2022.

29. Art. 8º Do contrato ou do termo de registro celebrado entre a empresa de aplicativo de entrega e o entregador deverão constar expressamente as hipóteses de bloqueio, de suspensão ou de exclusão da conta do entregador da plataforma eletrônica. § 1º A aplicação da exclusão de conta prevista no caput deste artigo será precedida de comunicação prévia, com antecedência mínima de 3 (três) dias úteis, e será acompanhada das razões que a motivaram, que deverão ser devidamente fundamentadas, preservadas a segurança e a privacidade do usuário da plataforma eletrônica. § 2º O prazo previsto no § 1º deste artigo não se aplica aos casos de ameaça à segurança e à integridade da plataforma eletrônica, dos fornecedores e dos consumidores, em razão de suspeita de prática de infração penal prevista na legislação vigente.

Considerações Finais

Ante a tudo que foi exposto, se faz necessário refletir sobre os impactos que a era digital trouxe para as novas dinâmicas de trabalho. O marco tecnológico expõe, ainda mais, uma sociedade consumista, marcada pela desigualdade, que ao mesmo tempo que é transformada e facilitada pela tecnologia, também amplia relações precarizadas.

O excesso de estímulos ao trabalho conectado, que induz uma entrega e a permanente conexão são as novas faces das relações de trabalho, mas devem possuir limites que respeitem a dignidade humana e a saúde do trabalhador. Uma força de trabalho fadigada e adoecida por excessos de jornada e pouco descanso é um retrato social que, historicamente, vem sendo discutido e amparado por direitos trabalhistas.

As legislações acerca das relações de emprego, tendo a Constituição Federal fonte garantidora, já preveem e delimitam as jornadas laborais, entretanto, a sociedade avança, se modifica e o trabalho não se limita mais a um espaço e período pré-fixados. Não há como conter o avanço das plataformas de intermediação de trabalho, porém, é imperioso garantir que o debate normativo acompanhe os avanços e permaneça garantindo proteção aos trabalhadores.

Essas ações possuem reflexos na saúde dos trabalhadores e, consequentemente, levantam a questão de como isso irá afetar a geração futura e como a sociedade irá arcar com as consequências.

No futuro, a massa trabalhadora será composta por jovens, muitos deles vivendo em um contexto social de ansiedade, presos em um cenário de empreendedorismo profissional, que estimula o pensamento de que basta se esforçar.

As interfaces digitais de trabalho que se utilizam de mecanismos de engajamento para estímulo da força de trabalho precisam ter limites para a jornada e demandas. O excesso de trabalho decorre de outras variantes, como alto índice de desemprego e baixa remuneração, que favorecem o cenário de autoexploração para obtenção de uma renda mínima capaz de manter uma renda mínima.

A gamificação é um mecanismo de engajamento muito útil, se bem direcionado. Todavia, é preciso atentar-se para as distorções nas relações de trabalho, o impacto desses mecanismos na saúde dos trabalhadores e o direito ao “não-trabalho” (Souto Maior, 2003) por meio do ócio e da desconexão, para equilíbrio das forças.

O debate jurídico e a legislação trabalhista precisam permitir que inovações benéficas sejam cultivadas, mas devem buscar conter o adoecimento da força produtiva. Nas palavras de Byung-Chul Han (2017, p.113), “A própria pausa se conserva implícita no tempo de trabalho. Ela serve apenas para nos recuperar do trabalho, para poder continuar funcionando.”

Referências

BASTOS, Catia Cristina de Araujo Quarterolli e SILVA, José Alexsandro da. Resenha – “GIG – A Uberização do Trabalho” (2019) – uma análise sob a psicopolítica segundo Byung-Chul Han, 21 de maio de 2020. Disponível em: <<https://trab21.blog/2020/05/21/resenha-gig-a-uberizacao-do-trabalho-2019-uma-analise-sob-a-psicopolitica-segundo-byung-chul-han/>> Acessado em 04 de nov. 2020

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acessado em 04 de nov. 2021

BRASIL. Decreto-lei nº 5.452, de 1º de maio de 1943. Consolidação das Leis do Trabalho. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm> Acessado em 04 de nov. 2021

BRASIL. Lei nº 605, de 5 de janeiro de 1949. Repouso semanal remunerado e o pagamento de salário nos dias feriados civis e religiosos. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l0605.htm> Acessado em 04 de nov. 2021;

BRASIL. Site do Tribunal Superior do Trabalho. Disponível em <<https://www.tst.jus.br/documents/10157/429ac88e-9b78-41e5-ae28-2a5f8a27f1fe>> Acessado em 04 de nov. 2021

BRASIL. Lei nº 14.297, de 5 de janeiro de 2022. Disponível em <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Lei/L14297.htm> Acessado em 07 jan. 2022.

FAVA, Fabrício. A emergência da gamificação na cultura do jogo, autor Fabricio Fava, pág.51 - Citação direta: Gamificação em debate 2018 Lucia Santaella, Sérgio Nesteriuk, Fabricio Fava (organizadores) Editora Edgard Blücher Ltda, ano 2018

HAN, Byung-Chul. *No enxame*: perspectivas do digital. Tradução de Lucas Machado, Petrópolis, Rj: Vozes, 2018

HAN, Byung-Chul. Psicopolítica – O neoliberalismo e as novas técnicas de poder. Belo Horizonte, Editora Âyiné, 2018

HAN, Byung-Chul. *Sociedade do Cansaço*. Tradução de Enio Paulo Giachini; 2ª edição ampliada -Petrópolis, Rj: Vozes, 2017

HUIZINGA, J. *Homo ludens: o jogo como elemento da cultura*. São Paulo: Perspectiva, 2001.

GABRIEL, Marcos. Ser entregador por aplicativo: quando sua vida vale menos do que uma entrega. Disponível em: < <https://avoador.com.br/opiniaio/ser-entregador-por-aplicativo-quando-sua-vida-vale-menos-do-que-uma-entrega/>>. Acessado em 04 de nov. 2021

SILVA, Paulo Henrique Franqueira e. Aplicativo de aperfeiçoamento pessoal com elementos de gamificação [manuscrito]/ Paulo Henrique Fraqueira e Silva –2016. Disponível em: <https://www.monografias.ufop.br/bitstream/35400000/223/6/MONO-GRAFIA_AplicativoAperfei%C3%A7oamentoPessoal.pdf>. Acesso em: Acessado em 03 de nov. 2021

SOUTO MAIOR, Jorge Luiz. *Do Direito à Desconexão do Trabalho*. São Paulo, 2003, p.01. Disponível em <https://www.jorgesoutomaior.com/uploads/5/3/9/1/53916439/do_direito_%C3%A0_desconex%C3%A3o_do_trabalho..pdf> Acessado em 03 de nov. 2021

SOUZA, Edney. A incrível gamificação da Rappi – uma estratégia de retenção para conquistar o mercado. Consultoria InterNey, 19 de abril de 2019. Disponível em: <<https://interney.net/2019/04/19/a-incrivel-gamificacao-da-rappi-uma-estrategia-de-retencao-para-conquistar-o-mercado/>>. Acesso em: Acessado em 05 de jan. 2021

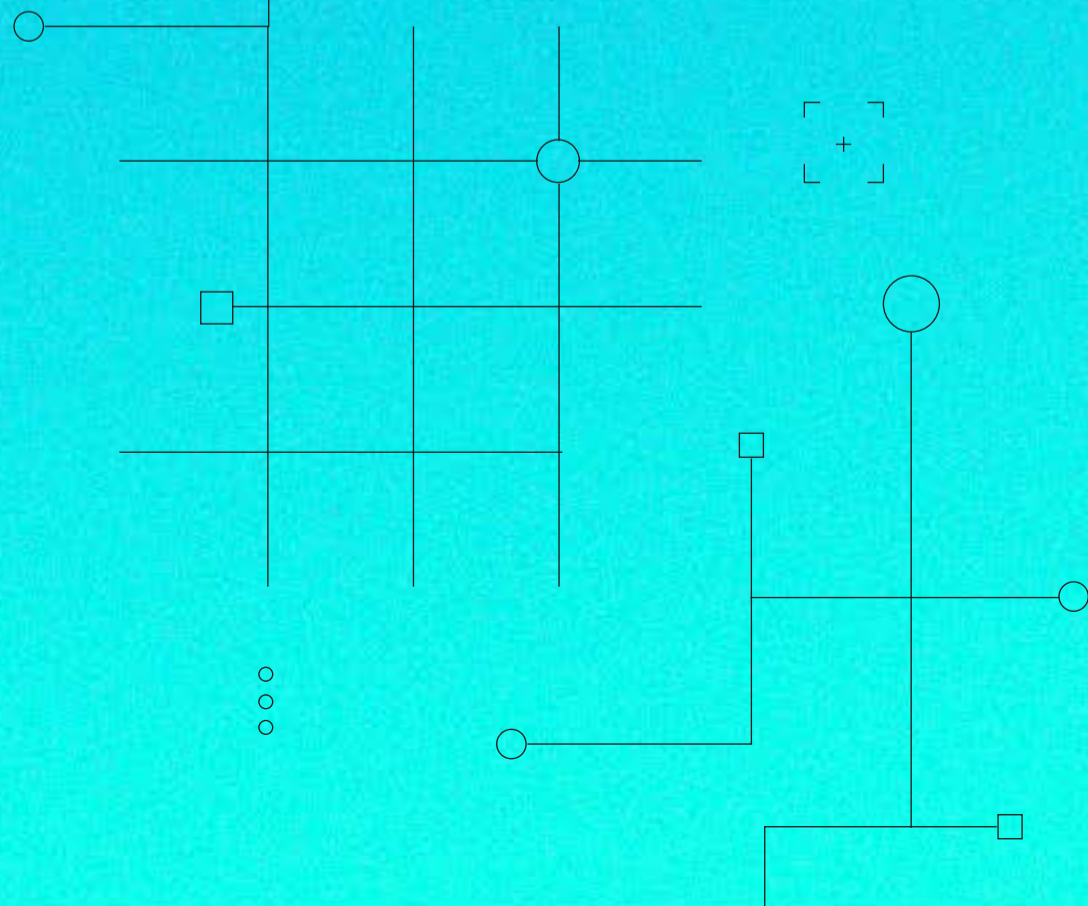
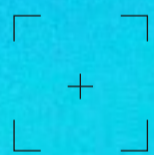
STANDING, Guy. *O precariado: a nova classe perigosa*. Tradução Cristina Antunes. Belo Horizonte: Autêntica Editora, 2019

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

10

Cenário atual das ordens globais de remoção de conteúdo na internet: aliadas ou adversárias dos usuários?

LARISSA SAD COELHO



Sumário: Introdução. 1. Visão comparativa das decisões que se tornaram referência na matéria. 2. Benefícios da atribuição de efeitos globais a ordens de remoção de conteúdo online. 3. Problemas decorrentes da atribuição de efeitos globais a ordens de remoção de conteúdo online. Considerações finais. Referências.

Introdução

Ferramentas de busca, como “Google.com”, se tornaram o primeiro destino de qualquer pessoa que tenha uma dúvida ou queira saber um pouco mais sobre determinado assunto, qualquer que seja a área do conhecimento em que esteja inserido. Rapidamente, filtra-se com os olhos, entre os resultados obtidos, aqueles de fontes conhecidas ou que pareçam confiáveis. De maneira geral, não tardaria muito para que esse usuário hipotético estivesse satisfeito com o conteúdo a que teve acesso. Talvez ele não perceba que, por diversas razões, como infrações de propriedade intelectual ou exercício do direito ao esquecimento, determinado resultado pode ter sido omitido do buscador por ordem judicial.

A remoção desse conteúdo pode significar a salvaguarda de direitos subjetivos importantes para a empresa que teve sua propriedade intelectual infringida ou para a pessoa que se sentia lesada com a divulgação de uma informação considerada irrelevante ou desatualizada². Por outro lado, pode significar também uma limitação imposta à pesquisa daquele primeiro usuário, ou seja, ao seu direito de acesso à informação e à liberdade de expressão do autor do conteúdo suprimido.

Dentro de um mesmo país ou região, faz sentido embarcar-se na árdua tentativa de equilíbrio do direito de acesso à informação, do interesse público em sua divulgação, da liberdade de expressão e do interesse econômico da ferramenta de busca ou rede social com a proteção do(s) direito(s) subjetivo(s) que justifica(m) a remoção desse conteúdo. Todavia, plataformas digitais, como buscadores e redes sociais, são atores globais e se utilizam de instrumentos

1. Advogada. Mestranda em Advocacia Internacional e Resolução de Disputas na Universidad Carlos III de Madrid, na Espanha. Aluna da Pós-graduação em Direito Digital (ITS Rio e UERJ). Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ), com experiência acadêmica na Université de Liège, na Bélgica.

2. Sobre o direito ao esquecimento, ver julgamento do caso paradigma na Europa: *Google Spain v. Mario Costeja Gonzales*. UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González, 13/05/2014, C-131/12. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>>. Último acesso em: 17 abr. 2022.

globais. A moderação de conteúdo realizada por essas plataformas, de acordo com seus valores e seus termos de uso internacionais, alcança repercussões globais, naturalmente, ao se aplicar para toda a empresa. Uma decisão tomada pelo Comitê de Supervisão da Meta³⁻⁴, por exemplo, produz efeitos no mundo inteiro, ainda que esse não seja um órgão judicial, tampouco de direito internacional⁵.

Isso faz com que magistrados de diferentes países decidam – seja por meio de decisão fundamentada, seja por desconhecimento da matéria – que suas ordens judiciais também tenham efeitos processuais extraterritoriais na internet, ultrapassando os limites de sua jurisdição. Historicamente, não havia necessidade de definir-se a extensão de decisões judiciais, pois o poder coercitivo de um Estado estava, naturalmente, restrito às suas fronteiras. Assim, para fazer com que uma decisão surtisse efeitos no mundo inteiro, seria necessário acionar cortes de cada um dos países em questão ou, excepcionalmente, recorrer a um tribunal internacional.

Sem embargo, com ferramentas de busca e redes sociais globais, surgiu aos judiciários locais a possibilidade de impor-se coercitivamente uma decisão para toda a empresa envolvida, em vários países do mundo, ainda que, tecnicamente, não se utilize um instrumento processual adequado para tanto.

Dessa forma, qual deve ser o alcance territorial do instrumento que efetiva decisões judiciais de desindexação de conteúdo? Da perspectiva do usuário, seria benéfico, por exemplo, um juiz brasileiro requerer a retirada do ar de determinada informação para o mundo inteiro, ou seja, proferir uma ordem global?

O presente artigo estuda as ordens globais de remoção de conteúdo na internet. Em primeiro lugar, (1) busca-se sistematizar o que foi decidido em alguns dos principais casos sobre a matéria. Depois, analisa-se, sob o ponto de

3. Mais informações sobre o Comitê de Supervisão, um órgão privado, estão disponíveis em: <<https://oversightboard.com/>>. Último acesso em: 17 abr. 2022.

4. Para um estudo dos eventos e influências que levaram à criação do Comitê de Supervisão, ver KLONICK, Kate. The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *Yale Law Journal*, Vol. 129, No. 2418, 2020. Disponível em: <<https://ssrn.com/abstract=3639234>>. Último acesso em: 17 abr. 2022.

5. A decisão que suspendeu as contas do Facebook e do Instagram do ex-presidente Trump, após suas publicações sobre a invasão do Capitólio, em Washington DC, em janeiro de 2021, é um exemplo disso. A íntegra dessa decisão (FB-691QAMHJ) está disponível em: <<https://oversightboard.com/decision/FB-691QAMHJ/>>. Último acesso em: 17 abr. 2022.

vista da proteção de direitos dos usuários, (2) as vantagens e (3) os prejuízos dessas ordens com efeitos globais. Por fim, expõem-se ponderações conclusivas.

1. Visão comparativa das decisões que se tornaram referência na matéria

Antes de adentrar-se os principais argumentos a favor e contra os efeitos globais de decisões que determinam a remoção de conteúdo online, passa-se a um breve resumo do que foi privilegiado nos julgamentos mais comentados sobre o tema até o momento. Este capítulo pretende servir como uma ferramenta de consulta para o(a) leitor(a).

Com o objetivo de permitir uma visão comparativa das principais decisões que julgaram a questão, apresenta-se, a seguir, em forma de quadro, uma síntese de seus dispositivos. Destaca-se que esse exame pretende ser sintético, por isso deixa de abordar outros casos também relevantes sobre o tema⁶. Observa-se, ainda, que a análise feita na última coluna, com relação ao posicionamento geral da decisão, se a favor ou contrária à produção de efeitos extraterritoriais, refere-se apenas à interpretação e à opinião da autora, constituindo apenas um dos múltiplos pontos de vista sob os quais essas decisões podem ser examinadas.

6. A Internet & Jurisdiction Policy Network mantém uma base de dados bem completa, com casos envolvendo internet ocorridos em todo o mundo. *I&J Retrospect Database*. Disponível em: <<https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6ljlwMjEtMTIifQ==>>. Último acesso em: 17 abr. 2022.

QUADRO I - Sistematização das principais decisões em matéria de efeitos extraterritoriais de ordens de remoção de conteúdo na internet.

Data	Caso	Jurisdição, órgão julgador	Resumo da decisão	Posição em relação aos efeitos extraterritoriais
16/06/2020	Id SAIJ: SUD0303370	ARGENTI-NA, Câmara Penal e Correccional Federal	Em prestígio ao princípio da territorialidade da lei, a ampliação da medida liminar teve seus efeitos revogados. A Câmara entendeu que a extensão da medida liminar, para que o bloqueio de sites ou serviços produzisse efeitos globais, violaria a lei estrangeira, excederia os poderes dos magistrados argentinos e criaria uma interferência intolerável na liberdade de expressão e no direito de buscar, receber e transmitir informações livremente ⁷ .	Contrária à produção de efeitos extraterritoriais.
10/12/2019	Clóvis de Barros Filho v. Google Brasil Internet Ltda., Agravo de Instrumento nº 2129648-38.2019.8.26.0000	BRASIL, Tribunal de Justiça do Estado de São Paulo	A 9ª Câmara de Direito Privado manteve a ordem de remoção global de um vídeo considerado ilícito, com o objetivo de proteger a intimidade das partes ofendidas com sua divulgação. Entendeu-se que a remoção apenas no Brasil não seria suficientemente eficaz e que não haveria justificativa para a continuidade de acesso por estrangeiros (ou pessoas fora do território nacional). Também se concluiu que não haveria ofensa aos princípios da soberania ou da territorialidade, uma vez que o conteúdo está hospedado dentro do território nacional. Destacou-se, no voto vencedor, a possibilidade de acesso ao conteúdo, no Brasil, por brasileiros, que fazem uso de mecanismos técnicos capazes de emular sua localização – como <i>proxy</i> e VPN (<i>Virtual Private Network</i> ou Rede Virtual Privada) – navegando como se estivessem fora do Brasil.	A favor da produção de efeitos extraterritoriais.

7. Em sentido contrário, nota-se uma tendência crescente entre países latino-americanos de estender seus poderes para além de seus territórios, por meio de leis, visando a preencher a lacuna de governança e regulação internacional na internet. United Nations Economic Commission for Latin America and the Caribbean (ECLAC). *Informe Sobre la Situación Regional 2020*. Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y El Caribe (Cepal), nov. 2020, p. 100. Disponível: <<https://www.internetjurisdiction.net/uploads/pdfs/Informe-sobre-la-situacio%CC%81n-regional-2020.pdf>>. Último acesso em: 17 abr. 2022.

03/10/2019	Eva Glawisch-nig-Piesczek v. Facebook Ireland Limited C-18/18 ⁸	UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia	A Diretiva 2000/31 da UE (sobre comércio eletrônico) não prevê qualquer limitação territorial ao alcance das medidas que os Estados-membros têm o direito de adotar em conformidade com essa diretiva. Isto é, Estados-Membros da UE podem ordenar a um provedor de hospedagem, como o Facebook, que remova informações cobertas pela ordem judicial em questão ou que bloqueie o acesso a essas informações no mundo inteiro dentro da estrutura de direito internacional relevante.	Intermediária. A favor da produção de efeitos extraterritoriais apenas em determinados casos, se compatível com o direito internacional.
24/09/2019	CNIL v. Google France C-507/17	UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia	A lei da União Europeia não obriga a Google a aplicar o direito europeu ao esquecimento globalmente. Esse direito se aplica dentro das fronteiras dos 28 países membros do bloco. Ou seja, operadores de internet são obrigados a removerem os links em questão de todas as extensões do site na União Europeia, independentemente do país em que a demanda se originou. Além disso, precisam adotar medidas para prevenir ou desincentivar seriamente que usuários localizados na União Europeia tenham acesso a esse conteúdo ao usarem uma versão do mecanismo de busca de fora da EU. Entretanto, de maneira geral, a decisão defende a legalidade de ordens globais de remoção de conteúdo e esclarece que Estados-membros continuam competentes para ordenar a desindexação global, por meio de cortes nacionais ou de autoridades nacionais de proteção de dados. Ou seja, a lei da UE tampouco proíbe a remoção global.	Intermediária. A favor da produção de efeitos extraterritoriais se permitido no ordenamento nacional em questão. O direito europeu não obriga nem proíbe a produção de efeitos globais.
28/06/2017	Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, [2017] 1 S.C.R. 824	CANADÁ, Suprema Corte do Canadá	Mantida a medida cautelar mundial contra a Google, que obriga a desindexação global dos sites de empresa infratora de propriedade intelectual. Além disso, o ônus de provar a existência de conflito de leis, ou seja, que, ao cumprir com essa decisão, a Google estaria violando leis de outras jurisdições, é da própria intermediária.	A favor da produção de efeitos extraterritoriais.

8. Ver CAVALIERE, Paolo. Glawisch-nig-Piesczek v. Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations. *European Data Protection Law Review*, v. 5, n. 4, 2019, pp. 573–578. Disponível em: <<https://ssrn.com/abstract=3519389>>. Último acesso em: 17 abr. 2022.

22/05/2000	LICRA & UEJF v. Yahoo! Inc. & Yahoo France	FRANÇA, Tribunal de Grande Instância de Paris	<p>Condenação do Yahoo! Inc. a adotar todas as medidas à sua disposição para dissuadir e tornar impossível toda visita ao Yahoo.com para participar do serviço de leilão de objetos nazistas, bem como para tornar impossível qualquer outro site ou serviço que faça apologia ao nazismo ou que defenda crimes nazistas.</p> <p>Ao Yahoo France, por sua vez, foi ordenada a obrigação de incluir um aviso aos usuários do Yahoo.fr, quando o resultado de sua pesquisa levar a conteúdo que constitui uma infração à lei francesa, de que a navegação deve ser interrompida, sob pena de incorrer em sanções estipuladas pela legislação francesa⁹.</p>	A favor da produção de efeitos extraterritoriais.
------------	--	---	--	---

2. Benefícios da atribuição de efeitos globais a ordens de remoção de conteúdo online

É certo que a divisão geopolítica do mundo em jurisdições não subsiste na internet, uma tecnologia essencialmente internacional (GEIST, 2001; SLANE, 2008)¹⁰. Os cabos que permitem conexões instantâneas entre as mais diferentes regiões do globo¹¹ não diferenciam os limites geográficos de cada país. Por essa razão, na prática, decisões judiciais que antes ficavam restritas ao território de cada nação podem alcançar, na internet, efeitos além das fronteiras nacionais¹², ainda que não esteja previsto um instrumento processual adequa-

9. Essa decisão foi muito criticada nos Estados Unidos, principalmente em razão das diferenças com que a liberdade de expressão é entendida em cada jurisdição. Alguns autores argumentam que o Tribunal de Grande Instância de Paris deveria ter observado o art. 10 da Convenção Europeia dos Direitos Humanos, supostamente mais protetivo. Nesse sentido: OKONIEWSKI, Elissa A. Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet. *American University International Law Review*, v. 18, n. 1, 2002, pp. 295-339. Disponível em: <<https://digitalcommons.wcl.american.edu/auilr/vol18/iss1/6/>>. Último acesso em: 17 abr. 2022.

10. Alguns autores defendem que a falta de fronteiras na internet impede que leis físicas sejam aplicáveis. GEIST, Michael A. Is There a There There? Toward Greater Certainty for Internet Jurisdiction, *Berkeley Technology Law Journal*, vol. 16, n. 3, out. 2001, pp. 1356-1357, p. 11. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=266932>. Último acesso em: 17 abr. 2022; SLANE, Andrea. Tales, Techs and Territories: Private International Law, Globalization, and the Legal Construction of Borderlessness on the Internet. *Law and Contemporary Problems*, v. 71, jul. 2008, pp. 129-152. Disponível em: <<https://scholarship.law.duke.edu/lcp/vol71/iss3/6>>. Último acesso em: 17 abr. 2022.

11. Um mapa desses cabos submarinos pode ser acessado em: <<https://www.submarinecablemap.com/>>. Último acesso em: 17 abr. 2022.

12. Exemplo claro disso foi a repercussão das ordens judiciais brasileiras de bloqueio ao WhatsApp em países vizinhos. Desde 2015, houve alguns casos em que juízes brasileiros determinaram a operadoras de conexão (empresas de telefonia) que bloqueassem o WhatsApp no Brasil, para exigir a entrega de dados que não estavam à sua disposição, em razão da criptografia ponta-a-ponta ou do armazenamento no exterior. Apesar de a suspensão ter como alvo o território brasileiro, outros países da América Latina foram afetados, como Chile, Argentina e Paraguai, pois a tecnologia em questão não é limitada às dimensões geográficas dos países. Esses bloqueios são discutidos no Supremo Tribunal Federal (STF), na ADPF 403 e na ADI 5527. Sobre os impactos no Chile, ver: Whatsapp es suspendido en Brasil y problemas con enlace

do. Este capítulo trata dos efeitos favoráveis ao usuário, gerados por ordens globais de remoção de conteúdo na internet.

A principal razão que motiva uma autoridade local a expedir uma ordem de retirada de conteúdo com efeitos extraterritoriais consiste na própria proteção do direito material subjacente. Isso porque, ao limitar-se o instrumento de efetivação dessa ordem – na extensão de sua jurisdição –, é evidente que também se restringe o escopo territorial de aplicação do direito subjetivo que justifica a remoção do conteúdo. Assim, por vezes, a limitação do alcance dos efeitos da decisão ao território nacional ou regional faz com que esse direito material não seja adequadamente assegurado, justamente pelo caráter mundial da internet.

Para dar um exemplo concreto, no caso *Google v. CNIL*¹³, a CNIL (autoridade francesa de proteção de dados) defendeu que a Google deveria retirar do ar os links em questão universalmente, para que o direito ao esquecimento de determinado usuário fosse efetivo. A autoridade considerou que a retirada dos links de todas as extensões do buscador na União Europeia (“UE”) e o bloqueio de acesso a partir do território francês aos links em extensões fora da União Europeia eram medidas insuficientes para proteger o direito do indivíduo, violando a Diretiva¹⁴ que o previa.

Nesse sentido, ao decidir por uma ordem que respeite o escopo territorial de sua jurisdição, determinada autoridade local corre o risco de não conferir proteção suficiente aos seus jurisdicionados, conforme os parâmetros da legislação aplicável. Como pontuou o Tribunal de Justiça da União Europeia, ao julgar o caso mencionado no parágrafo anterior:

Em um mundo globalizado, o acesso de usuários da internet – incluindo aqueles fora da UE – a um link referente a informações sobre uma pessoa cujo

internacional afecta al servicio en Chile. *Diario Financiero*. Disponível em: <<https://www.df.cl/empresas/telecom-tecnologia/whatsapp-es-suspendido-en-brasil-y-problemas-con-enlace-internacional#:~:text=Telecom%2FTecnolog%C3%ADa-,Whatsapp%20es%20suspendido%20en%20Brasil%20y%20problemas%20con%20enlace%20internacional,de%20mensajer%C3%ADa%20de%20manera%20normal>>. Acesso em: 17 abr. 2022.

13. *Google v. CNIL*. UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Google LLC v. Commission nationale de l’informatique et des libertés (CNIL)*, 24/09/2019, C-507/17. Disponível em: <<https://curia.europa.eu/juris/document/document.jsf?docid=218105&doclang=EN>>. Último acesso em: 17 abr. 2022.

14. Diretiva de proteção de Dados Pessoais na União Europeia. Diretiva 95/46/EC de 24/10/1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>>. Último acesso em: 17 abr. 2022. Como essa diretiva foi revogada em 25 de maio de 2018, sendo substituída pelo GDPR, o caso foi analisado com base em ambos os diplomas legislativos.

centro de interesses está situado na UE provavelmente causará efeitos imediatos e substanciais sobre essa pessoa dentro da UE¹⁵.

Implicitamente, declarações como essa sugerem que o direito material em questão só pode ser verdadeiramente protegido se a ordem de remoção do conteúdo for global (SAMONTE, 2019).

Dessa forma, por não estar prevista proteção internacional do direito subjetivo em questão nos mesmos padrões garantidos pela proteção local, o que ocorre com frequência – especialmente em matéria de proteção de dados pessoais, por sua regulação recente –, jurisdições nacionais são tentadas a implementar suas regulamentações globalmente, com o objetivo de proteger seus cidadãos¹⁶.

Esse, contudo, não é o único motivo pelo qual a necessidade de uma ordem global de remoção de conteúdo online pode ser justificada. No caso *Google Inc. v. Equustek Solutions Inc.*¹⁷, o direito material em questão – uma série de direitos de propriedade intelectual – já estava assegurado por tratados internacionais, essa era uma questão incontroversa¹⁸. Ainda assim, discutia-se a possibilidade ou não de uma decisão da Suprema Corte de British Columbia produzir efeitos extraterritoriais. Isso porque, apesar de a empresa cuja propriedade intelectual estava sendo violada ter sede no Canadá, a empresa infratora continuava vendendo os produtos impugnados em seus sites, para consumidores de todo o mundo, a partir de uma localidade desconhecida, fora do Canadá. Portanto, uma decisão que obrigasse a Google a cessar a indexação de certos resultados em seu buscador, mas que estivesse limitada ao território canadense, certamente não seria efetiva contra a contrafação perpetrada no mundo inteiro.

15. Tradução livre do parágrafo 57 do julgamento: “In a globalised world, internet users’ access – including those outside the Union – to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself.” (*Google v. CNIL*. UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Google LLC v. Commission nationale de l’informatique et des libertés* (CNIL), 24/09/2019, C-507/17).

16. Ainda no caso *Google v. CNIL*, o Tribunal de Justiça da União Europeia afirmou que seria justificável a presença de uma competência, por parte do legislador da UE, para estabelecer a obrigação, para um operador de mecanismo de busca, de realizar, ao conceder um pedido de supressão de referências, a supressão em todas as versões do seu mecanismo de busca (*Google v. CNIL*, parágrafo 57. UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Google LLC v. Commission nationale de l’informatique et des libertés* (CNIL), 24/09/2019, C-507/17).

17. *Google Inc. v. Equustek Solutions Inc.* CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc.*, 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824. Disponível em: <<https://canlii.ca/t/h4jg2>>. Último acesso em: 17 abr. 2022.

18. A Google concordou que a maioria dos países provavelmente reconhecerá direitos de propriedade intelectual e verá a venda de produtos piratas como um crime (*Equustek Solutions Inc. v. Jack*, parágrafo 144. CANADÁ, Suprema Corte de British Columbia, *Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc. v. Morgan Jack, Andrew Crawford, Datalink Technologies Gateways Inc., Datalink 5, Datalink 6, John Doe, Datalink Technologies Gateways LLC and Lee Ingraham*, 13/06/2014, 2014 BCSC 1063 (CanLII). Disponível em: <<https://canlii.ca/t/g7fpw>>. Último acesso em: 17 abr. 2022).

Segundo a decisão da Suprema Corte do Canadá:

Quando é necessário garantir a eficácia da medida liminar, *um tribunal pode conceder uma medida liminar ordenando a conduta em qualquer parte do mundo*. O problema, neste caso, está ocorrendo on-line e globalmente. A Internet não tem fronteiras - seu habitat natural é global. A única maneira de garantir que a medida liminar interlocutória atingisse seu objetivo era que ela fosse aplicada onde o Google opera - globalmente. Se a medida cautelar fosse restrita apenas ao Canadá ou ao google.ca, o remédio seria privado de sua capacidade de evitar danos irreparáveis, uma vez que os compradores fora do Canadá poderiam facilmente continuar comprando nos sites da D, e os compradores canadenses poderiam encontrar os sites da D mesmo se os sites da D fossem desindexados do google.ca.¹⁹

Nesse sentido, a Corte entendeu que não seria razoável impedir os efeitos extraterritoriais necessários para a efetividade da medida cautelar e que o ônus de provar que, ao cumprir com essa decisão, a Google estaria violando leis de outras jurisdições - principalmente com relação à liberdade de expressão, como argumentava - é da própria intermediária (Google)²⁰.

Ressalta-se que, no caso relatado, a ordem global de desindexação beneficia não apenas a empresa que estava sofrendo danos irreparáveis e buscava a proteção de sua propriedade intelectual, mas também o comércio global na internet e o respectivo mercado consumidor. Inadvertidamente, a Google estava facilitando infrações de propriedade intelectual, por meio de seu mecanismo de busca. A desindexação dos resultados que levavam ao site da empresa infratora, ou seja, que promoviam o uso e a venda de produtos que infringiam direitos de propriedade intelectual, também evita que consumidores - usuários da internet - comprem produtos falsificados e beneficia a concorrência por reprimir práticas comerciais desonestas.

19. Grifos nossos. Tradução livre do original: "Where it is necessary to ensure the injunction's effectiveness, a court can grant an injunction enjoining conduct anywhere in the world. The problem in this case is occurring online and globally. The Internet has no borders - its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates - globally. If the injunction were restricted to Canada alone or to google.ca, the remedy would be deprived of its intended ability to prevent irreparable harm, since purchasers outside Canada could easily continue purchasing from D's websites, and Canadian purchasers could find D's websites even if those websites were de-indexed on google.ca." (*Google Inc. v. Equustek Solutions Inc.*, p. 4. CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc.*, 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824)

20. *Google Inc. v. Equustek Solutions Inc.*, parágrafo 46. CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc.*, 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824.

Ademais, outro motivo pelo qual ordens globais de retirada de conteúdo podem fornecer uma proteção adequada ao usuário da rede se deve à possibilidade de se responder a uma violação de direitos que ocorre online na mesma medida ou dimensão geográfica, especialmente quando se trate de um crime contra a honra²¹. Isto é, a resposta de um usuário vítima da divulgação de informações consideradas ilegais – em geral, o pedido de retirada de tal conteúdo do ar – é capaz de alcançar o mesmo escopo territorial que a mensagem que lhe agride. Dessa forma, evita-se, por exemplo, que o conteúdo ilícito compartilhado atinja o mundo inteiro, enquanto o bloqueio de tal comunicação ocorra apenas no país de residência da vítima. Ou, ainda, que ao ofensor baste compartilhar a mensagem ilícita uma vez, ao passo que a vítima precise requerer o bloqueio de acesso a tal informação em múltiplas cortes judiciais diferentes.

Evidencia-se, portanto, que a atribuição de efeitos globais a ordens de remoção de conteúdo online pode ter importância considerável para a proteção de direitos dos usuários. Seja (i) para garantir a extensão do direito material subjacente à ordem; (ii) para assegurar que decisões judiciais que protegem usuários sejam efetivas; ou (iii) para reduzir a desigualdade entre a disseminação da mensagem do ofensor e a defesa da vítima, é inegável que os efeitos mundiais de tais ordens podem favorecer usuários e contribuir para a higidez da rede.

3. Problemas decorrentes da atribuição de efeitos globais a ordens de remoção de conteúdo online

Uma vez explicitados os benefícios que podem ser alcançados quando concedidos efeitos globais a ordens que determinam a retirada de determinada informação da internet, passa-se a analisar as repercussões negativas que esses mesmos efeitos podem gerar.

Inicialmente, é evidente que o cumprimento, por uma empresa que atua em escala mundial, de uma ordem de remoção de conteúdo com efeitos globais, emitida por uma autoridade competente em determinado país ou região, implica a sujeição de todas as demais jurisdições em que a empresa em questão presta serviços à decisão de retirada. Nesse sentido, surgem preocupa-

21. Toma-se como base para a formulação desse argumento o caso *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*. UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, 03/10/2019, C-18/18. Disponível em: <<https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=329468>>. Último acesso em: 17 abr. 2022.

ções relacionadas ao respeito à soberania de outras nações²², tendo em vista a imposição, em diversos países, de uma decisão tomada por uma autoridade interna alheia, que está inserida em outro sistema jurídico e se baseia em suas leis locais, além de estar influenciada por tradições culturais próprias.

Como destacou uma sentença da *Camara Criminal y Correccional Federal* da Argentina:

A pretensão de extensão de uma medida liminar que disponha sobre o bloqueio de domínios ou serviços sujeitos à lei estrangeira implicaria não só na convalidação de uma violação do marco normativo vigente nos países em que a ordem foi emitida, mas também na aceitação implícita de conceder a um magistrado argentino o poder de decidir que conteúdos podem ser encontrados e lidos na internet por habitantes de todo o mundo²³.

Nessa mesma linha, aduz-se a impossibilidade de intervenção de um Estado no território de outro Estado soberano sem seu consentimento²⁴. Segundo esse ponto de vista, tal intervenção contraria princípios basilares do Direito Internacional Público, como a igualdade soberana entre países (VARELLA, 2019), a autonomia nacional, e o princípio da não-intervenção (SHAW, 2008). Ademais, desconsidera fontes do direito internacional previstas no art. 38 do Estatuto da Corte Internacional de Justiça²⁵, como convenções internacionais e o costume (CRAWFORD, 2012) ou a cortesia internacional²⁶.

22. Nesse sentido: DE CASTRO, Gabriel Martins Ramalho. Os mecanismos de camuflagem de IP e a efetividade das decisões judiciais nacionais: a invalidade de ordens globais de remoção de conteúdo na internet. *Artigos aceitos para publicação Direito digital e setor público*, 2020.2, p. 5. ITS - Instituto de Tecnologia e Sociedade, UERJ - Universidade Estadual do Rio de Janeiro e CEPED.

23. Tradução livre do original: “La pretensión de extender la ampliación de una medida cautelar que disponga el bloqueo de dominios o servicios sujetos a ley extranjera, implicaría no sólo convalidar un quebrantamiento del marco legal vigente en los países en los que esa orden fuera impartida, sino también una aceptación implícita de otorgar a un magistrado argentino la potestad de decidir los contenidos que pueden ser hallados y leídos en internet por los habitantes de todo el mundo” (ARGENTINA, *Camara Criminal y Correccional Federal*, 16/06/2020, Id SAJ: FA20030015, sumario. Disponível em: <<http://www.saj.gov.ar/camara-nac-apelaciones-civil-comercial-federal-federal-ciudad-autonoma-buenos-aires--medida-cautelar-fa20030015-2020-06-16/123456789-510-0300-2ots-eupmocsollaf?#>>. Último acesso em: 17 abr. 2022).

24. Esse argumento foi sustentado pela Google neste mesmo caso na Argentina (ARGENTINA, *Camara Criminal y Correccional Federal*, 16/06/2020, Id SAJ: FA20030015, p.1).

25. Estatuto da Corte Internacional de Justiça, p. 26. Disponível em: <https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf>. Último acesso em: 17 abr. 2022.

26. Segundo Spry, as limitações territoriais à jurisdição equitativa são, em certa medida, determinadas por referência a questões de eficácia e de cortesia (Spry, Ian C. F. *The Principles of Equitable Remedies: Specific Performance, Injunctions, Rectification and Equitable Damages*. 9th ed. Pyrmont, N.S.W.: Lawbook, 2014, p. 37. Apud *Google Inc. v. Equustek Solutions Inc.*, p. 4. CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc.*, Robert Angus and Clarma Enterprises Inc., 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824.

Além disso, adotando-se o imperativo categórico de Kant²⁷, resta evidente que a universalização de tais condutas tomadas por cortes locais geraria consequências nocivas (LA CHAPELLE, FEHLINGER, 2016; WITTICH, 2019), senão vejamos. Se a um magistrado argentino for permitido atribuir efeitos globais a decisões de remoção de conteúdo na internet, logicamente, e em obediência ao princípio da reciprocidade, autoridades competentes de todo o mundo também disporiam de semelhante poder. Com a extensão dessa possibilidade para todos os países e regiões, a probabilidade de obter-se ordens conflitantes para o mesmo conteúdo, em diferentes jurisdições pelo mundo, é muito elevada. Trata-se, portanto, não apenas de um conflito de leis, mas de um conflito entre ordens vinculantes, sejam elas judiciais ou administrativas – como as provenientes de autoridades nacionais de proteção de dados, por exemplo.

No caso *Google LLC v. Equustek Solutions Inc.*²⁸, a Google alegava, perante as cortes canadenses, que o cumprimento da ordem global de desindexação dos sites da Datalink a obrigaria a violar leis dos Estados Unidos da América. Assim, requereu e lhe foi concedida, perante o Tribunal Distrital do Norte da Califórnia, medida provisória que impedia a execução da decisão canadense²⁹. Ao que tudo indica, esse cenário de obrigações contraditórias tende a se repetir progressivamente, impondo ônus cada vez mais gravoso às empresas globais (LUTZI, 2017).

Tendo em vista a sobreposição de ordens conflitantes, essas plataformas são obrigadas a tomar decisões complexas e selecionar que obrigação legal ou judicial cumprir, automaticamente descumprindo outra, diametralmente oposta³⁰. Em última instância, esse contexto poderia levar a disputas entre

27. Segundo Bertrand de La Chapelle e Paul Fehlinger, o imperativo categórico kantiano deve sustentar a regulamentação internacional da Internet (LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. *Global Commission on Internet Governance Paper Series*, n. 28, Abr. 2016, p. 5). Também nesse sentido: WITTICH, Stephan. Immanuel Kant and Jurisdiction in International Law. In: Stephen Allen et al. (Ed.). *The Oxford Handbook of Jurisdiction in International Law*. Oxford: Oxford University Press, 2019. Chapter 5, pp. 82-94.

28. *Google Inc. v. Equustek Solutions Inc.*, p. 4. CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc.*, 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824.

29. ESTADOS UNIDOS DA AMÉRICA, Tribunal Distrital do Norte da Califórnia, *Google Inc v. Equustek Solutions Inc.* (Equustek I), 02/11/2017, Case No. 5:17-cv-04207-EJD, SCC 34. Disponível em: < <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2589&context=historical>>. Acesso em: 17 abr. 2022.

30. Apesar de não tratar de remoção de conteúdo online, no caso paradigma *Microsoft Warrant*, a Microsoft se viu vinculada a uma decisão judicial dos EUA que lhe obrigava a entregar determinada informação e, ao mesmo tempo, à lei irlandesa, local de armazenamento do dado em questão, que proibia tal entrega (*United States v. Microsoft Corp.* ESTADOS UNIDOS DA AMÉRICA, Suprema Corte dos Estados Unidos da América, 16/04/2018, 584 U.S. ___ (2018)).

países³¹ – que buscam garantir o cumprimento de suas ordens vinculantes ou proteger empresa nacional – e ao que alguns autores chamam de “corrida armamentista legal” (SVANTESSON, 2019)³².

Ressalva-se, no entanto, que, apesar de constituir tema extremamente rico, o aprofundamento de tais questões foge ao escopo do presente artigo, que tem como ponto central a perspectiva do usuário da rede. Dessa forma, outras implicações afetam mais diretamente a este particular.

Entre elas, a restrição do acesso à informação em escala global. É certo que a remoção, com efeitos globais, de determinado resultado em mecanismos de busca ou de uma mensagem em redes sociais impede qualquer cidadão, no mundo todo, de acessar a respectiva informação. Talvez, nos casos em que essa remoção interrompe flagrante infração de direitos fundamentais, a restrição não seja sentida tão fortemente. Entretanto, ressalta-se que cada jurisdição enxerga o equilíbrio entre direitos e a ponderação de princípios de forma distinta, de acordo com suas tradições, regulamentações e jurisprudência³³. Desse modo, corre-se o risco de uma autoridade local isolada decidir pelo bloqueio de acesso a determinada informação em escala mundial, ainda que grande parte das nações impactadas por essa ordem discordem da interpretação empregada³⁴. Pouco a pouco, a internet se veria restringida por todos os lados³⁵.

Soma-se a isso a possibilidade de informações relevantes para usuários de determinado país serem retiradas da internet em razão de ordem global

31. Na falta de uma solução clara para esse conflito de obrigações, recai sobre essas empresas a definição de que obrigação judicial ou legal privilegiar e, conseqüentemente, que Estados prestigiar, de acordo com seus interesses comerciais. Nesse cenário, em que é impossível conferir efetividade às ordens e às normas de todos os países, alguns Estados têm maior poder de coerção sobre as plataformas do que outros, o que pode levar a sanções do ponto de vista internacional e a sérias disputas entre nações.

32. Uma referência à adoção unilateral de políticas públicas e privadas por diversos agentes no contexto da busca por uma solução rápida para o enfrentamento dos desafios regulatórios da internet, de forma descoordenada. SVANTESSON, Dan Jerker B. *Internet & Jurisdiction Global Status Report 2019*, Internet & Jurisdiction Policy Network, p. 17.

33. Nesse sentido: LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de Internet*. São Paulo: Editora Juarez de Oliveira, 2005, p. 220.

34. Conforme destacado no parágrafo 60 do julgamento do caso *Google v. CNIL*: “o equilíbrio entre o direito ao respeito pela vida privada e à proteção dos dados pessoais, por um lado, e a liberdade de informação dos internautas, por outro, pode variar de forma considerável no mundo” (tradução livre. *Google v. CNIL*, parágrafo 60. UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Google LLC v. Commission nationale de l’informatique et des libertés (CNIL)*, 24/09/2019, C-507/17).

35. Em contrapartida, não podemos perder de vista o fato de que a moderação de conteúdo exercida pelas próprias plataformas globais produz efeitos semelhantes.

proferida por outra jurisdição. Explica-se através de um exemplo hipotético. Considerando que o interesse público acerca da informação X é pouco expressivo no país A, este terá pouco interesse em proteger o direito de acesso a X, tendendo a privilegiar o direito material do outro lado da balança. Com isso, usuários do país B, onde X tem grande repercussão social, seriam prejudicados por eventual remoção do conteúdo, que já não estaria mais disponível em nenhum lugar do mundo.

Mas a consequência negativa dos efeitos globais das ordens de remoção que provavelmente mais afeta os usuários é a limitação à liberdade de expressão na internet. Como pontuado por Andrew Keane Woods: “a França não deveria ter a capacidade de limitar a liberdade de expressão dos nova-iorquinos” (WOODS, 2017). É dizer, cada jurisdição tende a priorizar direitos fundamentais de maneira distinta. Sob o ponto de vista dos cidadãos dos Estados Unidos, a liberdade de expressão, positivada na primeira emenda³⁶ à Constituição dos EUA, deve ser o mais ampla possível, restringindo-se ao máximo qualquer direito que a contraponha. Na França, por outro lado, outros direitos individuais – a exemplo daqueles relativos à proteção de dados pessoais, como o direito ao esquecimento – recebem alto grau de proteção e, naturalmente, podem ser privilegiados em detrimento da liberdade de expressão, que admite mais limitações na tradição francesa³⁷⁻³⁸.

Dessa forma, decisões que determinam a remoção de conteúdo na internet com efeitos globais acabam por chocar e impactar muito fortemente, em especial, países que preservam a liberdade de expressão em níveis tão elevados que a aproximam de um direito absoluto. Assim, uma ordem de remoção que jamais seria concedida nesses países acaba sendo executada em escala global na internet, incluindo seus territórios nacionais, sem que lhes seja dada oportunidade de analisar o caso em questão. Alega-se, nesse prisma, que caminhar-se-ia para uma realidade em que a proteção à liberdade de expressão na internet seria delimitada por um mínimo denominador comum.

36. Amendment I: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”.

37. Ver GREENBERG, Marc. A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market. *Berkeley Technology Law Journal*, vol. 18, n. 4, out. 2003, p. 1222. Disponível em: <<https://www.jstor.org/stable/24116933>>. Último acesso em: 17 abr. 2022.

38. Nota-se, ainda, que não são incomuns diferenças na própria aceção do direito à liberdade de expressão. Enquanto algumas jurisdições entendem que a livre manifestação do pensamento deve permitir declarações que beiram o discurso de ódio, outras entendem que o bloqueio de acesso a conteúdo desinformativo, por exemplo, contribui para o fortalecimento da liberdade de expressão.

Nesse contexto, é interessante analisar a interpretação empregada pelo Tribunal Distrital do Norte da Califórnia (EUA), em contraposição à perspectiva da Suprema Corte do Canadá, ao analisarem o mesmo caso. Enquanto o tribunal norte-americano entendeu que a ordem de remoção global expedida no Canadá “ameaça a liberdade de expressão na internet global”³⁹ – entre outras críticas manifestadas –, a Corte canadense destacou que “até o momento, não aceitamos que a liberdade de expressão exija a facilitação da venda ilegal de mercadorias”⁴⁰.

Percebe-se, então, que a atribuição de efeitos globais a ordens de retirada de conteúdo na internet pode provocar consequências perversas relevantes, como (i) a intervenção indevida no território de outro Estado soberano – o que pode ser visto como uma violação de princípios do Direito Internacional Público; (ii) a provável eclosão de conflitos entre ordens vinculantes contraditórias, judiciais ou administrativas; (iii) a restrição do acesso à informação na internet; ou (iv) a possível limitação à liberdade de expressão em escala global.

Considerações finais

Diante de todo o exposto, constata-se que seria impossível adotar-se uma visão maniqueísta sobre as ordens globais de remoção de conteúdo online. Elas são aliadas e adversárias dos usuários ao mesmo tempo. Se, por um lado, os efeitos globais permitem proteger direitos materiais dos usuários em toda sua extensão, conferir efetividade a decisões protetivas dos usuários e reduzir a disparidade de armas entre ofensor e vítima; por outro, podem causar problemas relacionados ao desrespeito à soberania de outras nações, a conflitos derivados de obrigações contraditórias, à limitação do acesso à informação e à restrição à liberdade de expressão na internet. Ademais, a ampla diversidade de circunstâncias envolvendo cada caso em que se cogita a atribuição de efeitos globais a essas decisões intensifica o desafio da busca por soluções.

Assim sendo, para que seja possível desfrutar dos benefícios da extensão dos efeitos dessas ordens de remoção na internet, faz-se necessário evitar

39. Tradução livre. ESTADOS UNIDOS DA AMÉRICA, Tribunal Distrital do Norte da Califórnia, *Google Inc v. Equustek Solutions Inc.* (Equustek I), 02/11/2017, Case No. 5:17-cv-04207-EJD, SCC 34, p. 06.

40. Tradução livre. CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc.*, Robert Angus and Clarma Enterprises Inc., 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824, parágrafo 48.

a concretização dos riscos mencionados, marcados por notável potencial de gerar danos graves⁴¹. Para isso, é necessário que posições consistentes sejam adotadas no plano internacional, o que deve ser buscado por meio do debate entre diferentes setores da sociedade em todo o mundo, em direção à devida regulamentação – como tratados que promovam novas formas de cooperação jurídica internacional⁴². De acordo com Bertrand de La Chapelle e Paul Fehlinger: “precisamos de mecanismos de cooperação inovadores que sejam tão transnacionais quanto a própria Internet”.

Referências

ARGENTINA, *Camara Criminal y Correccional Federal*, 16/06/2020, Id SAJJ: FA20030015, sumario. Disponível em: <<http://www.saij.gob.ar/camara-nac-apelaciones-civil-comercial-federal-federal-ciudad-autonoma-buenos-aires--medida-cautelar-fa20030015-2020-06-16/123456789-510-0300-2ots-eupmocsollaf?#>>.

Último acesso em: 17 abr. 2022.

CANADÁ, Suprema Corte de British Columbia, *Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc. v. Morgan Jack, Andrew Crawford, Datalink Technologies Gateways Inc., Datalink 5, Datalink 6, John Doe, Datalink Technologies Gateways LLC and Lee Ingraham*, 13/06/2014, 2014 BCSC 1063 (CanLII). Disponível em: <<https://canlii.ca/t/g7fpw>>. Último acesso em: 17 abr. 2022.

CANADÁ, Suprema Corte do Canadá, *Google LLC v. Equustek Solutions Inc., Robert Angus and Clarma Enterprises Inc.*, 28/06/2017, 2017 SCC 34 (CanLII), [2017] 1 SCR 824. Disponível em: <<https://canlii.ca/t/h4jg2>>. Último acesso em: 17 abr. 2022.

CAVALIERE, Paolo. *Glawischnig-Piesczek v. Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations*. *European Data Protection Law Review*, v. 5, n. 4, 2019, pp. 573 – 578. Disponível em: <<https://ssrn.com/abstract=3519389>>. Último acesso em: 17 abr. 2022.

41. A fim de solucionar a dificuldade de delimitação das situações em que efeitos extraterritoriais são bem-vindos, o Prof. Christian Perrone (ITS) propôs um elemento de praticidade, denominado “Teste da Jurisdição 3D”, que pretende conferir interoperabilidade às ordens judiciais (PERRONE, Christian. “*Efeito global da jurisdição: ‘Direito ao esquecimento’, propriedade intelectual e ‘Fake News’*”. Aula 04 de Direito Internacional e Jurisdição na Internet. Pós-Graduação Direito Digital UERJ-ITS. 11 nov. 2021).

42. Tradução livre. Trecho original completo: “like climate change or financial regulation, jurisdiction on the Internet is a global challenge that will only become more complicated if left unattended. States, companies, and civil society need to step up efforts to avoid the negative consequences of the current legal arms race, preserve the global nature of the Internet and address its misuse. We need innovative cooperation mechanisms that are as transnational as the Internet itself” (DE LA CHAPELLE, Bertrand; FEHLINGER, Paul. A legal arms race threatens the future of the internet. *Council on Foreign Relations*, 9 maio 2016, p. 2. Disponível em: <<https://www.cfr.org/blog/legal-arms-race-threatens-future-internet>>. Último acesso em: 17 abr. 2022).

CHANDER, Anupam. *The Electronic Silk Road: How the Web Binds the World in Commerce*. New Haven, Conn.: Yale University Press 2013). Disponível em: <<https://scholarship.law.georgetown.edu/facpub/2297/>>. Último acesso em: 17 abr. 2022.

COMITÊ DE SUPERVISÃO. Decisão sobre o caso 2021-001-FB-FBR (FB-691QAMHJ). 5 maio 2021. Disponível em: <<https://oversightboard.com/decision/FB-691QAMHJ/>>. Último acesso em: 17 abr. 2022.

CRAWFORD, James R. *Brownlie's Principles of Public International Law*. 8ª ed., Oxford: Oxford University Press, 2012.

DE CASTRO, Gabriel Martins Ramalho. Os mecanismos de camuflagem de IP e a efetividade das decisões judiciais nacionais: a invalidade de ordens globais de remoção de conteúdo na internet. *Artigos aceitos para publicação Direito digital e setor público*, 2020.2, p. 5. ITS - Instituto de Tecnologia e Sociedade, UERJ - Universidade Estadual do Rio de Janeiro e CEPED.

DE LA CHAPELLE, Bertrand; FEHLINGER, Paul. A legal arms race threatens the future of the internet. *Council on Foreign Relations*, 9 maio 2016, p. 2. Disponível em: <<https://www.cfr.org/blog/legal-arms-race-threatens-future-internet>>. Último acesso em: 17 abr. 2022.

ESTADOS UNIDOS DA AMÉRICA, Suprema Corte dos Estados Unidos da América, *United States v. Microsoft Corporation*, 16/04/2018, 584 U.S. ___ (2018).

ESTADOS UNIDOS DA AMÉRICA, Tribunal Distrital do Norte da Califórnia, *Google Inc v. Equustek Solutions Inc. (Equustek I)*, 02/11/2017, Case No. 5:17-cv-04207-EJD, SCC 34. Disponível em: <<https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2589&context=historical>>. Último acesso em: 17 abr. 2022.

ESTADOS UNIDOS DA AMÉRICA. The U.S. Bill of Rights (1791) "Amendment I: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". Disponível em: <<https://www.archives.gov/founding-docs/bill-of-rights-transcript>>. Último acesso em: 17 abr. 2022.

GEIST, Michael A. Is There a There There? Toward Greater Certainty for Internet Jurisdiction, *Berkeley Technology Law Journal*, vol. 16, n. 3, out. 2001, pp. 1356-1357 (2001). Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=266932>. Último acesso em: 17 abr. 2022.

GREENBERG, Marc. A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market. *Berkeley Technology Law Journal*, vol. 18, n. 4, out. 2003, p. 1222. Disponível em: <<https://www.jstor.org/stable/24116933>>. Último acesso em: 17 abr. 2022.

Internet and Jurisdiction Policy Network. *I&J Retrospect Database*. Disponível em: <<https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6IjIwMjEtM-TlIfQ==>>>. Último acesso em: 17 abr. 2022.

KLONICK, Kate. The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *Yale Law Journal*, Vol. 129, No. 2418, 2020. Disponível em: <<https://ssrn.com/abstract=3639234>>. Último acesso em: 17 abr. 2022.

LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. *Global Commission on Internet Governance Paper Series*, n. 28, Abr. 2016.

LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de Internet*. São Paulo: Editora Juarez de Oliveira, 2005, p. 220.

LUTZI, Tobias. Internet Cases in EU Private International Law – Developing a Coherent Approach. *International and Comparative Law Quarterly*, vol. 66, jul. 2017.

NAÇÕES UNIDAS. Estatuto da Corte Internacional de Justiça, Nova York, 1957, p. 26. Disponível em: <https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf >. Último acesso em: 17 abr. 2022.

OKONIEWSKI, Elissa A. Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet. *American University International Law Review*, v. 18, n. 1, 2002, pp. 295-339. Disponível em: <<https://digitalcommons.wcl.american.edu/auilr/vol18/iss1/6/>>. Último acesso em: 17 abr. 2022.

PERRONE, Christian. *Efeito global da jurisdição: ‘Direito ao esquecimento’, propriedade intelectual e ‘Fake News’*. Aula 04 de Direito Internacional e Jurisdição na Internet. Pós-Graduação Direito Digital UERJ-ITS. 11 nov. 2021.

SAMONTE, Mary. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law. *European Law Blog*, 29 out 2019. Disponível em: <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/#_ftn14>. Último acesso em: 17 abr. 2022.

SLANE, Andrea. Tales, Techs and Territories: Private International Law, Globalization, and the Legal Construction of Borderlessness on the Internet. *Law and Contemporary Problems*, v. 71, jul. 2008, pp. 129-152. Disponível em: <https://scholarship.law.duke.edu/lcp/vol71/iss3/6>>. Último acesso em: 17 abr. 2022.

SVANTESSON, Dan Jerker B. *Internet & Jurisdiction Global Status Report 2019*, Internet & Jurisdiction Policy Network.

SVANTESSON, Dan Jerker B. *Private International Law and the Internet*. 3. ed. Alphen aan den Rijn: Kluwer Law International B. V, 2016.

UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, 03/10/2019, C-18/18. Disponível em: <<https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=329468>>. Último acesso em: 17 abr. 2022.

UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, 24/09/2019, C-507/17. Disponível em: <<https://curia.europa.eu/juris/document/document.jsf?docid=218105&doclang=EN>>. Último acesso em: 17 abr. 2022.

UNIÃO EUROPEIA, Tribunal de Justiça da União Europeia, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*, 13/05/2014, C-131/12. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>>. Último acesso em: 17 abr. 2022.

UNIÃO EUROPEIA. Diretiva de proteção de Dados Pessoais na União Europeia, Diretiva 95/46/EC de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>>. Último acesso em: 17 abr. 2022.

United Nations Economic Commission for Latin America and the Caribbean (ECLAC); SOUZA, Carlos Affonso. *Informe Sobre la Situación Regional 2020*. Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y El Caribe (Cepal), nov. 2020. Disponível: <<https://www.internetjurisdiction.net/uploads/pdfs/Informe-sobre-la-situacio%CC%81n-regional-2020.pdf>>. Último acesso em: 17 abr. 2022.

VARELLA, Marcelo D. *Direito internacional público*. 8ª Ed. São Paulo: Saraiva Educação, 2019.

WITTICH, Stephan. Immanuel Kant and Jurisdiction in International Law. In: Stephen Allen et al. (Ed.). *The Oxford Handbook of Jurisdiction in International Law*. Oxford: Oxford University Press, 2019. Chapter 5, pp. 82 -94.

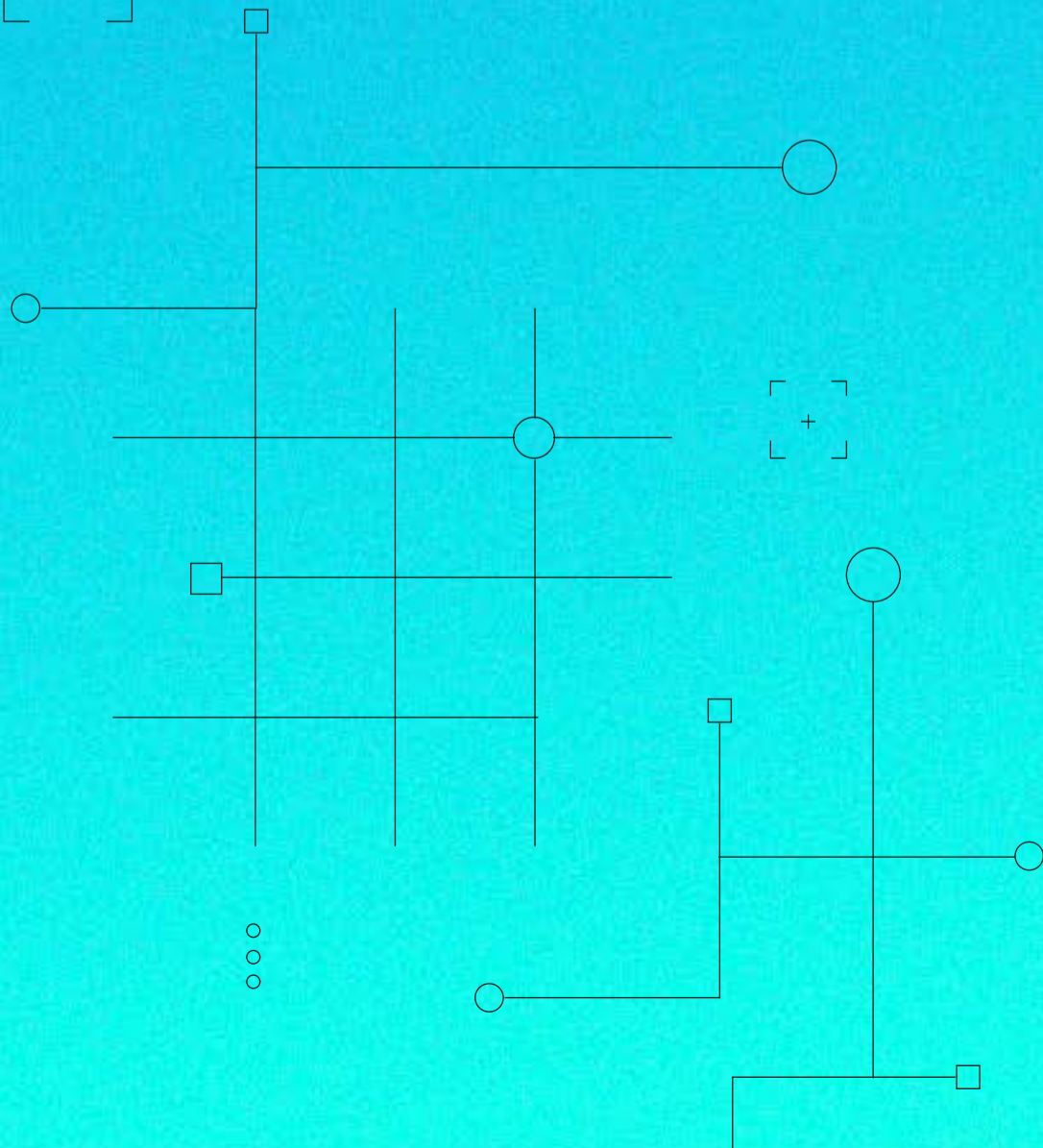
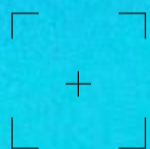
WOODS, Andrew Keane. *No, The Canadian Supreme Court Did Not Ruin the Internet*. Lawfare, 06 jul. 2017. Disponível em: <<https://www.lawfareblog.com/no-canadian-supreme-court-did-not-ruin-internet>>. Último acesso em: 17 abr. 2022.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DÍGITAL

11

A importância da regulação da moderação de conteúdo em mídias digitais no combate à desinformação

SABRINA WERVLOET



Sumário: Introdução; 1. Desinformação: aspectos relevantes; 2. Moderação de conteúdo; 3. A importância da regulação da moderação de conteúdo no contexto da desinformação; Considerações finais; Referências.

Introdução

Por ser inerente à comunicação humana, o fenômeno da desinformação não é recente e exclusivo do século XXI, apesar de a tecnologia atual ser o meio ideal para sua ampla disseminação e ampliação dos riscos e consequências para a sociedade (POSETTI; MATTHEWS, 2018, p. 1). Durante séculos, os processos políticos foram marcados pela criação de boatos e mentiras, seja pelos próprios políticos que disputavam a eleição, seja pela classe que os apoiava (BOTELHO, 2021, p. 650).² Assim, a construção de narrativas específicas para influenciar a opinião pública sempre foi recorrente. O que mudou é a frequência do seu uso e o seu alcance.

Com o advento da Internet e a mudança para um ambiente cada vez mais digital, a sociedade se vê diante de novas formas de se expressar, acessar informações e debater. As mídias digitais são amplamente utilizadas como ferramenta de informação, de acessar notícias e compartilhar conteúdo. Entretanto, por não existir checagem prévia do conteúdo postado, cabe ao usuário utilizar seu senso crítico e checar a informação recebida (TEFFÉ; SOUZA, 2019, p. 527). Ao mesmo tempo que proporciona tais vantagens, o meio digital permite um aumento no volume de desinformação, representando uma série de potenciais riscos e danos aos processos políticos democráticos e à sociedade em geral.

Por ser responsável, em grande parte, pela maneira como a opinião pública é formada e transmitida, as plataformas digitais assumem papel preponderante na atualidade, tornando-se o centro da discussão acerca do enfrentamento à desinformação.

1. Graduada em Direito pela Universidade Federal do Espírito Santo (UFES). Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS) em parceria com a Universidade Estadual do Rio de Janeiro (UERJ). E-mail: sabrinawervloet@hotmail.com.

2. Inúmeras informações historicamente narradas são questionáveis em razão de fatores incompatíveis com a realidade, não sendo incomum o entrelaçamento com o misticismo. Botelho et al. cita, por exemplo, o historiador bizantino Procópio de Cesareia, cujas narrações são repletas de exageros e inverdades sobre Justiniano e Teodora. O autor lembra, ainda, das notícias falsas ou incompletas dos pasquins, nos séculos XVII a XIX, em algumas localidades da Europa. (BOTELHO, Marcos César, et al. Eleições, Populismo e Desinformação: o papel das redes sociais frente a estigmatização da imprensa. In: 7 Journal of Institutional Studies, Revista Estudos Institucionais, v.7, n. 2, p. 649-680, mai/ago 2021, p. 650)

O presente trabalho tem por objetivo analisar o fenômeno da desinformação e estabelecer como a regulação sobre moderação de conteúdo pode auxiliar no combate a tal fenômeno. Para tanto, é realizada uma pesquisa exploratória, em revisão bibliográfica, delimitando os seus principais aspectos e mapeando os danos que podem advir da sua disseminação.

Mais especificamente, tem como objetivo principal questionar a importância da criação de uma legislação sobre moderação de conteúdo em mídias digitais como ponto de partida no combate à desinformação.

Busca-se evidenciar que em razão dos danos causados pela desinformação, se mostra imprescindível a regulação sobre moderação de conteúdo, com o intuito de contrabalançar a autorregulação, feita exclusivamente, atualmente, pelos provedores.

1. Desinformação: aspectos relevantes

Conforme Anna Brisola e Arthur Bezerra (2019, p. 4), para compreender a amplitude e importância do fenômeno da circulação de informações falsas e da desinformação na atualidade, é preciso, anteriormente, delimitar o ambiente informativo no qual esse fenômeno se proliferou.

Em decorrência da globalização e dos avanços tecnológicos nas áreas da comunicação e da informação, a vida social, econômica e política da população foi alterada significativamente, uma vez que possibilitou o rápido acesso às informações e o seu compartilhamento. Conforme Joana Machado (2018, p. 9), são características intrínsecas à sociedade da informação³ o uso da internet e a velocidade das comunicações.

Seria intuitivo imaginar, no início do século XXI, que o advento da internet promoveria uma maior participação dos cidadãos na democracia, já que ela facilita o acesso a informações e debates. Entretanto, segundo Manuel Castells (2003, p. 161-162), seu uso está aprofundando a crise generalizada de legitimidade política. O autor aponta que o acesso ao governo se dá, basicamente, pela política da mídia, a qual leva à prevalência da “política do escândalo”, cujo

3. “Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais. Há uma nova compreensão (mais abreviada) da relação entre tempo-espço, o que outrora acarretava maior cadência às interações sociais.” (BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Editora Forense. Rio de Janeiro, 2019, p. 36)

funcionamento se baseia em vazamentos de informação com o intuito de desonrar um oponente ou restaurar a imagem de determinado político.

Nesse contexto, as plataformas digitais fornecem um ambiente muito mais propício para a divulgação desse tipo de informação do que a mídia tradicional, pois além de haver um ambiente de anonimato e baixa regulação dos conteúdos, as informações que cada usuário recebe são determinadas e direcionadas através de algoritmos conforme o histórico de busca e reação de cada um. Assim, há uma propensão de que cada pessoa receba informações de acordo com suas ideologias e crenças. São as chamadas “bolhas de filtro” ou “câmaras de eco” (ALLCOTT; GENTZKOW, 2017, p. 211).

Nas palavras de Pascual Serrano (2010, p. 31), “os mecanismos de desinformação e manipulação são mais complexos que a mentira grosseira”. A desinformação não envolve, necessariamente, uma notícia completamente falsa, pois seria de fácil percepção pelos usuários. Ela é mais sutil; geralmente é uma “informação descontextualizada, fragmentada, manipulada, retirada de sua historicidade, tendenciosa, que apaga a realidade, distorce, subtrai, rotula ou confunde” (BRISOLA; BEZERRA, 2018, p. 4).

A sociedade de redes proporciona que cada usuário seja não apenas um receptor de conteúdo, mas também um reproduzidor que participa ativamente a cada compartilhamento, mesmo que em muitos casos não haja a intenção de causar danos, mas pela própria ignorância ou pela vontade de ter sua opinião validada (BERNARDI, 2019, p. 21).

O termo *fake news* vem sendo muito utilizado na contemporaneidade, principalmente após o período eleitoral de Donald Trump em 2016, para designar as notícias fabricadas com a intenção de causar danos (ALLCOTT; GENTZKOW, 2017, p. 211). Contudo, segundo a UNESCO, o termo *fake news* deve ser evitado, pois a palavra notícia significa informações verificáveis de interesse público, e qualquer informação que não atender a esse padrão não pode merecer o rótulo de notícia. “Nesse sentido, então, a expressão “notícias falsas” é um oxímoro que se presta a danificar a credibilidade da informação que de fato atende ao limiar de verificabilidade e interesse público” (UNESCO, 2019, p. 7).

Por estes motivos, o presente trabalho adotará o termo desinformação para se referir às informações veiculadas deliberadamente para confundir ou manipular a população por meio de transmissão de informações desonestas, com o fim de obter, em regra, algum benefício econômico e/ou político. (TEFFÉ; SOUZA, 2019, p. 526)

Um dos aspectos que diferencia o tratamento dado às *fake news* hoje e no passado é que no passado havia uma série de obstáculos quanto ao potencial lesivo dessas notícias, quais sejam: 1. Alto custo para abranger um número expressivo de pessoas; 2. Falta de flexibilidade para alterar o conteúdo, tendo em vista que era impresso; 3. Falta de conhecimento sobre o leitor, dificultando a formação de um perfil ideal a ser atingido por aquelas notícias; 4. Falta de contexto ideal para certificar a credibilidade do meio de distribuição da informação (ITAGIBA, 2017).

A popularização da internet facilitou sobremaneira o acesso e a difusão das novas tecnologias, facilitando a divulgação de informações em volume, diversidade e complexidade nunca imaginados anteriormente (PINHO FILHO, 2021, p. 16). Por consequência, os obstáculos mencionados acima no que se refere ao potencial lesivo de notícias falsas passam a ser naturalmente superados.⁴

Em 2018, um grupo de especialistas reunido pela União Europeia elaborou um relatório, chamado de *A Multi-dimensional Approach to Disinformation - Report of the independent High Level Group on fake news and online disinformation*, com o intuito de determinar iniciativas no combate à desinformação. Tal relatório adotou como desinformação todas as formas de informação falsa, imprecisa ou enganosa, elaborada e promovida para, intencionalmente, causar dano público ou com fins lucrativos. Concluiu-se que dentre os riscos de dano estão as ameaças ao sistema democrático de processos políticos e aos valores democráticos que moldam políticas públicas em setores como ciência, saúde e educação, por exemplo.

Conforme José Célio Filho (2021, p. 17), “independentemente de sua origem, se decorre de erro honesto, negligência na verificação das fontes, viés inconsciente ou de ação intencional (desinformação), informações enganosas têm o potencial de confundir e prejudicar indivíduos”. Entretanto, consoante o relatório supramencionado, a produção intencional de desinformação, com o objetivo deliberado de causar dano, é relativamente mais grave e deve ser encarada com teor mais crítico, pois os danos são extensivamente maiores.

4. Allcott e Gentzkow apontam diversas razões pelas quais as plataformas digitais podem ser propícias para a disseminação de notícias falsas. A primeira é que os custos para a produção de conteúdo são relativamente baixos. A segunda é que o formato das redes sociais dificulta o julgamento de veracidade de uma determinada informação. A terceira é que as pessoas são mais propensas a ler e compartilhar informações que estão alinhadas com sua posição ideológica, e isso é proporcionado pelas bolhas de filtro ou câmaras de eco. (ALLCOTT, Hunt; GENTZKOW, Matthew. *Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, Cambridge*, v. 31, n. 2, p. 211-236, 2017, p. 221. Disponível em: <<https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211>>. Acesso em: 09 jan. 2022.)

Por normalmente ser direcionada a um determinado grupo de indivíduos, a desinformação tende a afetar esses grupos de forma direta, mas temos que considerar os danos, ainda que indiretos, à sociedade em geral. Exemplo disso é o que vem ocorrendo durante o período pandêmico que vivemos na atualidade.

Durante a pandemia da Covid-19 ficou evidenciado o quão desastrosas podem ser as consequências da desinformação para a sociedade, tendo em vista a disseminação de teorias da conspiração e a politização de questões de saúde pública, tudo isso amplificado pelo amplo alcance que as mídias sociais proporcionam. No início da pandemia, houve diversas teorias alegando que o vírus teria sido criado em um laboratório pela China⁵, com objetivo de ser usado como arma biológica, e até mesmo negando a existência da pandemia⁶.

Tornaram-se comuns, ainda, os discursos acerca de tratamentos que não possuíam qualquer respaldo médico, colocando em risco a vida de milhares de pessoas, como o tratamento precoce utilizando o chamado ‘kit covid’, com o uso dos medicamentos hidroxicloroquina e ivermectina.⁷

A eficácia da vacina contra o vírus também foi alvo de inúmeros ataques, inclusive pelo presidente da República, Jair Bolsonaro, o qual se pronunciou, diversas vezes, no sentido de que seria ineficaz, sendo preferível o uso do ‘kit covid’.⁸

Moisés de Lemos Martins (2019, p. 20) aduz estarmos vivendo uma crise da cultura e do humano, resultante do descolamento da ética, da verdade, dos fatos.

(...) as tecnologias da informação e da comunicação não deixam de exprimir a crise da experiência contemporânea, a de um cotidiano acentrado, sem fundamento, que vive das emoções, e não sobretudo das ideias, num tempo de velocidade, acelerado, de mobilização «total» (Jünger), ou «infinita» (Sloterdijk, 2000).

5. CUETO, José Carlos. Origem do coronavírus: o que se sabe sobre o laboratório de Wuhan investigado pelos EUA. BBC. Disponível em: <<https://www.bbc.com/portuguese/internacional-57339240>>. Acesso em: 07 jan. 2022.

6. BERGAMO, Mônica. Google remove vídeos negando pandemia após intervenção do Ministério Público. Folha de São Paulo. Disponível em: <<https://www1.folha.uol.com.br/colunas/monicabergamo/2020/05/google-remove-videos-negando-pandemia-apos-intervencao-do-ministerio-publico.shtml>>. Acesso em: 07 jan. 2022.

7. Kit covid: o que diz a ciência? Saúde com Ciência. Centro de Comunicação Social da Faculdade de Medicina da UFMG. Disponível em: <<https://www.medicina.ufmg.br/kit-covid-o-que-diz-a-ciencia/>>. Acesso em: 07 jan. 2022.

8. SANTOS, José Matheus. CRISPIM, Roberto. Bolsonaro desdenha de vacina e enaltece ‘kit covid’ um dia após CPI lhe atribuir 9 crimes na pandemia. Folha de São Paulo. Disponível em: <<https://www1.folha.uol.com.br/poder/2021/10/bolsonaro-desdenha-de-vacina-e-enaltece-kit-covid-um-dia-apos-cpi-apontar-9-crimes-dele-na-pandemia.shtml>>. Acesso em: 07 jan. 2022.

Referido autor afirma que a crise da cultura está associada a dois fatores principais, “ao afundamento dos universais (designadamente ao afundamento das ideias de bom, belo e justo), e por outro lado, ao facto de a sociedade actual se ter convertido numa sociedade da comunicação generalizada [...], pela implantação global das redes de comunicação eletrónica” (MARTINS, 2019, p. 89-90).

Submersos em milhares de informações e distantes da racionalidade e das ideias, os indivíduos são atraídos pelo pensamento hegemônico, sendo levados a pensar de forma uniforme e sem preocupação em discernir a verdade da não verdade (BRISOLA; BEZERRA, 2018, p. 6).

Alguns autores nomeiam esse período disruptivo que estamos vivendo de “pós-verdade”, no qual as crenças pessoais e as emoções substituem os fatos e as evidências (AMARAL; SANTOS, 2019, p. 67). O termo é utilizado para referenciar um ambiente social de exaustão diante da infinidade de informações potencialmente distorcíveis, disponíveis para atender à narrativa e ao interesse que for conveniente (BOTELHO; ET AL, 2021, p. 653).

Diante desse cenário, torna-se imperativo que a sociedade busque formas de combater o fenômeno da desinformação e debata sobre a responsabilidade dos provedores por esses conteúdos, tendo em vista a gravidade de suas consequências para o regime democrático, as instituições de direito e as políticas públicas, como saúde e educação.

Moderação de conteúdo

A moderação de conteúdo em mídias digitais se torna cada vez mais relevante nos debates sobre regulação da Internet e governança não apenas no Brasil, mas no mundo. Isso se dá em razão da dimensão e ampliação dos impactos que os discursos online trazem para a sociedade, especialmente no que concerne a questões ideológicas e políticas, vide as eleições de Donald Trump, nos EUA, e de Jair Bolsonaro, no Brasil.

Hoje, a grande maioria da população mundial acessa diariamente plataformas digitais, seja por lazer ou por trabalho, fornecendo a essas plataformas uma infinidade de dados pessoais. Assim, a moderação de conteúdo nessas plataformas terá como pressuposto o tratamento de grandes quantidades de dados pessoais, sendo muitos deles sensíveis⁹. Por este motivo, deve haver

9. De acordo com o art. 5º, inciso II, da LGPD, é considerado dado sensível todo “dado pessoal sobre origem racial ou étnica,

uma análise cuidadosa quanto a obrigações de transparência, a fim de evitar o uso e a divulgação indevida desses dados (ARCHEGAS, 2021, p. 2).

Apesar de serem criadas e operadas por empresas privadas, as plataformas digitais, conforme exposto no tópico anterior, atuam diretamente na formação da opinião pública, influenciando não apenas no consumo de bens e serviços, mas servindo como lugar de debate de assuntos de extrema importância, como política, economia e sociedade. É forçoso concluir, então, que apesar de se tratar de atividade do setor privado, os direitos e garantias envolvidos são permeados pelo interesse público (ARCHEGAS, 2021, p. 3).

Para James Grimmelman (2015, p. 47), a moderação pode ser entendida como o conjunto de mecanismos de governança que estruturam a participação em uma comunidade para facilitar a cooperação entre a mesma e os usuários e entre estes, bem como prevenir abusos.

Os moderadores de uma plataforma possuem o poder de promover ou apagar postagens, atrair, suspender ou banir usuários. Suas tomadas de decisão podem influenciar nos assuntos em debate, assim como pode retirar o que não lhes interessa ou beneficia (GRIMMELMANN, 2015, p. 45).

Nesse cenário, ao passo que é necessário limitar, de alguma forma, a disseminação de desinformação, é preciso também considerar que a detenção exclusivamente pelas plataformas digitais dos assuntos permitidos ou não no âmbito do debate público é extremamente perigoso, conforme se evidenciou nos casos da eleição de Donald Trump e do Brexit envolvendo a Cambridge Analytica.

Diante das crises econômica e migratória, no ano de 2015, ocorreu a eleição de uma maioria conservadora no parlamento britânico e se intensificaram os pleitos pela saída da Inglaterra da União Européia (UE). Foi aprovado um plebiscito, cuja campanha teve aproximadamente três meses de duração e é alvo de inúmeros questionamentos quanto a sua probidade, especialmente quanto aos grupos que apoiavam a saída da UE.

Nesse período, houve a formação de dois tipos de bolhas, pró e contra a saída do bloco europeu, fazendo com que os usuários recebessem informações acerca da narrativa que concordavam. O centro da polêmica, assim como na eleição de Trump, reside no envolvimento da Cambridge Analytica e outras

convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

empresas associadas, as quais coletavam dados não autorizados por meio de perfis do Facebook e desenvolviam notícias direcionadas a determinado público-alvo (CADWALLADR, 2017).

Nessa questão envolvendo a Cambridge Analytica, suas subsidiárias e a campanha de Trump, depoimentos de antigos membros da empresa apontam, ainda, o uso de microdados do Facebook, com o fim de construir perfis e manipular os algoritmos, por empresas russas, tanto na eleição de Trump, quanto na campanha pró Brexit. (BERNARDI, 2017, p. 47).

Estes casos demonstram não apenas os potenciais riscos do monopólio por parte das plataformas na moderação de conteúdo, mas apontam, principalmente, a necessidade de que sejam estabelecidos, por intermédio da regulação, critérios destinados a orientar e fiscalizar essa prática.

No Brasil, o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e o Código de Defesa do Consumidor (CDC) tocam, de alguma maneira, nos conflitos que envolvam moderação de conteúdo. Entretanto, não há nenhuma legislação em específico que determine as diretrizes a serem seguidas, dificultando sobremaneira o estabelecimento de responsabilidade dos provedores, os quais adotam apenas os guias e diretivas elaborados por eles próprios.

Dessa forma, há um grande risco na autorregulação, tendo em vista que ela é realizada conforme as regras da própria plataforma, e aliado à demanda social de que a rede seja um ambiente socialmente saudável, sem a infinidade de desinformações, os debates acerca da moderação ganharam força. Ao mesmo tempo em que as pessoas demandam atitudes dos provedores quanto a moderação de desinformação, se este for realizado sem qualquer parâmetro e fiscalização, caímos no risco de situações discriminatórias, no sentido de a plataforma manter apenas o que lhe convém.

2. A importância da regulação da moderação de conteúdo no contexto da desinformação

A divulgação de notícias com conteúdo desinformativo sempre existiu na história, especialmente em períodos eleitorais. Contudo, no Brasil, a partir da eleição de Dilma Rousseff no segundo turno em 2014, tal fenômeno, juntamente com os discursos permeados de intolerância e ódio nas redes sociais, se expandiu exponencialmente. A partir desse ano a polarização política acentuou-se, gerando uma série de protestos pelo país, a favor e contra o impeachment da presidente eleita.

Tal ambiente de instabilidade e polarização perdura até o presente momento, tendo se intensificado ainda mais durante a eleição de Jair Bolsonaro, no ano de 2018, cuja campanha eleitoral foi marcada pelo fenômeno da desinformação.

José Célio Filho (2021, p. 93) aduz estarmos passando por uma transição paradigmática, na qual a sociedade das corporações/organizações se converte em sociedade das plataformas. Sendo este um ambiente favorável à desinformação, em especial pelas características das redes sociais digitais, se mostra necessária a definição de novos mecanismos de regulação.

No que se refere à atividade regulatória, ela pode ser dividida, segundo Virginia Haufler (2003, p. 237), em quatro categorias: a regulação tradicional, a corregulação, a regulação por múltiplas partes interessadas e a autorregulação.

A regulação tradicional é aquela desenvolvida, promulgada e aplicada pelos governos nacionais. Na corregulação ou autorregulação o governo determina as diretrizes baseadas em limites constitucionais positivos e negativos e o setor privado estabelece os parâmetros e critérios técnicos de regulação. A regulação por múltiplas partes interessadas envolve, além da iniciativa privada e do Estado, atores como a sociedade civil não organizada e movimentos sociais. Nela, os consumidores atuam como os responsáveis pela aplicação final do sistema, pois fiscalizam o cumprimento ou não das normas estabelecidas pelas empresas. Por fim, no modelo de autorregulação, o setor privado, abrangendo todos os grupos interessados, desenvolve padrões técnicos de boas práticas. Tal sistema é baseado em ações e padrões voluntários (HAUFLER, 2003, p. 237-238).

O Marco Civil da Internet, em seu art. 19, estipula que “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, [...], tornar indisponível o conteúdo apontado como infringente”. Ou seja, condiciona a responsabilização à existência de uma ordem judicial determinando a retirada do conteúdo, consagrando o princípio da inimputabilidade da rede. (TEFFÉ; SOUZA, 2019, p. 7)

Entretanto, conforme explicitado no tópico anterior, a ausência de uma legislação específica faz permanecer o sentimento de insegurança, pois a au-

torregulação não é suficiente para fornecer a confiabilidade necessária¹⁰¹¹, tornando comuns os questionamentos acerca da autorregulação e da criação de leis acerca da moderação de conteúdo das mídias digitais.

São colocadas em pauta, por exemplo, questões abrangendo qual seria o grau de autonomia dos provedores para traçar regras dos conteúdos permitidos ou não em sua plataforma; quais seriam as formas de aplicação dessas regras e como poderiam os usuários questionar a sua aplicação.

O Congresso Alemão, no ano de 2017, aprovou a NetzDG (*Network Enforcement Act*), de cunho punitivista, que obriga as redes sociais e outros provedores que hospedam informações de terceiros a remover conteúdo “manifestamente ou obviamente ilegal” após serem notificadas, sob pena de multa. Uma das principais críticas é que referida lei transfere para a plataforma a tarefa de delimitar o que seria ou não legal conforme o direito alemão, tornando complexo o seu trabalho (ESTARQUE; ARHEGAS, p. 20).

O Reino Unido, por outro lado, adotou uma postura menos punitivista. Em 2019, o governo publicou o *Online Harms White Paper*, propondo a criação de um órgão público e independente responsável pela implementação de padrões que garantam a segurança dos usuários e, ao mesmo tempo, se preocupe com a proteção da liberdade de expressão (ESTARQUE; ARHEGAS, p. 21).

No Brasil há uma série de Projetos de Lei acerca de moderação de conteúdo, sendo a mais relevante a PL nº 2.630/2020, conhecida por “PL das *Fake News*”, que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, já aprovada pelo Senado e encaminhada para a Câmara dos Deputados, onde segue em tramitação.

Há uma série de pontos de atenção que deverão ser enfrentados pelo Congresso Nacional, por serem incompatíveis com os princípios da LGPD e do Marco Civil da Internet. Alguns desses pontos são “críticas ao processo legislativo

10. “A empresa tem sido acusada de alimentar o ódio e a desinformação em diversos países, como o Sri Lanka, e servir de plataforma para governos autoritários, como nas Filipinas. [...] Outro comportamento do Facebook que tem sido alvo de reprovação é a política de tratamento diferenciado dado a políticos, em comparação a usuários comuns. Em 2019, Nick Clegg, Vice-presidente global de Políticas Públicas e Comunicação do Facebook, anunciou que a plataforma não iria encaminhar publicações de políticos para verificação de checadores independentes, como faz com outros conteúdos.” (ESTARQUE, Marina. ARHEGAS, João Victor. *Redes sociais e moderação de conteúdo: criando regras para o debate público a partir da esfera privada*. Relatório ITS, p. 8-9. Disponível em: <<https://itsrio.org/pt/publicacoes/redes-sociais-e-moderacao-de-conteudo/>>. Acesso em: 10 jan. 2022)

11. “antes, intermediários como jornais e televisão controlavam apenas aquilo a que o indivíduo podia ou não ter acesso; hoje, o intermediário pode granularizar cada interação do indivíduo com a plataforma, fazendo um microgerenciamento entre indução do comportamento e a censura do conteúdo.” (PINHEIRO, Guilherme. PINHEIRO, Alexandre. *Buscadores e redes sociais: limites da moderação e da liberdade editorial dos provedores de aplicações na internet*. In *Revista Estudos Institucionais*, v. 7, n. 2, pg. 588-605, mai/ago 2021, p. 598)

opaco e apressado, impactos negativos à inovação tecnológica, isolamento do Brasil dentro do cenário internacional, imprecisões conceituais, definição problemática de ‘conta inautêntica’, estímulo à censura etc.” (ARCHEGAS, 2021).

Em razão da relevância do tema para a democracia do país, seria de se esperar que a sociedade civil teria ampla participação no processo de criação da lei, como ocorreu com o Marco Civil da Internet. Contudo, foi votado de forma apressada e sem o devido debate com os diversos setores da sociedade.

Outra problemática a ser enfrentada é o isolamento internacional que as inúmeras regras para o funcionamento de redes sociais e aplicativos de mensagens pode trazer para os usuários pátrios, tendo em vista que ao lançar no mercado um novo produto ou funcionalidade é possível que não se enquadre nas regras estabelecidas para o Brasil, tornando inviável sua operação. (ITS, 2020, p. 2)

Outrossim, o texto possui uma série de conceitos imprecisos e que entram em conflito com diplomas já existentes, como é o caso do conceito de provedor de aplicação. No Marco Civil da Internet podem ser provedores apenas pessoas jurídicas, enquanto o projeto de lei inclui também pessoa física.

O art. 4º, inciso III, do referido projeto de lei prevê como um dos objetivos da lei “a busca por maior transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais, com a garantia do contraditório e da ampla defesa”. Em seu art. 13, dispõe sobre a publicação, a ser feita pelos provedores de redes sociais, de relatórios de transparência, nos quais deve informar os procedimentos e decisões de tratamento de conteúdo gerados por terceiros. Esses relatórios seriam analisados por um Conselho de Transparência e Responsabilidade na Internet, que também poderia sugerir diretrizes para a moderação de conteúdo. Entretanto, tal Conselho seria criado pelo próprio Congresso Nacional e todos os membros indicados pelo Poder Legislativo, de forma que não possuiria independência e autonomia algumas (ARCHEGAS, 2021, p. 22).

Ainda, cumpre evocar a problemática da definição de conta inautêntica presente no art. 5º, inciso II, definida como aquela “criada ou usada com o propósito de assumir ou simular identidade de terceiros para enganar o público”. Tal conceito toca em assuntos complexos como anonimato e conflitos entre nome civil e social de pessoas trans. Conforme o dispositivo, seria de incumbência do provedor determinar se a conta seria ou não inautêntica e removê-la, ação completamente subjetiva e complexa. Ademais, por colocar o foco nessas contas, acaba por negligenciar assuntos como os comportamentos au-

tomatizados e a desinformação criada e compartilhada por contas autênticas, que podem atuar como base de legitimidade e de orientação para a atuação de uma rede robotizada, causando danos mais graves e extensos. (ITS, 2021, p. 3)

Por fim, o controle cada vez mais amplo e rigoroso que o projeto de lei insere, com a obrigatoriedade de monitoramento de contas inautênticas e de quais perfis estariam disseminando desinformações, pode atuar como agente de estímulo à censura, pois as plataformas poderiam remover contas que não estariam irregulares apenas por ser mais prático e para não serem multadas, ocasionando sucessivas lesões à liberdade de expressão.

O projeto inicial trazia um conceito para a desinformação, que foi retirado na proposta final aprovada pelo Senado Federal, após uma série de debates e resistência por parte de alguns grupos. O que se conclui desses debates é que é preciso muito cuidado na construção de uma legislação sobre o tema para evitar a violação de direitos e que sirva como instrumento de censura para calar a divergência política (RODRIGUES, 2020, p. 46-48).

A criação de rol taxativo dos conteúdos que devem ser moderados, por exemplo, representa uma ameaça, pois pode ser editado com o intuito de censurar e instaurar uma situação de autoritarismo, como é o caso da MP nº 1.068/2021, editada pela Presidência da República. O que se percebe, neste caso, é que a moderação de conteúdo foi utilizada em caráter inverso, ou seja, com o intuito de determinar os assuntos que devem ser moderados, controlando, a seu favor, o que lhe for benéfico.

Dessarte, é necessário ter cautela para não permitir que a regulação tradicional corrobore para a instalação de um Estado de vigilância e que a autorregulação confira poderes absolutos de moderação a entes privados.

Mostra-se necessária uma atuação plural dos mais diversos segmentos, através a coexistência da regulação e da autorregulação, sendo responsabilidade daquela definir as obrigações e padrões regulatórios mínimos, a fim de orientar a atuação dos provedores e, ao mesmo tempo, conferir certa autonomia para regular outros aspectos de suas atividades.

Considerações finais

A sociedade vivencia as consequências do aumento descontrolado de produção e circulação de informações. Paralelamente, a crise da pós-verdade e a ampla disseminação de desinformação formam o cenário ideal para que a população seja facilmente manipulada e alvo de medidas restritivas de direito, seja por parte do próprio Estado, que pode utilizar a regulação como meio de

implementar leis que censurem determinados assuntos, seja pelos próprios reguladores, como no envolvimento da Cambridge Analytica no Brexit e eleições norte americanas de 2016.

Diante desse cenário, e considerando a cultura antipolítica e antimídia que o planeta vem vivenciando, a indústria da desinformação tem o potencial de conduzir e influenciar a opinião pública, sendo apta a influenciar o resultado de eleições ou colocar em dúvida a existência de uma pandemia, por exemplo.

No período da pós-verdade, os indivíduos são atraídos pelo pensamento hegemônico, sem a preocupação de distinguir a verdade da não verdade. Há, na realidade, uma relativização da verdade, e as opiniões pessoais passam a ocupar um patamar superior aos fatos e evidências.

A regulação da moderação de conteúdo surge como uma necessidade para diminuir os prováveis danos oriundos da desinformação. Todavia, o assunto deve ser tratado com cautela e ser amplamente debatido pelos mais variados setores da sociedade, para que os direitos fundamentais sejam devidamente resguardados.

Ainda, deve-se ter em mente que um diploma legal, por si só, não resolverá as questões levantadas no presente trabalho, sendo necessário não apenas uma iniciativa legislativa, mas também um investimento em educação, para que a população desenvolva uma competência crítica e tenha capacidade para discernir as informações que recebe.

Referências

ALLCOTT, Hunt; GENTZKOW, Matthew. *Social Media and Fake News in the 2016 Election*. *Journal of Economic Perspectives, Cambridge*, v. 31, n. 2, p. 211–236, 2017. Disponível em: <<https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211>>. Acesso em: 14 abr. 2022.

AMARAL, Inês. SANTOS, Sofia José. Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade. In: *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Imprensa da Universidade de Coimbra. Coimbra, 2019.

ARCHEGAS, João Victor. Proteção de dados e transparência em moderação de conteúdo na Europa, Reino Unido e Brasil. Relatório ITS, 2021. Disponível em: <<https://itsrio.org/pt/publicacoes/protecao-de-dados-e-transparencia-em-moderacao-de-conteudo-na-europa-reino-unido-e-brasil/>>. Acesso em: 14 abr. 2022.

BERGAMO, Mônica. Google remove vídeos negando pandemia após intervenção do Ministério Público. Folha de São Paulo. Disponível em: <<https://www1.folha.uol.com.br/colunas/monicabergamo/2020/05/google-remove-videos-negando-pandemia-apos-intervencao-do-ministerio-publico.shtml>>. Acesso em: 14 abr. 2022.

BERNARDI, Ana Julia Bonzanini. Redes sociais, fake news e eleições: medidas para diminuir a desinformação nos pleitos eleitorais brasileiros. Porto Alegre, 2019. Disponível em: <<https://www.lume.ufrgs.br/handle/10183/197602>>. Acesso em 14 abr. 2022.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Editora Forense. Rio de Janeiro, 2019.

BOTELHO, Marcos César, et al. Eleições, Populismo e Desinformação: o papel das redes sociais frente a estigmatização da imprensa. In: 7 Journal of Institutional Studies 2, Revista Estudos Institucionais, v.7 , n. 2, p. 649-680, mai/ago 2021.

BRISOLA, Anna. BEZERRA, Arthur Coelho. Desinformação e circulação de “fake news”: distinções, diagnóstico e reação. XIX Encontro Nacional de Pesquisa em Ciência da Informação. Londrina, 2018.

CASTELLS, Manuel. A Galáxia da Internet: Reflexões sobre a Internet, os Negócios e a Sociedade. Rio de Janeiro: Zahar, 2003.

COMISSÃO EUROPEIA. *A Multi-dimensional Approach to Disinformation - Report of the independent High Level Group on fake news and online disinformation*. 2018. Disponível em: <<https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1>>. Acesso em: 14 abr. 2022.

CUETO, José Carlos. Origem do coronavírus: o que se sabe sobre o laboratório de Wuhan investigado pelos EUA. Disponível em: <<https://www.bbc.com/portuguese/internacional-57339240>>. Acesso em: 14 abr. 2022.

ESTARQUE, Marina. ARCHEGAS, João Victor. Redes sociais e moderação de conteúdo: criando regras para o debate público a partir da esfera privada. Relatório ITS, p. 20. Disponível em: <<https://itsrio.org/pt/publicacoes/redes-sociais-e-moderacao-de-conteudo/>>. Acesso em: 14 abr. 2022.

GRIMMELMANN, James. *The virtues of moderation*. Yale J.L. & Tech, 2015, p. 45. Disponível em: <<https://scholarship.law.cornell.edu/facpub/1486/>>. Acesso em: 14 abr. 2022.

HAUFLER, Virginia. *New forms of governance: certification regimes as social regulations of the global market*. 2003, p. 237-247. Disponível em: <https://www.researchgate.net/publication/252743812_New_forms_of_governance_Certification_regimes_as_social_regulations_of_the_global_market>. Acesso em: 14 abr. 2022.

INSTITUTO DE TECNOLOGIA E SOCIEDADE. Nota Técnica sobre os Projetos de Lei nº 2927/2020 (Câmara) e nº 2630/2020 (Senado). Rio de Janeiro, 2020. Disponível em: <https://itsrio.org/pt/publicacoes/nota-tecnica-its-pls-contr-fake-news/>. Acesso em: 18 abr. 2022.

ITAGIBA, Gabriel. Fake news e Internet: esquemas, bots e a disputa pela atenção. Disponível em: <https://itsrio.org/wp-content/uploads/2017/04/v2_fake-news-e-internet-bots.pdf>. Acesso em 14 abr. 2022.

Kit covid: o que diz a ciência? Saúde com Ciência. Centro de Comunicação Social da Faculdade de Medicina da UFMG. Disponível em: <<https://www.medicina.ufmg.br/kit-covid-o-que-diz-a-ciencia/>>. Acesso em: 14 abr. 2022.

MACHADO, Joana de Moraes Souza. A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil. Editora Fi. Porto Alegre, 2018.

PINHEIRO, Guilherme. PINHEIRO, Alexandre. Buscadores e redes sociais: limites da moderação e da liberdade editorial dos provedores de aplicações na internet. In *Revista Estudos Institucionais*, v. 7, n. 2, p. 588-605, mai/ago 2021.

PINHO FILHO, José Célio Belém de. Desinformação e regulação de redes sociais digitais. Dissertação de mestrado. São Paulo, 2021.

POSETTI, Julie. MATTHEWS, Alice. *A short guide to the history of 'fake news' and disinformation*. 2018, p. 1. Disponível em: <<https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module>>. Acesso em 14 abr. 2022.

RODRIGUES. Theófilo Codeço Machado, et al. Desinformação e crise da democracia no Brasil: é possível regular *fake news*? In *Confluências, Revista Interdisciplinar de sociologia e direito*, v. 22, n. 3, 2020, p. 30-52. Disponível em: <<https://periodicos.uff.br/confluencias/article/view/45470>>. Acesso em: 14 abr. 2022.

SANTOS, José Matheus. CRISPIM, Roberto. Bolsonaro desdenha de vacina e enaltece 'kit covid' um dia após CPI lhe atribuir 9 crimes na pandemia. Folha de São Paulo. Disponível em: <<https://www1.folha.uol.com.br/poder/2021/10/bolsonaro-desdenha-de-vacina-e-enaltece-kit-covid-um-dia-apos-cpi-apontar-9-crimes-dele-na-pandemia.shtml>>. Acesso em: 14 abr. 2022.

SERRANO, Pascual. A Desinformação: como os meios de comunicação ocultam o mundo. Tradução de Luisa Prieto Lamas. Editora SENGE-RJ. Rio de Janeiro, 2010.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso Pereira de. Fake News: Como garantir liberdades e conter notícias falsas na internet. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de. Autonomia Privada, Liberdade Existencial e Direitos fundamentais. Belo Horizonte: Fórum, p. 525-543, 2019.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça. Revista IBERC, v. 1, n. 1, p. 01-28, nov.-fev./2019, Minas Gerais.

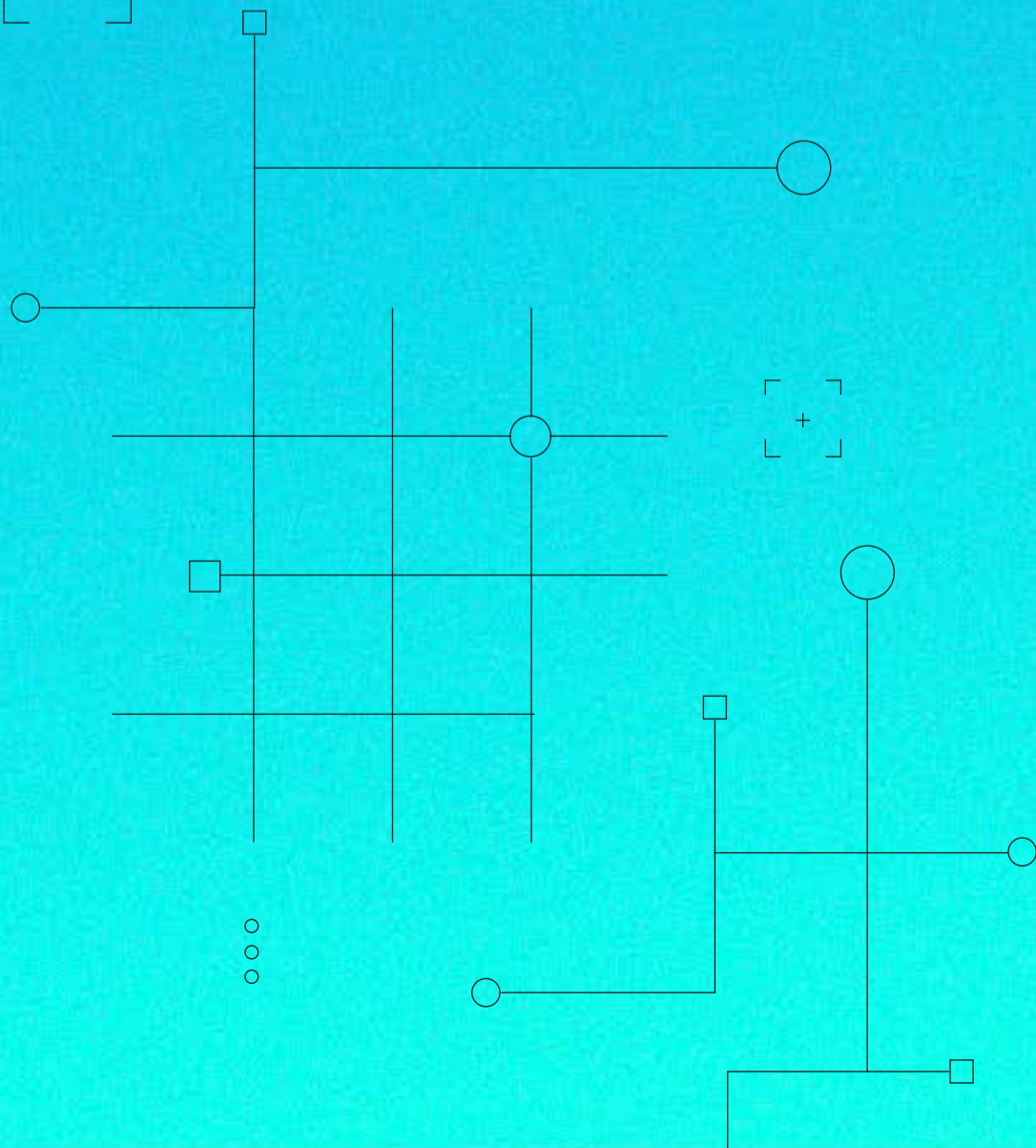
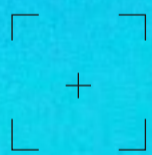
UNESCO. Jornalismo, *fake news* e desinformação: manual para educação e treinamento em jornalismo. 2019. Disponível em: <<https://unesdoc.unesco.org/ark:/48223/pf0000368647>>. Acesso em: 14 abr. 2022.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

12

A utilização das criptomoedas para a solução dos problemas urbanos: Ecochain e Gestão Integrada dos Resíduos Sólidos

GABRIEL MACIEL DE LIMA



Sumário: Introdução. 1. O crescimento urbano brasileiro e a Gestão Integrada dos Resíduos Sólidos. 2. As criptomoedas e blockchains na solução dos problemas urbanos. 3. Ecochain Moeda Verde: uma criptomoeda social no incentivo da gestão eficiente do lixo. Considerações finais. Referências.

Introdução

A popularização da internet e o advento do ambiente digital geraram um novo mercado, suscetível a constantes inovações e que transcende os limites dos estados nacionais. Esse novo ambiente fortaleceu o fenômeno da globalização, haja vista que facilitou a conexão entre regiões e modificou os conceitos de tempo e espaço.

Contudo, do mesmo modo que a internet trouxe melhorias ao mundo globalizado, criou novas necessidades, nunca antes pensadas, motivo pelo qual tornou-se imprescindível o incentivo à inovação nesse meio, para buscar a solução desses anseios.

O surgimento do comércio eletrônico (*e-commerce*) é exemplo disso, ao passo que acelerou os processos de venda e de transações entre indivíduos, estes que começaram a ficar insatisfeitos com a atuação rígida e burocrática das instituições bancárias, em razão de se verem limitados e muitas vezes impedidos de concretizar as transações de forma virtual, em face da exigência de realização de operações de desbloqueio de cartões ou aparelhos presencialmente.

Nesse sentido, surgiram as criptomoedas, moedas criadas para e pelo mundo virtual, como forma de assegurar a circulação de riquezas entre usuários do ambiente virtual, sem a necessidade de intermediários bancários.

O mundo está passando por uma verdadeira revolução no mercado monetário e cambial, tendo em vista as inúmeras modificações que essas novas moedas estão trazendo à economia. Com o passar do tempo e com o desenvolvimento da tecnologia *blockchain*, novas criptomoedas estão sendo criadas com o intuito de solucionar problemas existentes, dentre eles, os de estruturação e gestão das cidades.

1. Doutorando em Direito pela Universidade Federal de Pernambuco. Mestre em Direito pela Universidade Federal do Rio Grande do Norte. Bacharel em Direito pela Universidade Federal do Rio Grande do Norte. Membro do Grupo de Pesquisa Integração Regional, Globalização e Direito Internacional, da Universidade Federal de Pernambuco.

Nesse diapasão, cabe destacar a iniciativa da Ecochain Moeda Verde, criptomoeda social que incentiva práticas de reutilização e reciclagem de resíduos sólidos, atuando diretamente na redução do problema da produção do lixo no Brasil, criando uma gestão integrada de resíduos sólidos, conforme previsão da Lei Federal nº 12.305/2010.

Diante disso, esta pesquisa objetiva estudar os conceitos de criptomoe-da e *blockchains*, desenvolver o conceito de criptomoe-das sociais, analisar as iniciativas de criação de moedas virtuais que visam solucionar problemas das cidades e analisar a legalidade dessas novas moedas.

1. O problema do lixo no Brasil e a Gestão Integrada dos Resíduos Sólidos

O crescimento populacional no Brasil e o processo violento de urbanização geram prejuízos ambientais incalculáveis, principalmente no tocante à produção e destinação de resíduos sólidos. Isto porque, no último século, a formação das cidades brasileiras ocorreu de forma acelerada, desigual e conseqüentemente desordenada, o que ocasionou uma carência de políticas públicas ligadas ao planejamento urbano e espacial, resultando em um quadro de instabilidade social e ambiental (BEZERRIL, 2016).

Entre 2017 e 2018, cada brasileiro gerou pouco mais de um quilograma de resíduos sólidos por dia (ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE LIMPEZA PÚBLICA E RESÍDUOS ESPECIAIS, 2019, p, 12). Desse modo, é possível concluir que, a cada vinte segundos, a produção de lixo no Brasil aumenta, em média, 1 kg/dia.

Atualmente, o Brasil é o 4º maior produtor de lixo plástico no mundo, gerando uma média de 11.300.000 toneladas, sendo ultrapassado apenas pelos Estados Unidos, China e Índia (WWWF-BRASIL, 2021). Do total, mais de 10.300.000 toneladas foram coletadas (91%), mas apenas 145.000 toneladas (1,28%) foram efetivamente recicladas (WWWF-BRASIL, 2021). Esse é um dos menores índices da pesquisa e se encontra bem abaixo da média global de reciclagem plástica, que é de 9% (WWWF-BRASIL, 2021).

Diante do evidente problema na gestão dos resíduos sólidos no Brasil, urge a necessidade de estudar com maior profundidade o conteúdo da Lei Federal nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos (PNRS) (BRASIL, 2010).

O artigo 4º da Lei Federal nº 12.305/2010 define a Política Nacional de Resíduos Sólidos como o conjunto de princípios, objetivos, instrumentos, diretrizes, metas e ações adotados pelo Governo Federal, isoladamente ou em regime de cooperação com Estados, Distrito Federal, Municípios e/ou particulares, com o intuito de instituir gestão integrada e o gerenciamento ambientalmente adequado dos resíduos sólidos (BRASIL, 2010).

Resíduo sólido, conforme previsto na supramencionada Lei, no seu artigo 3º, inciso XVI, é todo material, substância, objeto ou bem descartado resultante de atividades humanas em sociedade, cuja destinação se procede nos estados sólido ou semissólido, bem como os gases contidos em recipientes e líquidos cujas particularidades tornem inviável o seu descarte na rede pública de esgotos ou em corpos de água (BRASIL, 2010).

Assim, depreende-se que a Política Nacional de Resíduos Sólidos visa a gestão satisfatória do lixo, preocupando-se com o gerenciamento adequado dos resíduos produzidos. A administração eficiente dos resíduos sólidos depende da atuação conjunta do poder público e do privado, de forma a promover o desenvolvimento de políticas públicas integradas para o tratamento dos detritos.

Dentre os objetivos da PNRS, dispostos no artigo 7º da Lei Federal nº 12.305/2010, estão a gestão integrada de resíduos sólidos e a articulação entre as diferentes esferas do poder público, e destas com o setor empresarial, com o intuito de desenvolver cooperação técnica e financeira para a gestão integrada de resíduos sólidos (BRASIL, 2010).

Estes objetivos evidenciam a preocupação do legislador em garantir o trabalho solidário entre os diversos setores do poder público e particulares, estes que devem participar igualmente da governança das políticas públicas de gestão do lixo.

O conceito de governança trata do *modus operandi* das políticas governamentais que abrangem questões relacionadas: à definição da mistura entre o público e privado nas políticas públicas; à participação e descentralização das obrigações; aos mecanismos de financiamento e ao alcance global das políticas públicas; e ao modelo político e institucional dos processos de decisão (LIMA; LIMA, 2017).

Apesar de existir confusão entre os conceitos de governança e governo, importa destacar que são conceitos totalmente diferentes. Enquanto o governo sugere atividades sustentadas por uma autoridade formal, pelo poder de polícia que garante a implementação das políticas devidamente instituídas,

a governança diz respeito às atividades apoiadas em objetivos comuns, que podem ou não advir de responsabilidades formais e não dependem, obrigatoriamente, do poder de polícia para que sejam aceitas e prosperem frente a possíveis resistências (LIMA; LIMA, 2017).

A Lei Federal nº 12.305/2010, que institui a Política Nacional dos Resíduos Sólidos, estabelece como prioridade para a gestão do lixo a atuação conjunta dos atores da sociedade, particulares ou oriundos do poder público, de modo a desenvolver uma governança integrada, participativa e eficiente para sanar o problema do lixo no Brasil.

O artigo 10 da supramencionada lei dispõe ser de incumbência do Distrito Federal e dos Municípios a gestão integrada dos resíduos sólidos gerados nos respectivos territórios, sem prejuízo das competências de controle e fiscalização dos órgãos federais e estaduais (BRASIL, 2010). No artigo 25, por sua vez, fica evidente a responsabilidade conjunta da administração pública, setor empresarial e coletividade pela efetividade das ações voltadas para assegurar a observância da PNRS (BRASIL, 2010).

A Lei Federal nº 12.305/2010 ainda prevê, no artigo 30, a instituição da responsabilidade compartilhada pelo ciclo de vida dos produtos, que consiste em uma série de etapas que envolvem o desenvolvimento do produto, a obtenção de matérias-primas e insumos, o processo produtivo, o consumo e a disposição final do resíduo sólido (BRASIL, 2010).

Dentre os objetivos desta gestão compartilhada, é possível citar os seguintes: promover o aproveitamento de resíduos sólidos, direcionando-os para a sua cadeia produtiva ou para outras cadeias produtivas; e estimular o desenvolvimento de mercado, a produção e o consumo de produtos derivados de materiais reciclados e recicláveis (BRASIL, 2010).

Com o aumento da produção do lixo no Brasil, a preocupação com o desenvolvimento de políticas que reduzam os impactos ambientais da geração de resíduos sólidos se tornou mais patente. Um dos principais objetivos da Política Nacional de Resíduos Sólidos brasileira, conforme previsão do artigo 7º, inciso II, da Lei Federal nº 12.305/2010, é a não geração, redução, reutilização, reciclagem e tratamento dos resíduos sólidos, bem como disposição final ambientalmente adequada dos rejeitos (BRASIL, 2010).

Para melhor compreensão dos dispositivos legais, importa diferenciar reciclagem, que consiste no processo de transformação dos resíduos sólidos envolvendo a alteração de suas propriedades físicas, físico-químicas ou biológicas, com vistas à transformação em insumos ou novos produtos; de reu-

tilização, que é o processo de aproveitamento dos resíduos sólidos sem sua transformação biológica, física ou físico-química (BRASIL, 2010).

A Lei Federal nº 12.305/2010, no artigo 7º, também prevê como principais objetivos da PNRS o incentivo à indústria da reciclagem, por fomentar o uso de matérias-primas e insumos derivados de materiais recicláveis e reciclados, de modo a reduzir a produção de resíduos sólidos; e integração dos catadores de materiais reutilizáveis e recicláveis nas ações que envolvem a responsabilidade compartilhada pelo ciclo de vida dos produtos (BRASIL, 2010).

O papel dos catadores de materiais reutilizáveis e recicláveis na gestão integrada dos recursos é imprescindível, haja vista que eles são parte fundamental para a administração eficiente dos resíduos sólidos.

Apenas na América Latina, cerca de 4.000.000 de pessoas sobrevivem do lixo, enquanto em todo o mundo 15.000.000 de indivíduos vivem dos resíduos sólidos (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2021). A longa cadeia de intermediários na gestão ineficiente do lixo faz com que cerca de 75% daqueles trabalhem de forma insalubre, procurando algo para vender em montanhas de lixo (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2021).

Projetos que integram os catadores diretamente nas ações que envolvam a responsabilidade compartilhada pelo ciclo de vida dos produtos não só servem para dirimir o problema dos resíduos sólidos brasileiros, mas também são importantes vetores para a melhoria social desses indivíduos, na medida em que melhoram as condições de trabalho destes e reduzem os intermediários.

Para que seja possível a implementação da Política Nacional de Resíduos Sólidos brasileira, prevista na Lei Federal nº 12.305/2010, é necessário que ocorra no Brasil uma reestruturação da governança do lixo, de modo a promover e desenvolver políticas públicas integradas, com a participação do setor público e privado, que visem a reutilização e reciclagem dos resíduos sólidos, o que resultaria em uma redução dos impactos ambientais provenientes dos rejeitos.

2. As criptomoedas e blockchains na solução dos problemas urbanos

Conforme será amplamente discutido neste tópico e nos que seguem, estão eclodindo no mundo inúmeras iniciativas de criptomoedas que pretendem solucionar os problemas urbanos. Como exemplo, é possível mencionar que o setor da produção e consumo de energia elétrica está passando por uma ver-

dadeira transformação, haja vista que já surgiram iniciativas que solucionam o problema da produção, escoamento e comercialização de energias renováveis (MOUGAYAR, 2017, p, 124-125).

Em razão da crescente inclusão das criptomoedas na economia mundial e do fortalecimento dessas moedas, em especial o *Bitcoin*, urge a necessidade do estudo dessa nova riqueza, seu conceito e funcionamento, bem como a sua relevância para o Desenvolvimento Nacional.

Nesse sentido, importa destacar o conceito de criptomoeda, também denominada de moeda virtual. Criptomoeda, em apertada síntese, é uma espécie de dinheiro virtual utilizado na intermediação de compra e venda de produtos, não sendo emitida por um banco central ou governo (SOUZA, 2018).

As criptomoedas são unidades de valor virtuais que surgem de forma não discricionária e altamente rígida (SOUZA, 2018). Diferentemente das moedas físicas, as moedas virtuais não são controladas por um banco central, transcendendo os limites estatais, sendo o seu valor de troca definido pela pura relação entre oferta e procura (SOUZA, 2018).

Frise-se que as moedas virtuais não podem ser confundidas com a virtualização do papel-moeda, tendo em vista que esta trata de um título financeiro que se encontra vinculado a uma determinada quantia de moeda física. Por exemplo, no momento que são realizadas transferências de valores entre contas correntes bancárias pela internet, se está transferindo dinheiro físico representado no meio eletrônico.

Contudo, este papel-moeda “virtualizado” nada mais é do que uma forma de facilitar as transações bancárias, não se assemelhando com o conceito de criptomoeda, que trata de uma moeda completamente digital e criada no ambiente da internet, não necessitando de intermediadores bancários para existir ou serem transferidas.

Uma moeda digital é como uma moeda real, contudo, não é emitida por bancos centrais nem é apoiada financeiramente na Moeda Nacional (ANDRADE, 2017). A emissão dessa moeda é descentralizada, não sendo decidida por aspectos políticos, mas puramente técnicos (ANDRADE, 2017).

A autoria do *Bitcoin*, primeira criptomoeda criada, foi conferida ao programador japonês com pseudônimo Satoshi Nakamoto, este que em 2009 desenhou e implementou o esquema de transferências da referida criptomoeda (EUROPEAN CENTRAL BANK, 2021). O sistema de transferência dos *Bitcoins* é baseado em uma arquitetura denominada *peer-to-peer*, formada por rede de computadores onde cada ponto (usuário) funciona como cliente e servidor,

permitindo o livre compartilhamento de dados sem a necessidade de um servidor central (EUROPEAN CENTRAL BANK, 2021).

O *Bitcoin* é uma moeda que ultrapassa as fronteiras de uma nação, podendo ser usado como moeda em todos os tipos de transação, competindo diretamente com as moedas oficiais já consolidadas, quais sejam, o Euro, o Dólar norte-americano, ou o Real (EUROPEAN CENTRAL BANK, 2021). Apesar de o *Bitcoin* ser a moeda virtual mais conhecida no mundo, outras criptomoedas estão se fortalecendo no mercado.

Em razão das características da arquitetura formada para o compartilhamento de criptomoedas, a utilização destas não necessita de intermediário bancário, tendo em vista que os próprios usuários se interligam e realizam transações entre si.

Essa arquitetura formada consiste nos *blockchains*, tecnologias que abrigam hoje a maior parte das moedas virtuais do mundo. Um *blockchain* é uma cadeia cronologicamente ordenada de blocos protegidos por um processo de resolução de fórmulas matemáticas denominadas *proof-of-work* (FERREIRA; PINTO; SANTOS, 2017). O encadeamento funciona pela adição de um algoritmo (*hash*) resultante do bloco anterior ao bloco seguinte, fazendo com que aquele torne-se parte do resultado seguinte (FERREIRA; PINTO; SANTOS, 2017).

Os blocos alinhados consecutivos asseguram que as transações sejam enviadas em ordem cronológica, fazendo com que uma operação não possa ser alterada com antecedência sem a modificação de todo o bloco (FERREIRA; PINTO; SANTOS, 2017). Além disso, a base de dados de um *blockchain* somente aceita a inclusão de blocos novos, nunca a remoção de dados já existentes, motivo pelo qual a referida tecnologia guarda todo o histórico das transações, desde a sua criação até a atualização mais recente (BRAGA; MARINO; SANTOS, 2017).

Em razão disso, um *blockchain* é um ambiente seguro para o registro de dados e operações, tendo em vista que não comporta adulteração ou modificação dos registros já realizados (BRAGA; MARINO; SANTOS, 2017). A cadeia de blocos é mantida simultaneamente por todos os nós da grande rede, não existindo local principal de armazenamento de dados suscetíveis a ataques ou modificações (BRAGA; MARINO; SANTOS, 2017).

Como o sistema se baseia em um mecanismo de incontáveis fórmulas derivadas de outros resultados, torna-se impossível a modificação dos dados já existentes, tendo em vista que o usuário teria que ter acesso à todas as fórmu-

las resultantes do somatório dos dados dos blocos. Para alterar os dados, o invasor teria que controlar mais de 51% do poder computacional da rede inteira, o que seria inviável (SOUZA, 2018, p. 68-69).

Ademais, em razão da divulgação de todas as transações de dados realizadas no sistema, torna-se impossível a falsificação de dados, pois, além das dificuldades supramencionadas, todos os usuários conseguem ter acesso aos dados apresentados, sendo praticamente impossível a realização de adulteração sem a ciência de todos os membros do sistema (SOUZA, 2018, p. 68-69). Um *blockchain* é um grande “livro contábil digital”, tendo em vista que todos os dados inseridos no sistema não podem ser alterados, bem como é possível o acesso às suas informações pelo público em geral.

A tecnologia de transações das criptomoedas, qual seja, o *blockchain* gera uma grande segurança na aquisição e utilização das moedas virtuais, tendo em vista que é praticamente impossível fraudar o sistema para adulterar as suas informações, bem como para realizar furtos dos bens dos seus usuários.

Os *blockchains* programáveis, como por exemplo o *Ethereum*, tem viabilizado uma verdadeira transformação nos mais variados âmbitos, chegando a desenvolver, inclusive, novos mercados e soluções que se utilizam do valor monetário das criptomoedas. Os indivíduos agora conseguem gerar renda por meio de ações simples do dia-a-dia, como o compartilhamento de seus dados ou a venda de excedente de energia produzida em sua residência (MOUGAYAR, 2017, p. 124-125).

Com o surgimento e desenvolvimento da *World Wide Web* (*www*), primeiro ambiente público da *internet*, empresas e programadores voltaram os seus esforços para a criação e desenvolvimento de soluções aos anseios sociais. Da mesma forma, com a ascensão dos *blockchains*, novos ambientes da *internet*, muitas iniciativas estão sendo criadas para sanar as necessidades sociais, dentre eles, os problemas das cidades.

Nesse sentido, é fundamental destacar uma importante iniciativa brasileira, a criptomoeda Ecochain Moeda Verde, criptomoeda social que visa incentivar os hábitos da reutilização e reciclagem de resíduos sólidos, de modo a contribuir ativamente para dirimir os problemas da gestão do lixo no Brasil.

3. Ecochain Moeda Verde: uma criptomoeda social no incentivo da gestão eficiente do lixo

Conforme mencionado no tópico anterior, a criptomoeda Ecochain Moeda Verde é uma iniciativa brasileira que visa incitar as práticas de reutilização e reciclagem do lixo, funcionando como um vetor de desenvolvimento ambiental e social. Antes de adentrar no funcionamento da Ecochain e sua relevância para o desenvolvimento brasileiro, importa primordialmente destrinchar o conceito de moeda social.

Atualmente, todos os países possuem a denominada moeda “oficial”, também conhecida como moeda corrente, que é a unidade de valor emitida por um determinado país, sendo o representativo do dinheiro em circulação de uma nação. No Brasil, criado pela Medida Provisória 546/94 (BRASIL, 1994) e atualmente normatizado pela Lei Federal nº 9.069/95 (BRASIL, 1995), o Real (R\$) é a moeda corrente.

A moeda social, por sua vez, é uma forma de moeda paralela, funciona de modo colateral à moeda corrente, sendo criada e administrada por seus próprios usuários, oriunda, portanto, da esfera privada da economia (SOARES, 2006, p. 135-136). Esse tipo de moeda não necessita ter qualquer vínculo com a moeda nacional, e sua circulação é baseada na confiança mútua entre os usuários, participantes de um grupo originado por adesão voluntária (SOARES, 2006, p. 135-136).

Em cada iniciativa de nova moeda social, a combinação dos valores que se pretende alcançar pode mudar, mas de maneira geral, dois significados gerais aparecem recorrentemente, quais sejam: a) a unidade de valor como “meio de troca” alternativo ou complementar, capaz de gerar melhores condições de vida aos aderentes; e b) como prática de reinvenção da economia, reconstruindo-a em moldes responsáveis e participativos, de forma integrada com outras esferas da vida (SOARES, 2006, p. 135-136).

Assim, para que se configure uma moeda social, é necessário que a unidade de valor possa ser utilizada como meio de troca, capaz de gerar melhorias nas vidas dos seus usuários, bem como que circule paralelamente à moeda corrente de uma comunidade. A confiança mútua entre os usuários, estes que não são obrigados a utilizar a moeda social, é indispensável, sendo fator determinante para o funcionamento da nova moeda.

Com o avanço da tecnologia e advento dos *blockchains* é possível que se conceba a necessidade de criação e desenvolvimento de um outro conceito, o de criptomoeda social. Isto porque, as relações com o “dinheiro” mudaram

drasticamente com o advento das moedas virtuais, estas que vêm modificando totalmente as formas de se contratar, negociar e transferir valores.

Assim como as moedas sociais, as criptomoedas sociais também funcionam paralelamente à moeda corrente, não possuindo quantificação fixa na unidade monetária de um país. As criptomoedas, de uma forma geral, são avaliadas na moeda corrente de uma comunidade, com base no valor concebido a partir da “oferta” e da “procura”.

Todavia, o valor monetário destas não é atrelado, necessariamente, às moedas nacionais, sendo estas apenas utilizadas para a compra e venda daquelas. Atualmente, já é possível utilizar as moedas virtuais como “meio de troca” alternativo ou complementar, sem vincular o seu valor às moedas nacionais.

Ademais, a criptomoeda social, diferentemente da moeda social, por funcionar em *blockchains* e conseqüentemente na *internet*, possui grande escalabilidade, sendo possível que aquela atinja ambientes e comunidades mais vastos e que consiga alcançar mais usuários.

A criptomoeda social amplia também a característica de confiança entre os usuários, inerente à moeda social, na medida em que a sua utilização é ambientada em *blockchains*. Conforme já esmiuçado no tópico antecedente, esses sistemas funcionam grandes “livros contábeis digitais”, tendo em vista que todos os dados inseridos no sistema não podem ser alterados.

Além disso, em um *blockchain*, todos os usuários conseguem ter acesso aos dados apresentados, sendo praticamente impossível a realização de adulteração sem a ciência de todos os membros do sistema.

A moeda virtual social possui um protocolo de confiança inerente ao sistema em que é ambientada, razão pela qual, para que exista confiança, não é necessário que todos os membros da comunidade se conheçam e se relacionem diretamente, o que aumenta a escalabilidade dessa nova tecnologia.

Destaque-se que a criptomoeda social, além de buscar a inserção do indivíduo na sociedade, promovendo políticas de desenvolvimento social, também visa incluir os cidadãos de uma comunidade nos ambientes virtuais, meio em que são transacionadas as criptomoedas. Os usuários dessas tecnologias passam a participar da nova dinamicidade das formas de contratar, pagar e transacionar dinheiro, atuando ativamente na revolução financeira pela qual os países estão passando.

Superado o desenvolvimento do conceito de criptomoeda social, importa apresentar a iniciativa da Ecochain Moeda Verde, moeda virtual social que

pretende reduzir os impactos da produção de resíduos sólidos no Brasil, por meio do incentivo à reutilização e reciclagem.

O Projeto Moeda Verde – Cidade Limpa foi instaurado pela Secretaria Municipal da Saúde de Santa Cruz da Esperança (SP), por meio da Lei Municipal nº 434/2017, que criou a Moeda Verde, utilizada como remuneração recebida pela entrega de materiais recicláveis por parte da população (SANTA CRUZ DA ESPERANÇA/SP, 2017). O lixo reciclável e reutilizável entregue ao Município era antes trocado por uma nota de plástico, a Moeda Verde, muito parecida com a antiga nota de R\$ 1,00 (um real), esta que podia ser utilizada no comércio local para a aquisição de alguns produtos (TIINSIDE, 2021).

A *startup* Ecochain, em parceria com a exchange de criptomoedas FlowBTC, a empresa de soluções para cidades Ti2Ci, e a especialista em inovação tecnológica LF1, levando em consideração o projeto Moeda Verde, desenvolveram a Ecochain – Moeda Verde (ECOs), criptomoeda social substitutiva da antiga moeda de plástico distribuída pelo Município de Santa Cruz da Esperança (ROSA, 2021).

Com o advento da ECOs o processo de troca de resíduos sólidos recicláveis e reutilizáveis por “dinheiro” continuou o mesmo, todavia, o uso da criptomoeda social conferiu confiabilidade e transparência, além de acelerar as transações (TIINSIDE, 2021). Além disso, a remuneração que antes era feita de maneira mecânica, agora ocorre de forma descentralizada, por meio do *blockchain* programável *Ethereum* (TIINSIDE, 2021).

A nova criptomoeda social também possibilita que o usuário troque a sua remuneração resultante do recolhimento do lixo por *Bitcoin*, outras criptomoedas ou por moeda corrente, diferentemente do que ocorria antes, qual seja, a substituição da Moeda Verde apenas por produtos em lojas locais (TIINSIDE, 2021). O processo antes restrito e aplicável apenas em pequenas comunidades, característica inerente da moeda social, se transformou em uma verdadeira fonte de renda alternativa para os catadores.

Outro ponto importante é que a iniciativa da criptomoeda social não gera ônus ao Poder Público, na medida em que os custos com a remuneração aos usuários são supridos pela venda do material reciclável e reutilizável às empresas (AGENDA AMBIENTAL DA ADMINISTRAÇÃO PÚBLICA, 2021).

Para fazer parte do projeto, o voluntário precisa apenas fazer o seu cadastro no site Ecochain Moeda Verde, aplicativo da iniciativa, na prefeitura das cidades parceiras ou em um posto de coleta (ROSA, 2021). O saldo da carteira do usuário pode ser acessado em qualquer dispositivo móvel, mas os tokens

também são disponibilizados em formato de QR Code físico, para os usuários que não possuem acesso à internet (ROSA, 2021).

É possível classificar a ECOs como criptomoeda social, na medida em que estas possuem escalabilidade e confiabilidade inerente à tecnologia *block-chain*. Além disso, trazem benefícios sociais e inclusão tecnológica, em razão de gerar uma nova fonte de renda aos voluntários que recolhem os resíduos sólidos reutilizáveis e recicláveis, estes que podem ser usados no ambiente digital ou substituído por moeda corrente.

Para que seja possível destacar a importância da supramencionada criptomoeda social, é fundamental destacar o conceito de Desenvolvimento Sustentável. Assim, o desenvolvimento deve ser pautado nos seguintes requisitos: na satisfação das necessidades básicas; na solidariedade com as futuras gerações; na participação da população envolvida; na preservação do meio ambiente e dos recursos naturais; na estruturação de um sistema social que garanta emprego, segurança social e respeito a outras culturas; e em programas de educação (GALLO, 2007).

A criptomoeda social ECOs é um importante vetor para o Desenvolvimento Sustentável brasileiro, na medida em que visa a preservação do meio ambiente e recursos naturais, por criar uma “nova vida” para o lixo. Além disso, a ECOs gera uma nova fonte de renda para os indivíduos, estes que atuam como vetores do desenvolvimento nacional.

Apesar da evidente importância da iniciativa, é imprescindível destacar que esta pode encontrar dificuldades de implementação, em razão dos grandes empecilhos no uso de criptomoedas em território brasileiro.

Em recente comunicado emitido em 16 de novembro de 2017, registrado sob o nº 31.379, o Banco Central do Brasil publicou um alerta sobre os supostos riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais (BANCO CENTRAL DO BRASIL, 2017). O BCB frisou que as criptomoedas não são emitidas ou garantidas por nenhuma autoridade monetária, motivo pelo qual não têm garantia de conversão para moedas nacionais (BANCO CENTRAL DO BRASIL, 2017). Segundo o órgão, o valor das moedas virtuais decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor (BANCO CENTRAL DO BRASIL, 2017).

O BCB ainda realçou que as empresas que negociam moedas virtuais não são reguladas ou supervisionadas pelo referido órgão. Ademais, ressaltou que não há no arcabouço legal e regulatório relacionado com o Sistema Financeiro Nacional, dispositivo específico sobre moedas virtuais (BANCO CENTRAL DO

BRASIL, 2017). O Banco Central do Brasil, afirmou que não regula nem supervisiona operações com moedas virtuais (BANCO CENTRAL DO BRASIL, 2017).

Os usuários que desfrutam das e trabalham com as criptomoedas ainda enfrentam grandes restrição para a utilização das moedas virtuais no âmbito brasileiro. Isto porque ainda existem inúmeros entraves para o uso das criptomoedas em território brasileiro, em razão da inexistência de regulação acerca do tema e pela sua recente inclusão no Brasil.

Contudo, mesmo com o posicionamento contrário do Banco Central do Brasil, iniciativas como a da criptomoeda ECOs devem ser desenvolvidas no Brasil. A Ecochain Moeda Verde é indispensável para a Política Nacional de Resíduos Sólidos.

Conforme mencionado, projetos que integram os catadores diretamente nas ações que envolvam a responsabilidade compartilhada pelo ciclo de vida dos produtos não só servem para dirimir o problema dos resíduos sólidos brasileiros, mas também são importantes vetores para a melhoria social desses indivíduos, na medida em que melhoram as condições de trabalho destes e reduz os intermediários.

Além disso, para que seja possível a implementação da Política Nacional de Resíduos Sólidos brasileira, prevista na Lei Federal 12.305/2010, é necessário que ocorra no Brasil a promoção e desenvolvimento de políticas públicas integradas, com a participação do setor público e privado, que visem a reutilização e reciclagem dos resíduos sólidos, resultando em uma redução dos impactos ambientais provenientes dos rejeitos.

A criptomoeda social ECOs desenvolve a política integrada de resíduos sólidos, em razão de empresas, Poder Público e população atuarem juntos na política para a reutilização e reciclagem de resíduos sólidos. Além disso, a referida criptomoeda ainda integra os catadores diretamente às políticas de gestão do lixo, gerando para eles uma fonte de renda direta, confiável e digna.

Considerações finais

O problema da gestão do lixo no Brasil é resultante da ineficiência da administração pública. A produção de lixo dos centros urbanos brasileiros cresce exponencialmente, todavia, as cidades ainda não possuem políticas de coleta de resíduos sólidos de qualidade, razão pela qual a situação da gestão do lixo no Brasil carece de melhorias urgentes.

Para que seja possível a implementação da Política Nacional de Resíduos Sólidos brasileira, prevista na Lei Federal 12.305/2010, é necessário que ocor-

ra no Brasil a promoção e desenvolvimento de políticas públicas integradas, com a participação do setor público, privado e com a inclusão dos catadores, que visem a reutilização e reciclagem dos resíduos sólidos, resultando em uma redução dos impactos ambientais provenientes dos rejeitos.

As novas moedas virtuais com cunho social podem ser conceituadas como criptomoedas sociais, na medida em que substituem o conceito de moeda social já existente, por trazerem maior confiabilidade, escalabilidade e por levar os cidadãos aos novos ambientes virtuais, fazendo com que estes façam parte da nova revolução dos setores monetário e cambial.

A Ecochain Moeda Verde pode ser classificada como criptomoeda social, na medida em que incentiva práticas de reutilização e reciclagem de resíduos sólidos, esta que atua diretamente na redução do problema da produção do lixo do Brasil, criando uma gestão integrada de resíduos sólidos.

Apesar dos embargos burocráticos ao uso das criptomoedas no Brasil, as criptomoedas sociais como a ECOs devem ser desenvolvidas, haja vista que estas funcionam como ferramenta indispensável à Política Nacional de Resíduos Sólidos.

A referida criptomoeda desenvolve a política integrada de resíduos sólidos, em razão de empresas, Poder Público e população atuarem juntos na política para a reutilização e reciclagem de resíduos sólidos. Além disso, ela ainda integra os catadores diretamente às políticas de gestão do lixo, gerando para eles uma fonte de renda direta, confiável e digna.

Referências

AGENDA AMBIENTAL DA ADMINISTRAÇÃO PÚBLICA. **Moeda Verde**. Disponível em: <https://a3p.eco.br/produto/moeda-verde-santa-cruz-da-esperanca/>. Acesso em: 27 ago. 2021.

ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, 2017.

ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE LIMPEZA PÚBLICA E RESÍDUOS ESPECIAIS (ABRELPE). **Panorama dos resíduos sólidos no Brasil 2018/2019**. São Paulo: ABRELPE, 2019.

BANCO CENTRAL DO BRASIL. **Comunicado nº 31.379, de 16 de novembro de 2017**.

Disponível em: <http://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017>. Acesso em: 27 ago. 2021.

BEZERRIL, Kellia de Oliveira. **Problemas socioambientais:** urbanização desordenada e consequências para a qualidade das águas subterrâneas de poços localizados nas imediações do lixão de cidade nova em Natal/RN. 2016. 206 f. Dissertação (Mestrado) - Curso de Geografia, Universidade Federal do Rio Grande do Norte, Natal, 2016.

BRAGA, Alexandre Melo; MARINO, Fernando C. Herédia; SANTOS, Robson Romano dos. Segurança de Aplicações Blockchain Além das Criptomoedas. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 17., 2017, Brasília. **Anais...** Brasília: Sociedade Brasileira de Computação-Sbc, 2017. p. 99-148.

BRASIL. Lei Federal nº 9.069, de 29 de junho de 1995. **Dispõe sobre o Plano Real, o Sistema Monetário Nacional, estabelece as regras e condições de emissão do REAL e os critérios para conversão das obrigações para o REAL, e dá outras providências.**

BRASIL. Lei Federal nº 12.305, de 02 de agosto de 2010. **Institui a Política Nacional de Resíduos Sólidos; altera a Lei no 9.605, de 12 de fevereiro de 1998; e dá outras providências.**

BRASIL. Medida Provisória Nº 542, de 30 de junho de 1994. **Dispõe sobre o Plano Real, o Sistema Monetário Nacional, estabelece as regras e condições de emissão do Real e os critérios para conversão das obrigações para o Real, e dá outras providências.**

EUROPEAN CENTRAL BANK. **Virtual currency schemes:** October 2012. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Acesso em: 27 ago. 2021.

FERREIRA, Juliandson Estanislau; PINTO, Filipe Gutemberg Costa; SANTOS, Simone Cristiane dos. Estudo de Mapeamento Sistemático sobre as Tendências e Desafios do Blockchain. **Gestão.org**, [s.l.], v. 15, n. , p.108-117, 31 dez. 2017. ANPAD. <http://dx.doi.org/10.21714/1679-18272017v15ed.p108-117>.

GALLO, Zildo. **Ethos, a grande morada humana:** economia, ecologia e ética. Itu: Ottoni, 2007.

LIMA, Thaisi Leal Mesquita de; LIMA, Gabriel Maciel de. **Os megaeventos esportivos no contexto das smart cities, Olimpíadas Rio 2016: o caso Porto Maravilha.** In: GUIMARÃES, Patrícia Borba Vilar et al (Org.). **Direito ao Desenvolvimento Sustentável:** Efetividade de políticas públicas e jogos olímpicos no Brasil. Natal: Max Limonad, 2017. p. 31-46.

MOUGAYAR, William. **Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet**. Rio de Janeiro: Alta Books Editora, 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Banco Mundial estima que 4 milhões de latino-americanos vivem do lixo reciclado**. Disponível em: <https://nacoesunidas.org/banco-mundial-estima-que-4-milhoes-de-latino-americanos-vivem-do-lixo-reciclado/>. Acesso em: 27 ago. 2021.

ROSA, Natalie. **Startup Ecochain lança criptomoeda para reduzir descartes e complementar renda**. Disponível em: <https://canaltech.com.br/criptomoedas/startup-ecochain-lanca-criptomoeda-para-reduzir-descartes-e-complementar-renda-128905/>. Acesso em: 27 ago. 2021.

SANTA CRUZ DA ESPERANÇA/SP. Lei Municipal 424, de 20 de abril de 2017. **Cria o Programa “Cidade Limpa” no Município de Santa Cruz da Esperança, Estado de São Paulo, conforme especifica**.

SOARES, Claudia Lucia Bisaggio. **Moeda social: uma análise interdisciplinar de suas potencialidades no brasil contemporâneo**. 2006. 252 f. Tese (Doutorado) - Curso de Ciências Humanas, Universidade Federal de Santa Catarina, Florianópolis, 2006.

SOUZA, Ranidson Gleyck Amâncio. Território das criptomoedas: limites à regulação estatal quanto à circulação de moedas no ciberespaço e possíveis alternativas. **Revista Brasileira de Políticas Públicas**, [s.l.], v. 7, n. 3, p.61-78, 6 fev. 2018. Centro de Ensino Unificado de Brasília. <http://dx.doi.org/10.5102/rbpp.v7i3.4902>.

TIINSIDE. **Santa Cruz da Esperança adota blockchain para desenvolvimento social**. Disponível em: <https://tiinside.com.br/17/05/2018/santa-cruz-da-esperanca-adota-blockchain-para-desenvolvimento-social/>. Acesso em: 27 ago. 2021.

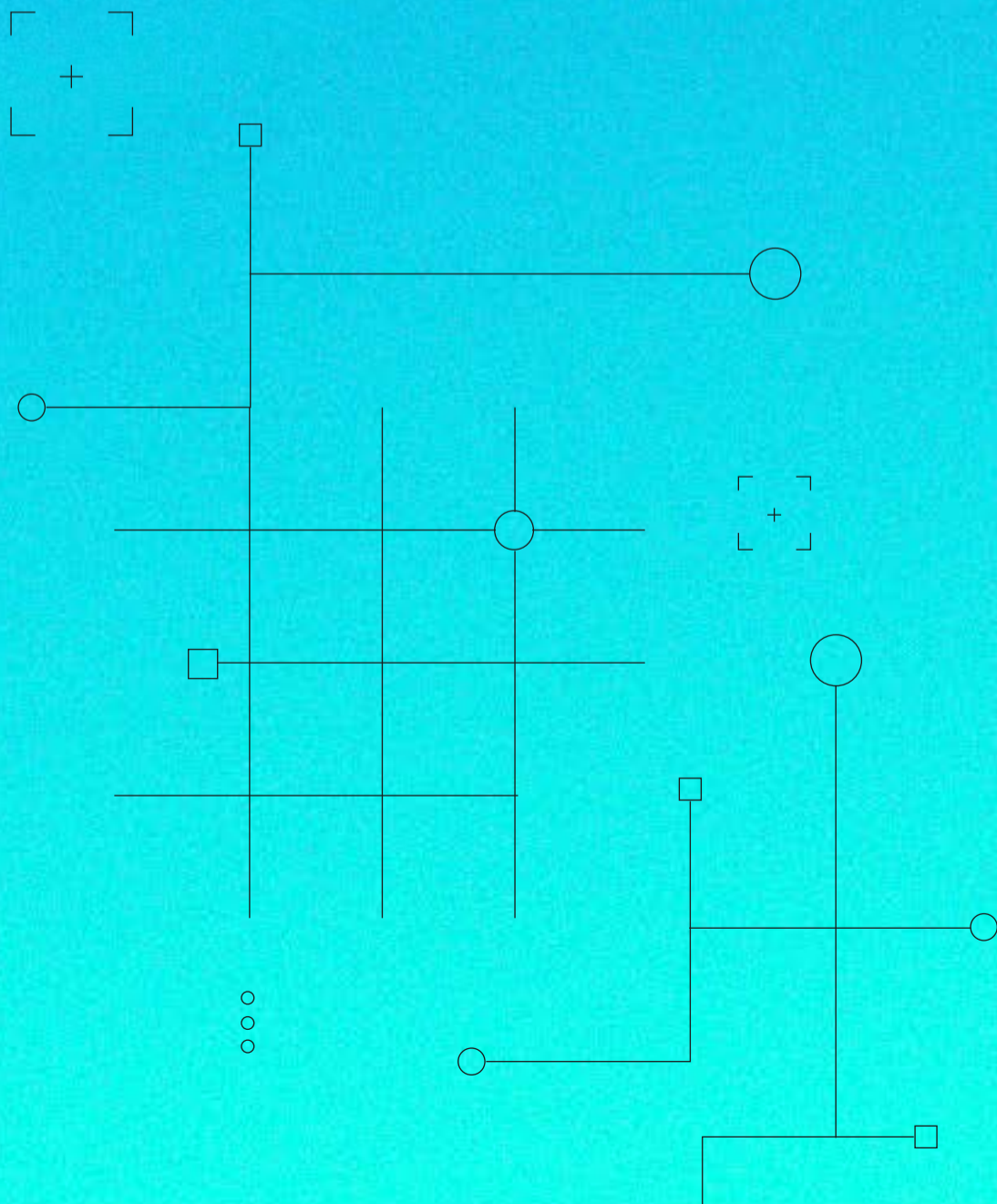
WWF-BRASIL. **Brasil é o 4º país do mundo que mais gera lixo plástico**. Disponível em: <https://www.wwf.org.br/?70222/Brasil-e-o-4-pais-do-mundo-que-mais-gera-lixo-plastico>. Acesso em: 27 ago. 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DÍGITAL

13

Regulação e inovação na administração pública: a criação de uma startup na Prefeitura do Rio

FÁBIO PIMENTEL DE CARVALHO



Sumário: Introdução. 1. O contexto político, social e econômico à época do desenvolvimento do projeto. 2. A criação da startup e da solução tecnológica. Considerações finais. Referências.

Introdução

Os impactos da regulação na inovação são objeto de diversos estudos, especialmente sobre seus efeitos na atividade inovadora do setor privado. No entanto, poucos trabalhos têm se dedicado a investigar os impactos da regulação na inovação no âmbito do setor público, notadamente no contexto dos municípios, muito embora sejam as cidades instituições cada vez mais importantes na organização político-social da atualidade.

A emergência de atividades econômicas suportadas pela tecnologia de plataformas de intermediação tem provocado significativos impactos sociais e sua investigação é objeto de vasto interesse da literatura científica (Sainaghi & Baggio, 2020).

No contexto destas novas tecnologias, ganha relevo o estudo daquelas dedicadas à intermediação do serviço de transporte privado de passageiros, como a Uber, a Lyft, a Cabify, dentre outras (Skok & Baker, 2019). A sua ampla difusão tem sido impulsionada por características estratégicas, como a redução de barreiras à entrada, a redução dos custos de corrida e a praticidade na contratação (Flores & Rayle, 2017). Adicionalmente, estes serviços têm provocado profundos impactos sociais e econômicos mundo afora (Zwick & Spicer, 2018; Chee, 2018; Leiren & Aarhaug, 2016), como a queda no volume de vendas de veículos, como sugerem Guo & Li (2020).

Integrantes de um fenômeno econômico – a *sharing economy* (Guo *et al.*, 2019) – em que, muitas vezes, fornecedores e prestadores de serviço podem trocar de papéis mutuamente (Tafreshian & Masoud, 2020), este modelo inovador provocou impacto imediato na indústria de táxis. Tal efeito, portanto, pode ser verificado através da variação dos preços das licenças (Teo *et al.*, 2019), da redução do número de corridas frente às novas modalidades e até mesmo do aumento do número de queixas contra os serviços de táxi (Willis. & Tanos. 2020).

1. Advogado. Bacharel em direito, Especialista em Propriedade Intelectual pela PUC-Rio e em Direito e Informática pela Universidade do Minho. Mestre em Economia e Gestão da Inovação pela Faculdade de Economia da Universidade do Porto. Ex-Trainee da Diretoria-Geral da Concorrência na Comissão Europeia. Global Data Protection project Manager na Sodexo S/A (Paris) e sócio em Pimentel Aniceto Advogados.

O Estado, cujo papel na economia é frequentemente visto como algo que deva ser limitado (Mazzucato, 2014), não está imune ao surgimento destes novos modelos. Para os Governos, emerge o enorme desafio de disciplinar o funcionamento das plataformas privadas, equilibrando interesses e expectativas de todos os agentes envolvidos (Connoly, 2020).

Disciplinar o funcionamento desses novos negócios é tarefa que afeta a administração pública de maneira geral, mas que pode igualmente produzir efeitos particulares no âmbito municipal, em especial no que diz respeito à inovação. Afinal, muito embora boa parte da atividade regulatória se dê em contexto federal, as atividades que são objeto da regulação se desenvolvem em âmbito da administração local.

O presente artigo realizou um estudo de caso do programa Táxi.Rio, indicando que, motivada pelo processo regulatório dos aplicativos privados de transporte no país, a Prefeitura do Rio de Janeiro decidiu promover uma reforma inovadora na gestão do serviço de táxis, a partir da criação de uma startup dentro do governo, que permitiu a introdução de uma plataforma tecnológica pioneira no país.

1. O contexto político, social e econômico à época da criação da startup

Dados do último censo populacional da Organização das Nações Unidas dão conta de que até 2050, dois terços da população do planeta estará nas cidades (ONU, 2018). No Brasil, de acordo com o Instituto Brasileiro de Geografia e Estatística, em 2015, 84,7% dos habitantes já viviam em áreas urbanas, sendo certo, ainda, que na região Sudeste, onde está o Rio de Janeiro, essa estimativa já ultrapassava os 93% da população. Esta conjuntura de adensamento populacional urbano, aliada ao desenvolvimento de tecnologias móveis, acabou contribuindo substancialmente para que o país se tornasse uma referência na difusão de modelos de *e-hailing* como o da Uber (Audouin & Neves, 2018). Sendo atualmente um dos maiores mercados mundiais da Uber, empresa que responde por cerca de quinze milhões de corridas diárias no mundo, a operação brasileira, presente em aproximadamente quinhentas cidades, reúne quinhentos mil motoristas e mais de vinte milhões de usuários (Insardi & Lorenzo, 2019).

O Rio de Janeiro, maior destino turístico do Hemisfério Sul, conta com uma população de 6,7 milhões de habitantes, acomodados em 160 bairros distribuídos em território continental e insular. Sendo um grande centro urbano, o

Rio é terra fértil para o aporte de novos modelos de negócio, como aqueles em que uma plataforma de intermediação desempenha papel central na organização do arranjo produtivo. Dentre elas, destacam-se as de transporte individual privado de passageiros, como a Uber, que iniciou suas operações na cidade durante a Copa do Mundo 2014, obedecendo à uma lógica de entrada nos mercados estabelecida a partir da observância de dois elementos nodais: o potencial de receita e o cenário regulatório (Swofford, 2020), que consistia basicamente na ausência de regulamentação específica para o serviço de transporte individual privado de passageiros, em detrimento de um conjunto regulatório bastante denso para o serviço prestado por taxistas. À época, sua chegada provocou uma enorme reação negativa por parte dos taxistas; pressionado, o Legislativo local que acabou por editar de uma lei municipal², em 2015, que proibiu a atividade das aplicações (Elizardo, 2015). Em resposta, as empresas de aplicações deflagraram uma guerra nos tribunais, manejando diversos processos cujas decisões judiciais³ suspenderam liminarmente os efeitos da lei ora referida, permitindo, portanto, a manutenção de suas atividades, bem como sua conseqüente expansão.

A entrada das plataformas de mobilidade no mercado escancarou o “súbito” anacronismo do modelo de negócios dos táxis. Sendo o táxi um serviço de utilidade pública de transporte individual de passageiros por natureza e tendo esta atividade a regulação de responsabilidade das prefeituras no Brasil, que concedem licenças e autorizam taxistas a trabalharem, é natural pensar que estes entes da Federação tenham papel central nestas questões, muito embora seja notório também que o aporte destas plataformas provocou amplos e intensos debates nos Três Poderes da República no Brasil.

Em linhas gerais, pode-se dividir o processo regulatório da atividade econômica do transporte intermediado por plataformas em seis fases. Como já mencionado num primeiro momento, a partir do início das operações das plataformas, intensos embates envolvendo motoristas privados, taxistas e autoridades públicas tomaram conta do cenário nacional. A reação média dos agentes públicos, naquela altura, foi refutar a ordem da atividade recém estabelecida e, em claro movimento que pretensamente buscava proteger a atividade dos

2. _Lei Complementar nº 159, de 29/9/2015.

3. _Por exemplo, o processo nº 0406585-73.2015.8.19.0001, do Tribunal de Justiça do Estado do Rio de Janeiro, em que foi proferida decisão, no dia 8/10/2015, determinando que as autoridades se abstivessem de adotar qualquer medida que restringisse ou inviabilizasse o exercício da atividade econômica das plataformas.

taxistas de congêneres alegadamente ilegal, exararam inúmeros expedientes normativos – essencialmente leis e decretos municipais – restringindo ou até mesmo proibindo o serviço de transporte intermediado por plataformas digitais.

Posteriormente, em reação à esta tendência, as empresas detentoras de plataformas propuseram diversas ações judiciais buscando a suspensão liminar dos efeitos daqueles atos normativos, com a consequente garantia da manutenção das atividades até que houvesse pronunciamento judicial definitivo. O sucesso dessa estratégia foi crucial para que a permanência e expansão do negócio das plataformas fosse assegurada até a formação de um arcabouço legislativo e regulatório.

Em 15 de junho de 2016 iniciou-se na Câmara dos Deputados a tramitação do Projeto de Lei (PL) nº 5587/2016. A primeira versão deste texto tinha um viés duramente restritivo à operação das plataformas, buscando aproximar o novo setor das regras então já praticadas em relação ao serviço de táxis. A Uber, por exemplo, engendrou uma vultuosa campanha contra a primeira versão do PL, que apelidou de “Lei do Retrocesso”⁴. A movimentação das plataformas privadas, aliada à pressão popular, acabaram por ocasionar diversas emendas ao texto original, que alteravam substancialmente o conteúdo do projeto. Após quase dois anos de intensos debates no Congresso Nacional, foi promulgada a Lei nº 13.640/2018, um substitutivo do PL original extremamente modificado em sua essência e que, na verdade, regulamentava a atividade de forma praticamente oposta à ideia original, tornando-se flexível o suficiente para adequar o poder normativo à realidade já então consolidada, a partir de uma premissa geral de não-proibição e entregando exclusivamente aos Municípios e ao Distrito Federal a competência para regulamentar e fiscalizar a atividade do transporte remunerado individual privado de passageiros, categoria dentro da qual o legislador inseriu a atividade intermediada pelas plataformas.

Logo após a entrada em vigor da Lei 13.640/2018, teve início um movimento de regulamentação em âmbito municipal, à exemplo do que ocorreu em outros países, como a China (Zhang, 2019), oportunidade em que diversas cidades editaram normas para disciplinar o exercício da atividade de transporte intermediado por plataformas eletrônica, à luz da autorização conferida pela por aquele diploma federal, tais como o Rio de Janeiro, a partir do Decreto nº

4. Disponível em <https://www.uber.com/us/en/lei-do-retrocesso/>, acessado em 12/12/2021.

44.339 de abril de 2018. Nesta altura, a cidade possuía cerca de 150 motoristas de aplicações (Magalhães, 2018), número que cresceu para 188 mil em 2019 (IBGE, 2019).

Meses depois, em julgamento histórico, iniciado em dezembro de 2018 e concluído em maio de 2019, o Supremo Tribunal Federal considerou inválidas leis locais de cidades brasileiras que proibiam ou regulavam restritivamente a atividade das plataformas, fixando a tese de que a proibição ou restrição da atividade das aplicações de mobilidade é inconstitucional, cabendo aos governos municipais apenas a regulamentação da atividade, observando-se os limites impostos na legislação federal⁵. Considerando que as operações da Uber no Brasil iniciaram-se em 2014 e tendo em vista, ainda, que segundo dados do Conselho Nacional de Justiça⁶, uma ação judicial leva em média 1,9 ano para ser sentenciada, isto é, para receber a primeira decisão de mérito em grau ordinário, salta aos olhos a celeridade com que o tema em comento percorreu todas as instâncias do Poder Judiciário, o que apenas torna mais evidente seu contorno social extremamente relevante.

Atualmente, diversas cidades brasileiras possuem marcos regulatórios próprios, ou seja, há potencial para que coexistam, no Brasil, 5.570 regulações diferentes, o que, por si só, já pode representar um óbice à regulação em si. Além disso, em linhas gerais, dois pontos parecem ser especialmente complexos: a fiscalização da prestação do serviço em si, que torna-se praticamente inviável sem que haja limitação objetiva quanto ao número de agentes no mercado – que foi justamente o que restou decidido pelo Supremo Tribunal Federal – e o entendimento jurisprudencial que vem se formando nos tribunais brasileiros⁷, no sentido de que as plataformas não estão obrigadas a pagarem pelo uso intensivo do sistema viário urbano das cidades. Isto é, decisões judiciais mais recentes estão transformando estes agentes económicos em verdadeiros *free riders*, engendrando a chamada *tragédia dos comuns*.

No Rio de Janeiro, como já mencionado, o legislativo municipal editou leis, o Executivo decretos e o Judiciário proferiu também diversas decisões sobre o

5. _Julgamento do Recurso Extraordinário nº 1.054.110/SP, Relatoria do Min. Roberto Barroso, ocorrido em 5 de maio de 2019.

6. _Disponível em <https://www.cnj.jus.br/pesquisas-judiciarias/justica-em-numeros/>, acessado em 10/12/2021.

7. _Nos autos do Recurso Especial nº 1.789.233, o Ministro Og Fernandes, do Superior Tribunal de Justiça, negou seguimento a recurso do Distrito Federal contra acórdão do Tribunal de Justiça do Distrito Federal, que considerou ilegal a cobrança de preço público pelo uso normal de bem público comum, quando não há individualização do bem utilizado nem restrição ao acesso da coletividade.

tema. Nesse sentido, porém, foi notório que todos esses expedientes normativos não foram capazes de harmonizar as relações sociais.

Os episódios de violência entre ambas as categorias se tornaram assunto recorrente na imprensa⁸, agravando, dia após dia, o conflito. Greves seguiram-se de parte a parte, causando enormes transtornos para o trânsito da cidade⁹. Noutro giro, sabe-se ainda que a redução do custo das viagens realizadas por transporte individual, uma realidade trazida pelas plataformas privadas de intermediação, fez com que fosse estabelecido certo fluxo migratório de passageiros dos transportes coletivos, de massa, para a nova modalidade, provocando impactos na mobilidade urbana (Silva *et al.*, 2019). Além disso, a profissionalização da atividade de motoristas de plataformas, antes condutores eventuais, catalisou o conflito entre esses e os taxistas.

É importante destacar que em 2017, momento em que o projeto de lei (PL) anteriormente referido estava sendo debatido no legislativo federal, havia um forte indicativo de que a legalidade da atividade intermediada por empresas como a Uber seria reconhecida e, portanto, regulada. Foi nesse contexto de mudança do escopo original do PL nº 5587/2016 para um então possível cenário de legalização daquela atividade econômica que a Prefeitura do Rio de Janeiro anunciou uma profunda remodelação do serviço de táxis na cidade. Esta remodelação se daria a partir do desenvolvimento de uma plataforma de mobilidade urbana, semelhante às aplicações privadas já existentes e pioneira na administração brasileira, de maneira a modernizar o serviço de utilidade pública prestado pelos taxistas, bem como sua gestão pela própria prefeitura (Ouchana & Schmidt, 2017), denominada Táxi.Rio.

2. A criação da startup e da solução tecnológica

Em 29 de maio de 2017, o Prefeito da Cidade do Rio de Janeiro editou o Decreto nº 43.256, que declarou o táxi patrimônio imaterial da cidade¹⁰, fazendo incidir, portanto, especial atenção sobre a atividade. Na mesma oportuni-

8. _Como a notícia disponível em <https://www.tecmundo.com.br/uber/112230-taxistas-depredam-area-reservadauber-aeroporto-do-rio-janeiro.htm>, acessado em 12/12/2021.

9. _Como noticiou o Estadão, disponível em <https://brasil.estadao.com.br/noticias/geral,taxistas-travam-ruas-do-rioem-protesto-contr-uber,10000024225>, acessado em 12/12/2021.

10. _Inteiro teor do ato normativo encontra-se disponível em <https://leismunicipais.com.br/a1/rj/r/rio-de-janeiro/decreto/2017/4326/43256/decreto-n-43256-2017-declara-patrimonio-cultural-carioca-o-taxi-comumamarelo-e-azul-na-cidade-do-rio-de-janeiro>, acessado em 14/12/2021.

de, foi anunciada a criação da plataforma de intermediação de serviços de transporte individual, pública, operada por táxis, batizada de Táxi.Rio¹¹. O desafio de desenvolver um serviço absolutamente distinto dos serviços públicos tradicionais acabou por demandar uma significativa reformulação no modelo de trabalho no governo municipal. À época, o órgão designado para liderar a iniciativa foi Empresa Municipal de Informática (IPLANRIO), responsável pela gestão dos recursos de tecnologia da prefeitura. Na página de divulgação da iniciativa, www.taxi.rio, desde o dia do anúncio do projeto, uma ferramenta permitia à população em geral – inclusive taxistas – que contribuísse com a modelagem do serviço, propondo ideias¹², com o objetivo de que a solução pudesse já desde a concepção ter razoável aderência ao mercado, reduzindo, ainda, as chances de retrabalho, na medida em que os recursos – públicos – eram escassos. A pergunta central lançada era: “O que você acha que pode melhorar no serviço de táxi do Rio de Janeiro?”. Até julho de 2017, mais de 2,5 mil pessoas já haviam participado desta iniciativa e suas sugestões foram agrupadas em um conjunto de duzentas ideias.

A participação popular na construção do novo modelo foi fundamental para definir os eixos centrais do programa, notadamente porque os utilizadores são agentes fundamentais no processo de inovação (Von Hippel *et al.*, 2011). Estes eixos foram utilizados para balizar o desenvolvimento do projeto e eventualmente corrigir falhas de mercado a partir do uso da tecnologia. Como exemplos, podem-se citar: (i) a modernização do sistema de contratação (*rail hiding*) do transporte; (ii) transparência e previsibilidade, a partir da oferta antecipada e não vinculativa para o passageiro, de informações como custo da viagem, tempo estimado até a chegada do motorista e até o destino pretendido, além da identificação adequada do condutor; (iii) flexibilização da tarifa, respeitado limitado máximo estabelecido pela regulamentação municipal, de forma a permitir a concessão de descontos pelos condutores; (iv) distribuição mais uniforme da frota e integração com outros modais de transporte, (v) produção de massa de dados nunca antes obtida na história do serviço, para análises e incrementos nas políticas de engenharia de tráfego e mobilidade urbana¹³,

11. _Como amplamente divulgado pela imprensa, por exemplo em <https://g1.globo.com/rio-dejaneiro/noticia/crivella-da-mais-detalle-sobre-app-e-torna-taxistas-patrimonio-cultural-do-rio.ghtml> e <https://noticias.r7.com/rio-de-janeiro/crivella-torna-taxi-patrimonio-cultural-da-cidade-e-lanca-aplicativo-taxirio29052017> acessados em 12/12/2021.

12. _Disponível em <http://www.rio.rj.gov.br/web/taxirio/noticias?id=7442134>, acessado em 13/12/2021.

13. _Neste sentido, em 22 de agosto de 2018, foi editado o Decreto nº 44.932, que criou grupo de trabalho para elaboração

como, por exemplo, tempo tripulado *versus* tempo ocioso, distâncias percorridas, faturamento médio, para fins de fixação de uma tarifa justa e embasada; (vi) maximização da atuação do taxista como parceiro do governo municipal, a partir da troca constante de informações em tempo real; (vii) utilização do serviço de táxis, em modelo corporativo, pelo governo municipal, em substituição à locação de veículos ou manutenção de frota própria, com vistas a otimizar os recursos públicos; (viii) fiscalização mais efetiva do serviço prestado, na medida em que, munido das informações e meios adequados, o passageiro consegue fornecer *feedback* preciso de cada viagem contratada; (ix) otimização do tráfego, com a redução dos deslocamentos não-tripulados, redução dos tempos de embarque, com o despacho da corrida para o motorista que se encontre mais próximo do passageiro e redução do tempo de desembarque, com a utilização de meios de pagamento automatizados; (x) mobilização da frota de táxis para atendimento a situações de risco civil, como eventos climáticos, além de crises de desabastecimento, greves, dentre outros, além do direcionamento desta para cobertura de grandes eventos, como Rock in Rio, partidas de futebol, etc; (xi) desenvolvimento de programas de capacitação e incentivo para os condutores; (xii) ampliação da segurança do transporte, tendo em vista que todas as viagens são monitoradas pela prefeitura, podendo-se, inclusive, aferir se um condutor excedeu o limite de velocidade, por exemplo.

A construção participativa do projeto – congregando população, taxistas, passageiros, agentes públicos de diversas áreas e demais *stakeholders*, conjugada com a utilização de técnicas de gestão de projetos, de desenvolvimento ágil e da percepção voltada à modelagem a partir da impressão de quem toma o serviço (*user experience*), representou verdadeiro esforço de inovação no processo criativo no setor público no Rio de Janeiro. Essa nova metodologia de trabalho acabou por reformular também o modo como a administração, notadamente a Empresa Municipal de Informática (IPLANRIO)”. Merece registro, nesse particular, que a Fundação João Goulart, estrutura municipal responsável pela capacitação e aprimoramento de servidores públicos municipais, foi agraciada com o Prêmio Ser Humano 2019, concedido pela Associação Brasileira de Recursos Humanos (ABRH), justamente pela prática denominada GTTs – Grupos transversais de trabalho, que consistem exatamente na organi-

de estudos de políticas de mobilidade urbana, a partir dos dados gerados pela operação da plataforma Táxi.Rio, conforme <https://leismunicipais.com.br/a1/rj/r/rio-de-janeiro/decreto/2018/4493/44932/decreto-n44932-2018-cria-grupo-de-trabalho-para-elaboracao-de-estudos-que-embasem-politicas-publicas-de-mobilidadeurbana-utilizando-os-dados-gerados-pela-plataforma-taxi-rio?r=p>, acessado em 8/12/2021.

zação sistemática do trabalho de elaboração de políticas públicas a partir da união de esforços de equipas multidisciplinares de agentes públicos e demais *stakeholders* dos diversos temas¹⁴, que utilizam-se de processos e times enxutos.

Após o começo do período de desenvolvimento da aplicação em si, tiveram início, em junho de 2017, os testes de funcionamento da primeira versão. Cerca de 150 taxistas voluntários e 300 passageiros, servidores públicos da prefeitura, participaram dessa etapa, que incluía não só a utilização em si da aplicação, mas também sessões de *brainstorming* e dinâmicas coletivas. Em agosto de 2017 foi encerrada a fase de testes e, a partir do *feedback* dos testadores, foram implementadas melhorias na ferramenta.

Em 1º de novembro de 2017 foi realizada a primeira viagem de táxi intermediada pela aplicação, feita pelo autarca entre sua residência e a sede do governo municipal.¹⁵ Dos pilares que compunham a estrutura do projeto emergiram diversas iniciativas, sendo as de maior relevo aquelas que se passa a detalhar abaixo:

Meritocracia e elemento coercitivo: taxistas mais bem avaliados pelos passageiros são autorizados a operarem, em regime de exclusividade, na cobertura de grandes eventos, como os desfiles de Carnaval no sambódromo, o Rock in Rio, dentre outros. Isso estimula que condutores se esmerem para, no dia a dia, prestarem um serviço de qualidade, de maneira que sejam bem avaliados e possam aceder a estes megaeventos. Trata-se, portanto, da inversão de um círculo vicioso de má prestação de serviços em um círculo virtuoso. Ademais, importa também destacar aqui também que a adesão dos taxistas ao novo serviço foi absolutamente facultativa, contrariando assim a lógica de coercitividade embutida na ideia de alteração de comportamentos que deve permear as políticas públicas. Nesse caso em especial, dada a necessidade premente de adequação do serviço às novas premissas e instrumentos tecnológicos existentes, a coerção deu-se preponderantemente de maneira mitigada; os próprios motoristas sentiram-se “obrigados” a aderirem ao uso da aplicação, a despeito da prefeitura jamais ter imposto a adesão, facultativa até os dias atuais, inclusive, seja para incluírem-se digitalmente e participarem

14. Conforme noticiado em <https://odia.ig.com.br/colunas/servidor/2019/11/5829177-fundacao-joao-goulartganha-premio-de-gestao-publica.html>, acessado em 12/12/2021.

15. Conforme noticiado em <https://extra.globo.com/noticias/economia/crivella-vai-trabalhar-de-taxirio-mas-recusadesconto-paga-78-pela-corrada-22018693.html>, acessado em 13/12/2021.

de uma fatia do mercado da qual estavam alijados, seja para, a partir do regime meritocrático, poderem trabalhar nos megaeventos, que são também, por óbvio, grandes polos geradores de viagem. Assim, a coercitividade de forma explícita pôde ser identificada unicamente em casos de mau comportamento, quando os taxistas podem ser suspensos e até mesmo banidos da plataforma.

Módulo “Taxista informa”: a partir da criação deste módulo, o serviço de táxis integrou-se à gestão da cidade. Taxistas passaram a operar como agentes da prefeitura, reportando, em tempo real, a partir do georreferenciamento de suas aplicações, ocorrências como semáforos danificados, crimes, buracos nas vias, falhas de iluminação pública e outras situações de zeladoria do espaço urbano.¹⁶ Esta contraprestação colaborativa foi considerada pelo então prefeito a remuneração da classe pela disponibilização da plataforma, inclusive.

Construção de um conjunto de parcerias para capacitação profissional dos taxistas: foram estabelecidas parcerias com escolas técnicas que oferecem cursos de treinamento para uso de tecnologias móveis, inglês para turistas e relações interpessoais, por exemplo. Como forma de prestigiar os concluintes desses cursos, todos são também convidados a participarem da cobertura dos grandes eventos da cidade. Ainda, foram estabelecidas outras parcerias, como por exemplo a realizada com a Caixa Econômica Federal, para abertura de contas, concessão de crédito em condições especiais e até mesmo educação financeira, na medida em que a renovação da frota, obrigatória por lei, representava outro círculo vicioso no sistema, tendo em conta a dificuldade dos taxistas em organizarem-se economicamente e obterem os rendimentos necessários para isso.

Espaço Táxi.Rio: Em 18 de janeiro de 2018, foi inaugurado¹⁷ um espaço dedicado ao atendimento presencial de condutores e passageiros, localizado na entrada da sede do governo municipal. Neste espaço, usuários podem, por exemplo, receber instruções de como utilizar a aplicação pública, bem como solucionar questões de qualquer ordem relativas ao serviço.

16. _Como noticiado em <https://g1.globo.com/rio-de-janeiro/noticia/crivella-da-mais-detalle-sobre-app-e-tornataxistas-patrimonio-cultural-do-rio.ghtml>, acessado em 13/12/2021.

17. _Como referido em <https://noticias.r7.com/rio-de-janeiro/rj-no-ar/videos/crivella-inaugura-espaco-taxirio-nestaquinta-feira-18-18012018>, acessado em 13/12/2021.

Módulo Corporativo¹⁸: A introdução deste módulo¹⁹ passou a permitir a substituição gradual da frota própria e locada da Câmara pelo uso do táxi para transporte de servidores públicos. Assim, ao invés de incorrer nos altos custos de manutenção de frota, bem como em contratos para aluguer de viaturas, a administração municipal passou a ter a possibilidade pagar apenas pelos quilômetros efetivamente percorridos, tendo à sua disposição milhares de carros distribuídos pela cidade. O funcionamento é simples: devidamente autenticado, o funcionário público pode, a partir de seu telefone, solicitar uma corrida. Não obstante a economia em si, a transparência também foi aprimorada, já que todos os trajetos são devidamente registrados.

Módulo de transporte sanitário: Este módulo foi especialmente pensado para atender a uma necessidade específica dos pacientes da rede municipal de saúde que fazem tratamos como o de hemodiálise, isto é, precisam de transporte para chegarem à unidade hospitalar, mas não necessariamente em ambulâncias.

Comunicação *real time* com o Centro de Operações Rio (COR): O COR foi o primeiro equipamento olímpico a ficar pronto, tendo sido inaugurado pela cidade em 2010. Conta com mais de mil câmaras distribuídas pela cidade, além de reunir, num mesmo ambiente, representantes das forças armadas, policiais, bombeiros, defesa civil e concessionários de serviços públicos, permitindo uma atuação conjunta em resposta aos eventos e crises da operação da cidade. Taxistas e passageiros recebem mensagens *push* em tempo real, informando sobre eventos que podem impactar em suas rotinas, como chuvas, fechamento de vias etc. Além disso, o COR é capaz de monitorar o posicionamento geográfico de cada táxi que esteja operando na plataforma, podendo, inclusive, entrar em contato com o taxista para confirmar ocorrências ou mesmo solicitar apoio em caso de emergência.

Criação de logomarca próprios e conjunto de iniciativas de divulgação do projeto: Mesmo que de natureza pública, era necessário promover a divulgação do novo serviço à população. Uma logomarca, inspirada no famoso Pão de Açúcar e nos *bigorilhas*, assim chamados os sinais luminosos que estão nos tetos dos táxis a indicar se estão livres ou não, foi desenvolvida e estampada

18. Regulamentado através do Decreto nº 45.716/2018, disponível em http://smaonline.rio.rj.gov.br/legis_consulta/58026Dec%2045716_2019.pdf, acessado em 13/12/2021.

19. Conforme noticiado em <https://diariodotransporte.com.br/2019/03/18/decreto-de-crivella-determina-queservidores-da-prefeitura-deverao-usar-app-taxi-rio-corporativo-em-seus-deslocamentos/>, acessado em 13/12/2021.

na lataria dos veículos. Deve-se destacar, nesse sentido, a identificação de um forte movimento, por parte dos próprios taxistas, para fortalecer e divulgar esta marca. Nas redes sociais, é possível identificar, através da pesquisa com a *hashtag* #taxi.rio, centenas de manifestações espontâneas de publicidade, além de perfis e materiais como camisolas, talões de recibos, capas para o estofado dos carros, dentre outros produtos²⁰. Há, inclusive, um grupo organizado intitulado “equipe de mkt Taxi.Rio”, que organiza *crowdfundings* para arrecadar recursos revertidos para a publicidade do serviço.

Outros relevantes reflexos da implantação do Táxi.Rio foram observados tanto no Legislativo municipal, como até mesmo perante o Conselho Administrativo de Defesa Econômica (CADE) e, ainda, no âmbito da cooperação entre o Rio de Janeiro e outras cidades, o que acabou por revelar outra característica fundamental das startups: a existência de um modelo de negócio repetível e escalável.

No que se refere ao Legislativo, uma série de projetos de lei seguiram-se à implantação do projeto. A Tabela 1 sintetiza os projetos de lei já aprovados.

Tabela 1. Principais iniciativas legislativas relacionadas ao Táxi.Rio.

Fonte: Autoria própria.

Data da proposição	Nº Projeto de Lei	Autor	Objeto	Situação em 7/1/2022
30/08/2018	963/2018	Ver. Jorge Felipe	INSTITUI O TAXI.RIO COMO PLATAFORMA OFICIAL DE ESTÃO DE TÁXIS DO MUNICÍPIO DO RIO DE JANEIRO E DÁ OUTRAS PROVIDÊNCIAS	Aprovado. (Lei municipal nº 6082/2020)
18/09/2018	974/2018	Ver. Leonel Brizola	TOMBA COMO BENS DE NATUREZA IMATERIAL DA CIDADE DO RIO DE JANEIRO O SERVIÇO DE TÁXI AMARELINHO, BEM COMO A PLATAFORMA TAXI.RIO	Aprovado. (Lei municipal nº 6725/2020)

Em relação às questões concorrenciais, tem-se notícia de que a Associação Brasileira Online to Offline (AB2O), que congrega dentre seus associados²¹ a Cabify (à época uma empresa operante no Brasil) e a 99, *players* do mercado

20. _Como exemplos, são <https://www.instagram.com/taxiriorj/>, <https://www.instagram.com/explore/tags/taxirio/>, acessado em 13/12/2021.

21. _Como disponível em <https://o2obrasil.com.br/#associados>, acessado em 13/12/2021.

de plataformas privadas de intermediação de transporte, ofereceu Representação perante o Ministério da Economia contra o programa público TAXI.RIO, alegando, em suma, a prática de concorrência desleal por parte da Prefeitura. Em consequência, o CADE, autoridade da concorrência no Brasil, instaurou inquérito para apurar a acusação, tendo concluído, em 28 de setembro de 2019, pela inexistência de qualquer prática anticoncorrencial²², reconhecendo, portanto, que “(...) a deliberada escolha política pública pelas prefeituras se insere em um contexto mais amplo de regulação”, acrescentando, ainda, que “(...) a elaboração do aplicativo pela prefeitura constitui política pública na medida em que pode endereçar alguns aspectos históricos de falha fiscalizatória no serviço de táxi apontados na Representação e inegavelmente existentes no mercado de transporte de passageiros.”²³

Ainda, reafirmando a capacidade de repetição e escalabilidade do negócio, foram estabelecidos diversos acordos de cooperação entre municípios brasileiros, sendo o destacado aquele que selou a parceria entre Rio de Janeiro e São Paulo, maior cidade do Brasil, lançada na segunda em abril de 2018²⁴. Recentemente, a Prefeitura do Rio anunciou que mais de 30 cidades já se encontram no *roadmap* de crescimento do Táxi.Rio, tais como Maceió, Alagoas²⁵. O projeto completou quatro anos de efetiva operação em 1º de novembro de 2021. Notícias daquele mês dão conta de que o Táxi.Rio realiza, mensalmente, mais de 600 mil viagens²⁶²⁷²⁸. A Tabela 2 sintetiza as principais características de uma startup e os elementos correspondentes identificados no caso em estudo.

22. _Nos termos da decisão contida no Processo nº 08700.006067/2018-18, acessado em 13/12/2021.

23. _Conforme disposto na Nota Técnica nº 15/2019/CGAA4/SGA1/SG/CADE, inserida no processo acima referido, consultado acessado em 3/12/2021.

24. _Como noticiado em <https://g1.globo.com/sp/sao-paulo/noticia/em-tom-de-campanha-doria-lanca-aplicativo-detaxi-em-sao-paulo.ghtml>, acessado em 16/12/2021.

25. _Como noticiado em <https://prefeitura.rio/fazenda/prefeitura-do-rio-sela-parceria-com-maceio-e-leva-taxi-riopara-a-capital-alagoana/>, acessado em 13/12/2021.

26. _Como noticiado em <https://valor.globo.com/brasil/noticia/2021/12/02/tecnologia-da-prefeitura-do-rio-atraiuoutras-cidades.ghtml>, acessado em 13/12/2021.

27. _Como noticiado em <https://www1.folha.uol.com.br/cotidiano/2019/12/em-crise-prefeitura-do-rio-suspendepagamentos.shtml>, acessado em 6/1/2022.

28. _Como se infere do contido em <http://www.rio.rj.gov.br/web/taxirio/noticias?id=10564531>, acessado em 6/1/2022.

Tabela 2. Principais iniciativas legislativas relacionadas ao Táxi.Rio. Fonte: Adaptado de Bruna Puga.

Característica de uma startup	Elementos correspondentes identificados no caso em estudo
Caráter inovador	A iniciativa em si de oferecer, como serviço público, um serviço inicialmente oferecido apenas pelo setor privado é inovadora. Ainda, é correto afirmar que o projeto possui diversas outras vertentes inovadoras, como a própria revisão dos modelos de trabalho dentro da prefeitura, por exemplo.
Processos e times enxutos	O time responsável pelo desenvolvimento do projeto era extremamente enxuto, notadamente porque composto por servidores públicos com anos de experiência na prefeitura. Os processos também precisavam ser o mais enxutos possível, de forma que a implementação do projeto se tornasse viável e sustentável no tempo.
Recursos escassos	A escassez de recursos é inerente à atividade pública. No caso do projeto Táxi.Rio, o momento vivido pela Prefeitura do Rio era tão desafiador que em 2019 todos os pagamentos chegaram a ser suspensos. ²⁶
Modelo de negócio repetível e escalável	O Táxi.Rio foi reproduzido e/ou escalado para atender diversas cidades do país, demonstrando assim a capacidade do modelo de negócio.
Agilidade nas decisões	A centralização da coordenação em um único órgão da prefeitura, que contava com profissionais de diversas áreas do negócio, garantiu que a tomada e execução das decisões fossem céleres o suficiente para
Execução rápida	Entre o anúncio do projeto, em maio, e a primeira viagem, em novembro, transcorreram menos de seis meses de execução, com o emprego de métodos ágeis, como o Scrum. Além disso, uma estrutura com central de atendimento telefônico e suporte 24h/7 garantiu uma entrega ágil.
Foco na validação da solução no mercado	O balizamento do desenvolvimento da solução nas respostas coletadas na enquete realizada, somada às fases de teste demonstram que, desde o princípio, o foco estava na validação da solução no mercado. Em poucos meses o Táxi.Rio alcançou números expressivos de corridas, passageiros e taxistas utilizadores da plataforma. ²⁷
Custo estrutural baixo	O projeto se utilizou da estrutura de tecnologia já existente na Prefeitura, de maneira que o custo extra foi absolutamente residual.

Considerações finais

O presente artigo teve por objetivo analisar a relação entre a atividade regulatória no âmbito federal e a produção de efeitos no contexto da inovação em nível local, a partir da análise do caso Táxi.Rio, desenvolvido pela Prefeitura do Rio de Janeiro no momento em que o Legislativo e Executivo federais regulamentavam as plataformas privadas de transporte, como a Uber.

A observação do contexto histórico sugere a existência de uma relação direta entre a regulação em âmbito federal e a produção de inovação no âmbito local, indicando, portanto, a possibilidade da presença de um Estado inovador como consequência de um Estado regulador.

Para além disso, foi possível identificar também que o modelo proposto e implementado pela prefeitura reúne características que sugerem ter havido, na verdade, a estruturação de uma *startup* dentro do governo municipal.

Nesse sentido, é forçoso concluir que a decisão pela adoção de um modelo de trabalho como esse foi fundamental para que a colocação do serviço público à disposição da sociedade tenha sido possível, notadamente por se tratar de um tipo de serviço – intermediação de viagens – que a população conhecia e utilizava exclusivamente a partir da prestação empreendida pelo setor privado.

O que se conclui, portanto, é que a atividade regulatória do Estado, em sentido amplo, foi capaz de promover inovação com impactos positivos de diversas naturezas na própria administração pública local, inclusive no que diz respeito à gestão do serviço de táxis. Percebeu-se, dessa feita, que é possível e positiva a coexistência dos fenômenos – regulatório e de produção de inovação, ao revés de outros casos semelhantes, onde a regulação resultou na manutenção e reforço do *status quo*, sem qualquer efeito em termos de inovação, como no estudo de Pelzer *et al.* (2019).

Referências

Audouin, M., & Neves, C. (2018). What are the regulations for ICT-based mobility services in urban transportation systems? The cases of ride-booking regulation in São Paulo and Rio De Janeiro. *WIT Transactions on the Built Environment*, 176(March), 95-106. [doi: 10.2495/UT170091](https://doi.org/10.2495/UT170091)

Chee, F. M. (2018). An uber ethical dilemma: Examining the social issues at stake. *Journal of Information, Communication and Ethics in Society*, 16(3), 261-274. [doi: 10.1108/JICES-03-2018-0024](https://doi.org/10.1108/JICES-03-2018-0024)

Connoly, J. M. (2020). No Uber, no tourists? Public attitudes toward municipal regulation of the sharing economy. *Local Government Studies*, 47, 1-16. [doi: 10.1080/03003930.2020.1794844](https://doi.org/10.1080/03003930.2020.1794844)

Elizardo, M. (25 de agosto de 2015). Câmara do Rio aprova lei que prevê multa a motoristas do Uber. *O Globo*. <http://g1.globo.com/rio-de-janeiro/noticia/2015/08/camara-do-rio-aprova-lei-que-prevemulta-motoristas-do-uber.html>, acessado em 30/12/2021.

Flores, O., & Rayle, L. (2017). How cities use regulation for innovation: The case of Uber, Lyft and Sidecar in San Francisco. *Transportation Research Procedia*, 25, 3756-3768. [doi: 10.1016/j.trpro.2017.05.232](https://doi.org/10.1016/j.trpro.2017.05.232)

Guo, Y., Xin, F., & Li, X. (2020). The market impacts of sharing economy entrants: Evidence from USA and china. *Electronic Commerce Research*, 20(3), 629-649. [doi: 10.1007/s10660-018-09328-1](https://doi.org/10.1007/s10660-018-09328-1)

Guo, Y., Li, X., & Zeng, X. (2019). Platform competition in the sharing economy: Understanding how ridehailing services influence new car purchases. *Journal of Management Information Systems*, 36(4), 1043-1070. doi: 10.1080/07421222.2019.1661087

Insardi, A., & Lorenzo, R. O. (2019). Measuring accessibility: A big data perspective on uber service waiting times. *RAE Revista de Administração de Empresas*, 59(6), 402-414. doi: 10.1590/S0034759020190606

Leiren, M. D., & Aarhaug, J. (2016). Taxis and crowd-taxis: Sharing as a private activity and public concern. *Internet Policy Review*, 5(2), 1-17. doi: 10.14763/2016.2.420

Magalhães, L. E. (23 de abril de 2018). Rio tem cerca de 150 mil motoristas credenciados por aplicativos. *O Globo*. <https://oglobo.globo.com/rio/rio-tem-cerca-de-150-mil-motoristas-credenciados-poraplicativos-22584739>, acessado em 5/12/2021.

Mazzucato, M. (2014). *O Estado empreendedor: Desmascarando o mito do setor público vs. setor privado*.

São Paulo: Portfolio-Penguin.

ONU. (2018). *World Urbanization Prospects 2018*. <https://population.un.org/wup/>, acessado em 10/12/2021

Ouchana, G. & Schmidt, S. (2017). Prefeitura lança aplicativo de táxi para município do Rio. *O Globo*.

<https://oglobo.globo.com/rio/prefeitura-lanca-aplicativo-de-taxi-para-municipio-do-rio-1-21407866>, acessado em 11/12/2021.

Pelzer, P., Frenken, K., & Boon, W. (2019). Institutional entrepreneurship in the platform economy: How uber tried (and failed) to change the dutch taxi law. *Environmental Innovation and Societal Transitions*, 33, 1-12. doi: 10.1016/j.eist.2019.02.003

Puga, Bruna. (2021). Contratação de pessoal no âmbito das startups. (Material utilizado no curso de Pósgraduação em Direito Digital da Universidade do Estado do Rio de Janeiro/ITS Rio).

Sainaghi, R., & Baggio, R. (2020). Clusters of topics and research designs in peer-to-peer accommodation platforms. *International Journal of Hospitality Management*, 88, 102393. doi: 10.1016/j.ijhm.2019.102393

Silva, M. A. V., Souza, C. O., Nascimento, F. A. C., Saldanha, L. E. C., Santos, T. F., Carvalho, T. S. (2019): Elaboração e análise de trabalho técnico-ambiental de impacto no tráfego e mobilidade urbana no município, relacionado aos serviços de carona remunerada e táxi: Fundação COOPETEC (Universidade Federal do Rio de Janeiro).

Skok, W., & Baker, S. (2019). Evaluating the impact of uber on London's taxi service: A critical review of the literature. *Knowledge and Process Management*, 26(1), 3-9. doi: 10.1002/kpm.1573

Swofford, J. L. (2020). Uber's early entry decisions in the US. *Applied Economics*, 52(25), 2723-2729. doi: 10.1080/00036846.2019.1694633

Tafreshian, A., & Masoud, N. (2020). Using subsidies to stabilize peer-to-peer ride-sharing markets with role assignment. *Transportation Research Part C*, 120, 102770. doi: [10.1016/j.trc.2020.102770](https://doi.org/10.1016/j.trc.2020.102770)

Teo, T. S. H., Kimes, S. E., & Yong, Z. (2019). The rise and fall of taxi club management in New York. *INFORMS Transactions on Education*, 20(1), 28-32. doi: [10.1287/ited.2019.0207cs](https://doi.org/10.1287/ited.2019.0207cs)

Von Hippel, E., Ogawa, S. e De Jong, J. P. J. (2011): The age of consumer-innovator: MIT Sloan Management Review.

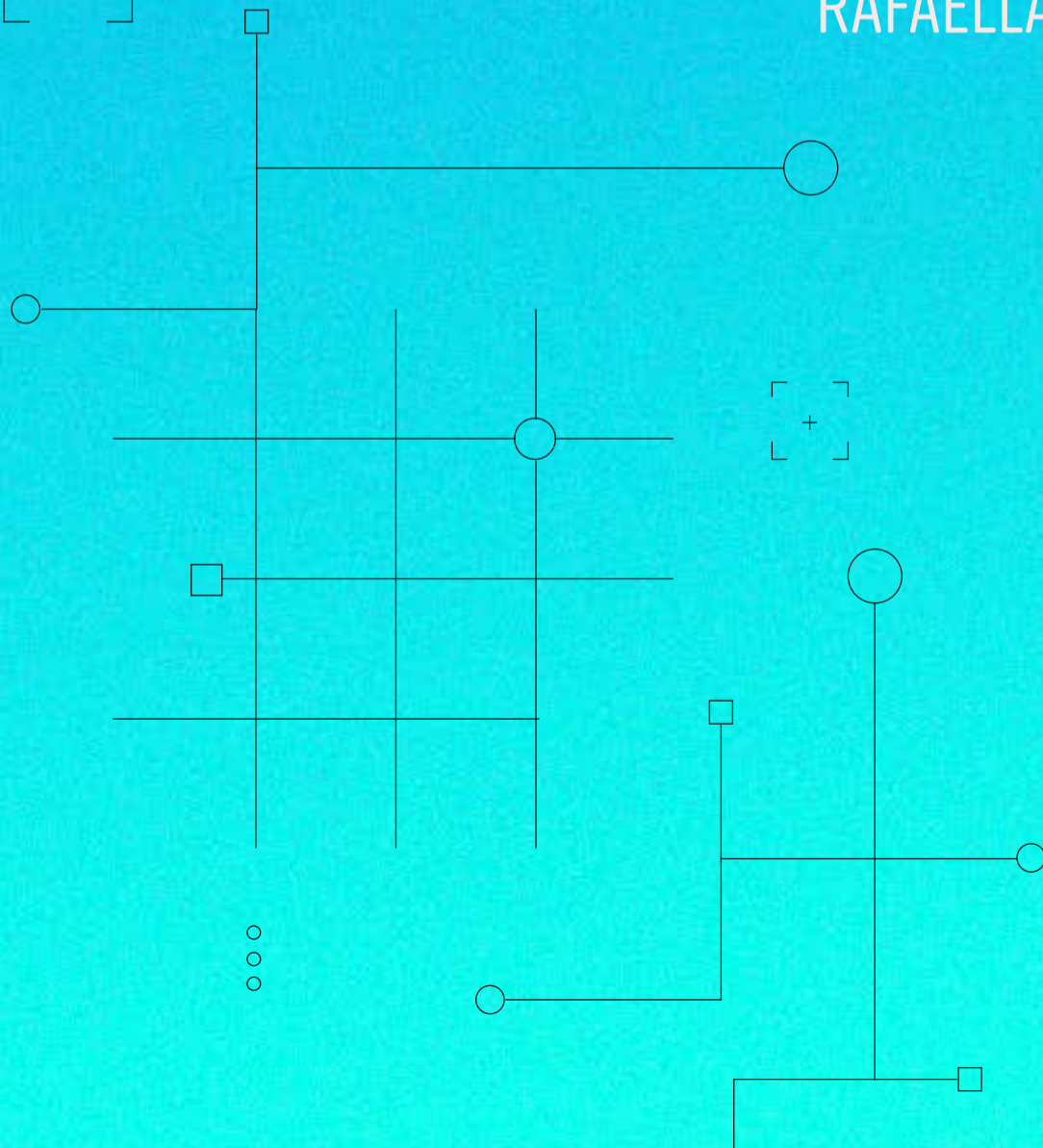
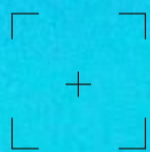
Willis, G., & Tranos, E. (2021). Using 'Big Data' to understand the impacts of Uber on taxis in New York City. *Travel Behaviour and Society*, 22, 94-107. doi: [10.1016/j.tbs.2020.08.003](https://doi.org/10.1016/j.tbs.2020.08.003)

Zhang, C. (2019). China's new regulatory regime tailored for the sharing economy : The case of Uber under Chinese local government regulation in comparison to the EU, US, and the UK. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 35(4), 462-475. doi: [10.1016/j.clsr.2019.03.004](https://doi.org/10.1016/j.clsr.2019.03.004)

Zwick, A., & Spicer, Z. (2018). Good or bad? Ridesharing's impact on Canadian cities. *Canadian Geographer*, 62(4), 430-436. doi: 10.1111/cag.12481

**As contribuições e os
desafios do open banking
no mercado financeiro
sob a perspectiva da
proteção de dados e da
concorrência**

RAFAELLA FERNANDES DOS SANTOS



Sumário: Introdução. 1. *Open Banking* e sua representação no mercado financeiro e consumidor. 1.1. Conceito e origens do *Open Banking*. 1.2. Regulação do *Open Banking* pelo Banco Central e suas fases de implementação. 2. Reflexos sobre aspectos concorrenciais e de proteção de dados. 2.1. *Open Banking* e o potencial de mitigação da concentração bancária no país. 2.2. A importância do consentimento como base legal para o compartilhamento de dados no *Open Banking*. 3. Mudanças decorrentes do *Open Banking* na prestação de serviço bancário e na competitividade do mercado. 3.1. Tendências para implementação do *Open Banking*. 3.2. Desafios relacionados ao *Open Banking*. Considerações finais. Referências.

Introdução

Muito tem se falado sobre as inovações tecnológicas que permeiam o setor financeiro a fomentar a agilidade buscada pelos consumidores, como o *Open Banking*, um ecossistema de interoperabilidade que irá permitir o compartilhamento de informações e serviços financeiros pelos clientes bancários em plataformas de tecnologia, instituído por fases pelo Banco Central como fomento à inovação e à concorrência na prestação de serviços de pagamento.

A abertura do sistema financeiro tem como um dos principais objetivos o fomento da inclusão financeira, necessidade que se tornou mais evidente no contexto da pandemia de Covid-19, além do incentivo à competitividade entre instituições mais consolidadas do setor e os novos entrantes, representados pelas *fintechs*. Trata-se de uma das etapas do movimento de extensão da abertura do mercado financeiro, convencionalmente chamado de *Open Finance*, que amplia o compartilhamento de informações para outros serviços do mercado financeiro, como plataformas de investimento, corretoras de seguros e fundos de previdência.

O presente artigo pretende trazer noções básicas que envolvem esse novo modelo de negócio no tocante aos serviços bancários, sem a intenção de esgotar o tema, percorrendo a regulação pelo Banco Central e suas etapas de implementação, que está se concretizando de forma gradual por representar uma mudança cultural no setor financeiro, a fim de analisar as repercussões do compartilhamento de dados bancários por instituições financeiras sob o viés da experiência do usuário, da proteção de dados e da concorrência.

1. Advogada graduada em Direito pela Universidade Federal Fluminense (UFF) e pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ) em parceria com o Instituto de Tecnologia e Sociedade (ITS) e o Centro de Estudos e Pesquisas no Ensino do Direito (Ceped).

1. *Open Banking* e sua representação no mercado financeiro e consumidor

1.1 Conceito e origens do *Open Banking* e a regulação Banco Central do Brasil

De acordo com o Banco Central do Brasil, o *Open Banking* é um sistema que permite aos clientes de produtos e serviços bancários o compartilhamento de dados entre diferentes instituições a partir de diferentes plataformas, e não apenas pelo aplicativo ou site do banco, proporcionado pela tecnologia de Interfaces de Programação de Aplicações (*Application Programming Interface* – APIs), isto é, sistemas computacionais que conversam entre si em uma rede usando uma linguagem em comum, permitindo a outros agentes de mercado interagir tecnologicamente com os sistemas informáticos das instituições financeiras (GOETTENAUER, 2020).

Por ser um fenômeno relativamente recente, a produção acadêmica sob o ponto de vista jurídico ainda é incipiente. Assim, para uma melhor compreensão dos objetivos do *Open Banking*, é importante analisar os primeiros marcos regulatórios no mundo, mais precisamente a regulação britânica e europeia, responsáveis por medidas para abertura do sistema financeiro que configuraram a primeira expressão do *Open Banking* no mundo.

Na União Europeia, a regulação do sistema se deu gradualmente, tendo início com o Regulamento nº 260/2012 com a finalidade de estimular a concorrência entre sistemas de pagamentos interoperáveis e racionalizar o funcionamento do mercado interno do bloco. Posteriormente, foi sancionada a Diretiva nº 2015/2366, também conhecida como PSD2 (*Second Payments Services Directive*), com o objetivo de definir padrões tecnológicos aos agentes de mercado para simplificação no desenvolvimento de arranjos de pagamentos, denominados *third party payment providers* (VIOLA, HERINGER, 2020).

Com a vigência da referida diretiva, o Reino Unido foi submetido à interferência regulatória em seu sistema financeiro, visto que à época ainda pertencia à União Europeia. Foi criado um órgão próprio² em parceria entre a autoridade concorrencial do país³ e os nove maiores bancos britânicos, responsável

2. *Open Banking Implementation Entity* (OBIE)

3. *Competition and Markets Authority* (CMA)

pela idealização da tecnologia para acesso aos dados bancários dos clientes e a interoperabilidade em um único aplicativo (VIOLA, HERINGER, 2020).

No Brasil, a implementação do sistema aberto financeiro é regulamentado pela Resolução Conjunta nº 01/2020 do Conselho Monetário Nacional e o Banco Central do Brasil, atualizado pela Resolução Conjunta nº 1, de 4 de maio de 2020 para integrar o termo “*Open Finance*” em substituição ao “*Open Banking*”. Trata-se de iniciativa que integra um conjunto de medidas estabelecidas para o crescimento da eficiência do mercado financeiro, chamado de “Agenda BC#”, estruturado em cinco dimensões: inclusão; competitividade; transparência, educação e sustentabilidade (VIOLA, THOMAZELLI, 2020).

Dessa forma, os objetivos definidos na resolução são: o incentivo à inovação; a promoção à concorrência; o aumento de eficiência do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB); e a promoção da cidadania financeira. A regulamentação também definiu os principais requisitos do *Open Banking*, tais como os participantes obrigatórios e voluntários, o escopo mínimo de dados e serviços a serem compartilhados, os processos de consentimento, autenticação e confirmação, e as responsabilidades dos participantes, além dos requisitos mínimos de segurança, entre outros.

De acordo com a Resolução Conjunta nº 01/2020, os principais atores do sistema do *Open Banking* são: (i) o cliente, titular dos dados bancários; (ii) a instituição transmissora de dados, que compartilha com a instituição receptora os dados; (iii) a instituição financeira receptora dos dados, que apresenta solicitação de compartilhamento à instituição transmissora; (iv) a instituição detentora de conta, que mantém a conta de depósitos à vista ou de poupança ou a conta de pagamento pré-paga de cliente; e (v) instituição iniciadora de transação de pagamento, autorizada pelo Banco Central por meio Resolução BCB nº 80, de 25 de março de 2021, que realiza a função de iniciação de pagamento sem deter fundos transferidos na prestação do serviço.

A participação de cada agente pode ser obrigatória ou facultativa, a depender da natureza dos dados compartilhados, do porte econômico e da relevância das atividades das instituições. Por exemplo, os participantes enqua-

drados no Segmento 1 (S1)⁴, e Segmento 2 (S2)⁵ do Sistema Financeiro Nacional (SFN) são obrigados a participar do sistema, possibilitando o compartilhamento de canais de atendimento e oferecimento de produtos e serviços de contas, tais como operações de crédito e câmbio, arranjos de pagamento, seguros e previdência. A participação voluntária é válida às demais instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil que não se enquadram nos Segmentos S1 e S2, e às instituições que tenham firmado contrato de correspondente no país, cujo objeto contemple, por meio eletrônico, a recepção e encaminhamento de propostas referente a operações de crédito e de arrendamento mercantil.

A implementação do *Open Banking* foi idealizada de forma gradual, referente aos padrões tecnológicos para o compartilhamento de dados e serviços, contemplando quatro fases previstas na Resolução BCB nº 109 de 24 de junho de 2021. Na primeira fase, houve a disponibilização ao público das informações padronizadas sobre canais de atendimento e características de produtos e serviços, com início em fevereiro de 2021. A segunda fase foi introduzida em agosto de 2021 com a possibilidade de solicitação pelos clientes do compartilhamento dos dados cadastrais e transacionais entre as instituições participantes. Na terceira fase, iniciada em outubro de 2021, os clientes passaram a poder compartilhar serviços de iniciação de transações de pagamento, começando com o Pix, seguido da entrada gradual dos demais arranjos de pagamento, bem como do encaminhamento de proposta de crédito.

Finalmente, na quarta e última fase, que teve início em dezembro de 2021, foi habilitado o compartilhamento de informações sobre operações de câmbio, investimentos, seguros, previdência complementar aberta e contas-salário, bem como acessar informações sobre as características dos produtos e serviços com essa natureza disponíveis para contratação no mercado. Esta última fase introduz o *Open Finance*, com previsão de conclusão em maio de 2022, cuja relevância é expressiva, uma vez que amplia a possibilidade de surgimento de novas soluções para a oferta de produtos e serviços financeiros,

4. De acordo com o artigo 2º, parágrafos 1º e 2º da Resolução nº 4.553 de 30 de janeiro de 2017, as instituições do Segmento 1 (S1) são bancos múltiplos, comerciais, de investimento, de câmbio, além de caixas econômicas que possuem porte igual ou superior a 10% (dez por cento) do Produto Interno Bruto (PIB), ou exerçam atividade internacional relevante, independentemente do porte da instituição. Exemplos: Banco do Brasil, Bradesco, BTG Pactual, Caixa Econômica Federal, Itaú e Santander.

5. De acordo com o dispositivo acima citado, o Segmento 2 (S2) compreende as instituições de porte inferior a 10% (dez por cento) e igual ou superior a 1% (um por cento) do PIB e pelas demais instituições de porte igual ou superior a 1% do PIB. Exemplos: Banrisul, Banco do Nordeste, BNDES, Citibank, Credit Suisse, Safra e Votorantim.

com o compartilhamento dos dados transacionais referentes aos produtos e serviços de cada escopo, mediante prévia autorização do cliente.

Conforme demonstrado no próximo capítulo, o cerne do sistema é o fomento da competitividade entre os agentes já consolidados no mercado e novos atores mediante a interoperabilidade, em prol do desenvolvimento de novos modelos de negócio voltados para a oferta de produtos mais adequados ao perfil de clientes.

2. Reflexos do *Open Banking* sobre aspectos concorrenciais e de proteção de dados

2.1 *Open Banking* e o potencial de mitigação da concentração bancária no país

Como já mencionado, o *Open Banking* é uma das iniciativas da Agenda BC# para o fomento à competitividade, diante da necessidade de redução da concentração bancária pelas grandes instituições financeiras. Nessa esteira, o *Open Banking* pode representar um marco para os novos entrantes, majoritariamente compostos por *fintechs*, plataformas centradas em soluções de tecnologia para o desenvolvimento de produtos e serviços financeiros (FUNDO MONETÁRIO MUNDIAL, 2019), reguladas pela Resolução 4.656 do Conselho Monetário Nacional (CMN).

Com o desenvolvimento de soluções para sistema aberto bancário por instituições com menor consolidação no mercado, vide o rol de participantes da Resolução Conjunta nº 01/2020 exposto no capítulo anterior, o movimento indica o favorecimento da inovação e da concorrência no sistema financeiro, bem como um benefício direto ao consumidor final, podendo-se ampliar a oferta de produtos e serviços bancários inclusive àqueles clientes que sequer eram contemplados pelas instituições tradicionais (PWC, 2020).

Há uma notável discrepância aos novos entrantes em comparação aos atores já estabelecidos e concentradores de dados que pode representar certa barreira de consolidação das *fintechs*. Por outro lado, as instituições financeiras tradicionais, no intuito de manter a consolidação em relação aos novos concorrentes, buscam novas tecnologias e oportunidades de racionalização de custos, realizando parcerias com as próprias *fintechs*, configurando um novo ecossistema em que os vetores de concorrência e parcerias se integram em benefício da redução de custos e maior acesso aos serviços financeiros.

Com efeito, o mercado financeiro sempre necessitou do desenvolvimento tecnológico, principalmente no tocante à segurança dos dados dos clientes, motivo pelo qual os bancos possuem vanguarda no uso da tecnologia, tendo sido os primeiros a se utilizar em larga escala. Na primeira era da globalização, entre o final do século XIX e metade do século XX, ocorreu predominância de transações analógicas e tecnologias como o telégrafo. A partir de meados da década de 1960, a digitalização das transações financeiras coincidiu com a concentração da atividade bancária em grandes instituições e a constituição de grandes bancos de dados informáticos da atividade financeira dos clientes. Atualmente o mundo vive uma simbiose sem precedentes entre sistema financeiro e tecnologia, cujo ponto de partida é considerado a crise econômica de 2008, que resultou na atuação de empresas de pequeno porte concorrendo no mercado com grandes atores já estabelecidos (GOETTENAUER, 2020).

De fato, dentro da perspectiva de adaptações tecnológicas exigidas pelo Banco Central para a participação ao *Open Banking*, as *fintechs* podem apresentar vantagens no tocante à adaptação de seus sistemas e na incorporação de novas tecnologias, em comparação com as instituições tradicionais. Por outro lado, as *fintechs* enfrentam notória desvantagem concorrencial de entrada no setor por não possuir, em comparação às grandes instituições, um banco de dados consolidado com atividades econômicas de pessoas físicas e jurídicas, considerando que o setor financeiro está baseado na guarda, transmissão e tratamento de informação, cujo arcabouço permite às instituições o desenvolvimento de serviços personalizados de acordo com as necessidades dos clientes (VIOLA, HERINGER, 2020).

Nessa conjuntura, há uma dicotomia em relação ao ecossistema de inovação no mercado financeiro, visto que, não obstante o crescimento exponencial das *fintechs*, ainda há uma concentração bancária expressiva no Brasil, embora tenha sofrido uma redução no ano de 2020, conforme Relatório de Economia Bancária elaborado pelo Banco Central. A mitigação da concentração pode ser atribuída à transformação digital no setor bancário, um dos impactos socioeconômicos decorrentes da pandemia da Covid-19, em razão da busca por serviços bancários menos onerosos e menos burocráticos, mormente para o recebimento de auxílio-emergencial concedido pelo governo federal entre 2020 e 2021, sendo para muitos a primeira oportunidade de “bancarização”.

A efervescência do mercado financeiro na era digital exige das instituições financeiras a adoção de soluções ágeis e digitais, especialmente aos bancos tradicionais. São diversos arranjos de pagamentos e bancos digitais adentrando ao Sistema de Pagamentos Brasileiro (SPB), estimulados pela re-

gulação do Banco Central do Brasil e sua agenda de inovação. Por isso, o sistema financeiro aberto promete mitigar esse gargalo relacionado ao acesso aos dados para os novos entrantes, pois haverá maior consolidação de banco de dados para melhor oferecimento de produtos e serviços bancários a partir do compartilhamento de dados dos clientes derivados de instituições financeiras tradicionais.

2.2 A importância do consentimento como base legal para o compartilhamento de dados no Open Banking

Não obstante as novas oportunidades para os consumidores e a promessa do aumento da competitividade, a consolidação do *Open Banking* levanta certas questões em relação ao controle dos dados pessoais dos titulares, uma vez que o maior fluxo de dados a partir do emprego de APIs abertas acarretará em expressivo aumento no volume de informações compartilhadas e maior preocupação com mecanismos eficazes de segurança (TRINDADE, 2021).

A interoperabilidade que permite o funcionamento das APIs abertas está intimamente atrelada ao direito à portabilidade, previsto no artigo 18, inciso V, da LGPD, no sentido de proporcionar a transmissão e reutilização dos dados pessoais, que resultam no oferecimento de serviços mais adaptáveis às necessidades do cliente bancário. Trata-se de expressão da autodeterminação informativa do titular dos dados, possibilitando ao cliente, titular dos dados bancários, trocar o prestador de serviços sem perder o *status quo* já conquistado no prestador de serviços inicial (VIOLA, THOMAZELLI, 2020).

Para autorizar o compartilhamento de dados, o cliente deve estar certificado de que as instituições participantes cumpram com o dever de cautela para mitigar riscos de incidentes no tratamento. As vantagens atribuídas à interoperabilidade não podem ser concebidas sem uma legítima preocupação com a segurança dos dados, afinal trata-se de um ambiente onde os usuários desejam ter confiança de que suas informações são seguramente manuseadas, de maneira que o modelo de negócio dos participantes também deve ser guiado pela privacidade (DELOITTE, 2018).

A Regulação Conjunta nº 01/2020 é uma imposição legal e regulatória para permitir a portabilidade dos dados bancários do cliente entre instituições financeiras, assim como a interoperabilidade dos seus sistemas, assegurando-se a proteção de dados, de modo a que seja preservada e estimulada a concorrência no mercado financeiro, além da autodeterminação dos seus titulares no âmbito do sistema financeiro. Por isso, um dos principais desafios

para os participantes será a consolidação do trinômio “portabilidade – interoperabilidade – proteção de dados” pessoais para o funcionamento do *Open Banking* (TRINDADE, 2021).

Assim, o compartilhamento dos dados no sistema aberto deve se dar, principalmente, mediante a prévia e expressa solicitação do cliente, após as etapas de consentimento, autenticação e confirmação, conforme art. 10 da Resolução Conjunta nº 01/2020, respeitando-se a exigência da base legal prevista no art. 7º, inciso I, da LGPD. A fim de garantir a segurança e proteção de dados do cliente, a obtenção do consentimento pelas instituições participantes deve apresentar a identificação do cliente, possuir linguagem clara e objetiva, com prazo compatível com as finalidades do consentimento, limitado a 12 meses, com informações discriminadas das instituições transmissoras e detentora da conta, bem como dos dados e serviços que serão compartilhados.

Nesse sentido, é possível afirmar que a preocupação com a segurança é uma das contribuições mais relevantes do *Open Banking*, o que pode ser considerada uma iniciativa moldada pelo *privacy by design*, visto que é o próprio cliente bancário, como titular dos seus dados, quem opta por iniciar o compartilhamento, obedecendo as etapas do consentimento, da autenticação e da confirmação da solicitação do usuário.

Cabe lembrar que o *Open Banking* fora viabilizado na Europa a partir da Diretiva nº 2015/2366 da União Europeia, isto é, anteriormente à vigência da GDPR em 25 de maio de 2018 (Art. 94, 1, Regulamento UE 2016/679). Já no Brasil, o *Open Banking* está sendo implementado com o espírito da Lei nº 13.709/18, a Lei Geral de Proteção de Dados (LGPD). Nesse diapasão, o sistema financeiro aberto brasileiro está alicerçado pelos princípios e regras concorrentes à LGPD, e na autodeterminação informativa, isto é, o cliente é o titular dos seus dados pessoais.

Assim, o *Open Banking* tem o potencial para despontar como um modelo de negócio bem sucedido baseado na convergência da experiência do usuário e de mecanismos de proteção de dados e garantia da privacidade, que poderá ser um diferencial de mercado a fomentar a competitividade no setor bancário.

3. Mudanças decorrentes do *Open Banking* na prestação de serviço bancário e na competitividade do mercado

3.1 Tendências para implementação do *Open Banking*

Diante dos pontos acima mencionados, é certo que o estímulo do *Open Banking* à inovação pode solucionar gargalos encontrados pelo sistema bancário tradicional, como a aprovação de crédito mais rápida e menos burocrática, o uso da tecnologia para melhorar a experiência do cliente e o estímulo à competitividade entre *fintechs* e grandes bancos.

A partir da interoperabilidade do sistema, proporcionada pela disponibilização de APIs para a transferência de dados do cliente, o *Open Banking* tem potencial de facilitar os modelos de negócios calcados em plataformas abertas, uma tendência denominada *banking as a platform*, que mescla a oferta de produtos e serviços próprios com os de terceiros, incluindo instituições não financeiras, bem como agregar novos clientes com a utilização das APIs para distribuição de serviços financeiros, em uma tendência de mercado conhecida como *banking as a service*, que pode representar vantagens de redução de custos às instituições e ao consumidor que solicitou o compartilhamento dos dados (ZACHARIADIS, OZCAN, 2017).

Nesse diapasão, a interoperabilidade exigida pelo *Open Banking* exigirá das instituições o desenvolvimento de interfaces abertas e a padronização na formatação de dados, o que poderá implicar em mudanças na organização interna de seus sistemas, sendo indispensável o investimento em gestão de informações, além da elaboração de princípios e regras de governança interna, a fim de viabilizar a resolução de disputas entre participantes e clientes (VIO- LA, THOMAZELLI, 2020).

Recorda-se que o *Open Banking* integra uma das medidas da Agenda BC#, um conjunto de reformas para melhorias ao mercado financeiro. Dentre as dimensões da agenda, destacam-se as que mais se relacionam com a abertura do sistema financeiro: (i) inclusão, no sentido de buscar a facilitação do acesso ao mercado; (ii) competitividade, com o propósito de estabelecer adequada precificação pelo desenvolvimento tecnológico; e (iii) educação financeira, a fim de conscientizar os consumidores a participarem do mercado e cultivar hábitos financeiros saudáveis, como o uso responsável do crédito e controle do orçamento doméstico.

Tais fatores possuem o potencial de contribuir para a democratização financeira da população, melhorar o acesso ao crédito e mitigar os efeitos do superendividamento, afinal o usuário poderá acessar melhores condições e verificar os melhores juros praticados por cada instituição. Destaca-se o momento de estímulo de novos arranjos ao Sistema Brasileiro de Pagamentos (SPB), com um aumento exponencial da abertura de contas de pagamento, proporcionada pelo aquecimento do mercado das *fintechs* e pela regulação do Banco Central, de modo que a adesão ao *Open Banking* pode contar com muitos brasileiros recentemente “bancarizados”, como uma expressão da promoção da cidadania financeira, um dos objetivos traçados pelo Banco Central na implementação do sistema financeiro aberto.

3.2 Desafios relacionados ao *Open Banking*

Apesar de tantos pontos positivos advindos do ecossistema do *Open Banking*, um ponto sensível à adesão da população brasileira ao *Open Banking* é a defasagem na bancarização e no acesso à internet nas classes mais baixas, especificamente D e E. Não obstante a digitalização da sociedade nos últimos anos, principalmente no setor bancário, há uma parcela da população que não possui tanto conforto com as novas tecnologias, como, por exemplo, os idosos, que possuem maiores vulnerabilidades como consumidores finais na prestação de serviços bancários, sobretudo no contexto de fraudes mediante engenharia social, cada vez mais crescente nos últimos anos.

Não por acaso o *Open Banking* ainda é desconhecido pela maioria da população brasileira, sendo mais provável a adoção pela população mais jovem, seja pela maior disposição para compartilhamento de dados, seja pelo conforto com as novas tecnologias, além da maior probabilidade de mudança de banco entre a geração *millennial* e a geração Z, que buscam cada vez mais serviços personalizados (PWC, 2018). Essa tendência indica um desafio das instituições na promoção de campanhas publicitárias para fomentar a adesão ao sistema financeiro aberto e, principalmente, empenhar iniciativas de conscientização da segurança cibernética em linguagem simples e direta, em referência ao artigo 8º do Código de Defesa do Consumidor, para estimular um ambiente confortável aos usuários para o compartilhamento de dados.

Uma das questões mais sensíveis do *Open Banking* são os riscos de incidentes de segurança no âmbito do *Open Banking*, cabendo às instituições participantes o comprometimento total com investimentos em segurança e privacidade, como meio de prevenção da ocorrência de danos em virtude do tratamento de dados pessoais, conforme artigo 6º, inciso VIII, da LGPD. Por

isso, a participação no *Open Banking* torna imprescindível o investimento massivo em tecnologia de segurança da informação, com etapas rígidas de autenticação, haja vista a responsabilidade das instituições participantes pela confiabilidade, integridade, disponibilidade, segurança e sigilo dos dados⁶,

Assim, a concretização da autodeterminação informativa deve ir além de um mero argumento de mercado, devendo as instituições estarem alinhadas com as políticas de segurança cibernéticas para garantir o controle dos dados pertencentes aos usuários, assunto de elevada estima ao Banco Central, que publicou normas específicas disciplinando a política de segurança cibernética e os requisitos para a contratação de serviços de computação em nuvem.⁷

Como visto anteriormente, a implementação do *Open Banking* no Brasil foi baseada na proteção dos dados dos usuários e no incentivo à eficiência e competitividade do setor bancário. Neste sentido, a Lei Geral de Proteção de Dados dispõe a competência da Autoridade Nacional de Proteção de Dados (ANPD) para articular com autoridades reguladoras públicas, inclusive para aplicação de sanções administrativas (artigos 55-J e 55-k, parágrafo único), o que torna impositivo o diálogo entre a ANPD, o Banco Central do Brasil (BCB) e o Conselho Administrativo de Defesa Econômica (CADE).

Sendo uma inovação recente, ainda há muitas especulações sobre a efetiva adesão da população brasileira ao *Open Banking*, contudo é inegável que se trata de uma iniciativa louvável do Banco Central, em prol da competitividade no mercado financeiro e do empoderamento do consumidor, fatores que estão interligados ao tratamento adequado dos dados pessoais. Portanto, o êxito do sistema aberto financeiro depende, essencialmente, da simbiose entre questões relacionadas ao direito da concorrência, à proteção de dados pessoais e ao Sistema Financeiro Nacional, o que exigirá a supervisão conjunta dos respectivos órgãos reguladores e fiscalizadores acerca do funcionamento do *Open Banking* pelos atores participantes.

Considerações finais

A implementação do *Open Banking* no Brasil tem tudo para ser um exemplo a ser seguido, visto que, diferentemente de outros países, sua implementação

6. Art. 31 da Resolução Conjunta nº 1, de 4 de maio de 2020.

7. Resolução nº 4.658/18 do BCB, que estabelece a obrigação de uma política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem e Circular nº 3.909/18, que regula os requisitos para a contratação desses serviços.

foi baseada na proteção dos dados dos usuários e no incentivo à eficiência e competitividade do setor bancário, com a supervisão exclusiva do Banco Central em todas as fases de implementação.

A consolidação da interoperabilidade de serviços, atrelada ao funcionamento das APIs que possibilitam o compartilhamento de dados do cliente e acesso de terceiros ao sistema da instituição financeira, deve permitir o fomento da concorrência por diminuir as barreiras de entrada e acesso de novos atores aos dados consolidados dos consumidores oriundos de instituições tradicionais do mercado. Por tais questões, há grandes expectativas de que o *Open Banking* seja uma virada de chave na atividade bancária e expectativa de melhora na prestação do serviço ao consumidor final.

Mesmo sendo uma ideia promissora, o *Open Banking* se esvaziará em seu propósito se não estiver em consonância com os princípios e regras que regem a Lei Geral de Proteção de Dados Pessoais (LGPD), afinal, os dados pertencem aos usuários, e não aos bancos, uma vez que o maior atrativo do sistema aberto é a garantia de um ambiente de confiança aos clientes para o compartilhamento de seus dados bancários e pessoais com outras instituições e em provedores de terceiros em que sequer possui cadastro ou conta.

Portanto, o *Open Banking* representa, indubitavelmente, uma ideia promissora em relação ao fomento da concorrência no setor bancário, que enfrenta uma notória concentração de mercado em poucos bancos tradicionais. Contudo, não pode em dissonância com a LGPD, afinal, os dados pertencem aos usuários, e não aos bancos. É essencial, portanto, a supervisão dos órgãos reguladores nacionais, não apenas do Banco Central do Brasil (BCB), como também da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Administrativo de Defesa Econômica (CADE), uma vez que só poderá alcançar seu objetivo se estiver alinhado com os propósitos de concorrência e proteção de dados.

Referências

BRASIL. Presidência da República. Ministério da Economia. Banco Central do Brasil. Relatório de Economia Brasileira 2020. 2021. Disponível em: <https://www.bcb.gov.br/publicacoes/relatorioeconomiabancaria>. Acesso em 06 jan. 2022.

BRASIL. Presidência da República. Ministério da Economia. Banco Central do Brasil. *Open Banking*. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/openbanking>. Acesso em 09 jan. 2022.

BRASIL. Presidência da República. Ministério da Economia. Banco Central do Brasil. Resolução Conjunta nº 1, de 4 de maio de 2020. Implementação do Sistema Financeiro Aberto. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055>. Acesso em: 21 dez. 2021.

BRASIL. Presidência da República. Ministério da Economia. Banco Central do Brasil. Resolução BCB nº 109 de 24/6/2021. Disponível em: <https://www.bcb.gov.br/estabilidade/financeira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=109>. Acesso em: 09 jan. 2022.

DELOITTE. *Open Banking - Privacy at the epicentre*. 2018. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-privacy-epicentre-170718.pdf>. Acesso em 01 fev. 2022.

FUNDO MONETÁRIO MUNDIAL. *Fintech: The Experience So Far*. 2019. Disponível em: <https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056>. Acesso em 30 dez. 2021.

GOETTENAUER, Carlos. *Open Banking e o Modelo de Banco em Plataforma: a necessidade de reavaliação da definição jurídica de atividade bancária*. In: Revista da Procuradoria-Geral do Banco Central. v. 14 n. 1 (2020). 2020. Disponível em: <https://revistapgbc.bcb.gov.br/index.php/revista/article/view/1025>. Acesso em 06 jan. 2022.

PWC. *The future of banking is open & how to seize the Open Banking opportunity*. Reino Unido: 2018. Disponível em: <https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf>. Acesso em 06 jan. 2022.

PWC. Pesquisa *Fintech Deep Dive 2020*. Brasil: 2020. Disponível em: <https://www.pwc.com.br/pt/estudos/setores-atividade/financeiro/2021/pesquisa-fintech-deep-dive-2020.html>. Acesso em 30 dez. 2021.

RUBINSTEINN, Gabriel. *Open Banking* ainda é desconhecido por 84% dos brasileiros, aponta pesquisa. Exame, 2021. Disponível em: <https://exame.com/future-of-money/pix-open-banking/open-banking-ainda-e-desconhecido-por-84-dos-brasileiros-aponta-pesquisa/>. Acesso em 09 jan. 2021.

TRINDADE, Manoel Gustavo Neubarth. *Open Banking – Trinômio Portabilidade – Interoperabilidade – Proteção de Dados Pessoais no âmbito do Sistema Financeiro*. Revista Jurídica Luso-Brasileira, 4ª ed. Ano 07. 2021. Disponível em: <https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-7-2021-n-4/216>. Acesso em 04 fev. 2022.

VIOLA, Mario; HERINGER, Leonardo; COSTA, Janaína. Relatório *Open Banking* e Proteção de Dados. Instituto de Tecnologia e Sociedade: Rio de Janeiro, 2020. Disponível em: <https://itsrio.org/pt/publicacoes/open-banking-e-protecao-de-dados>. Acesso em 21 dez. 2021.

VIOLA, Mario, THOMAZELLI, Patrícia. Relatório Portabilidade de Dados, Interoperabilidade e *Open Banking*. Instituto de Tecnologia e Sociedade: Rio de Janeiro, 2021. Disponível em: <https://itsrio.org/pt/publicacoes/relatorio-portabilidade-de-dados-interoperabilidade-e-open-banking/>. Acesso em 09 jan. 2022.

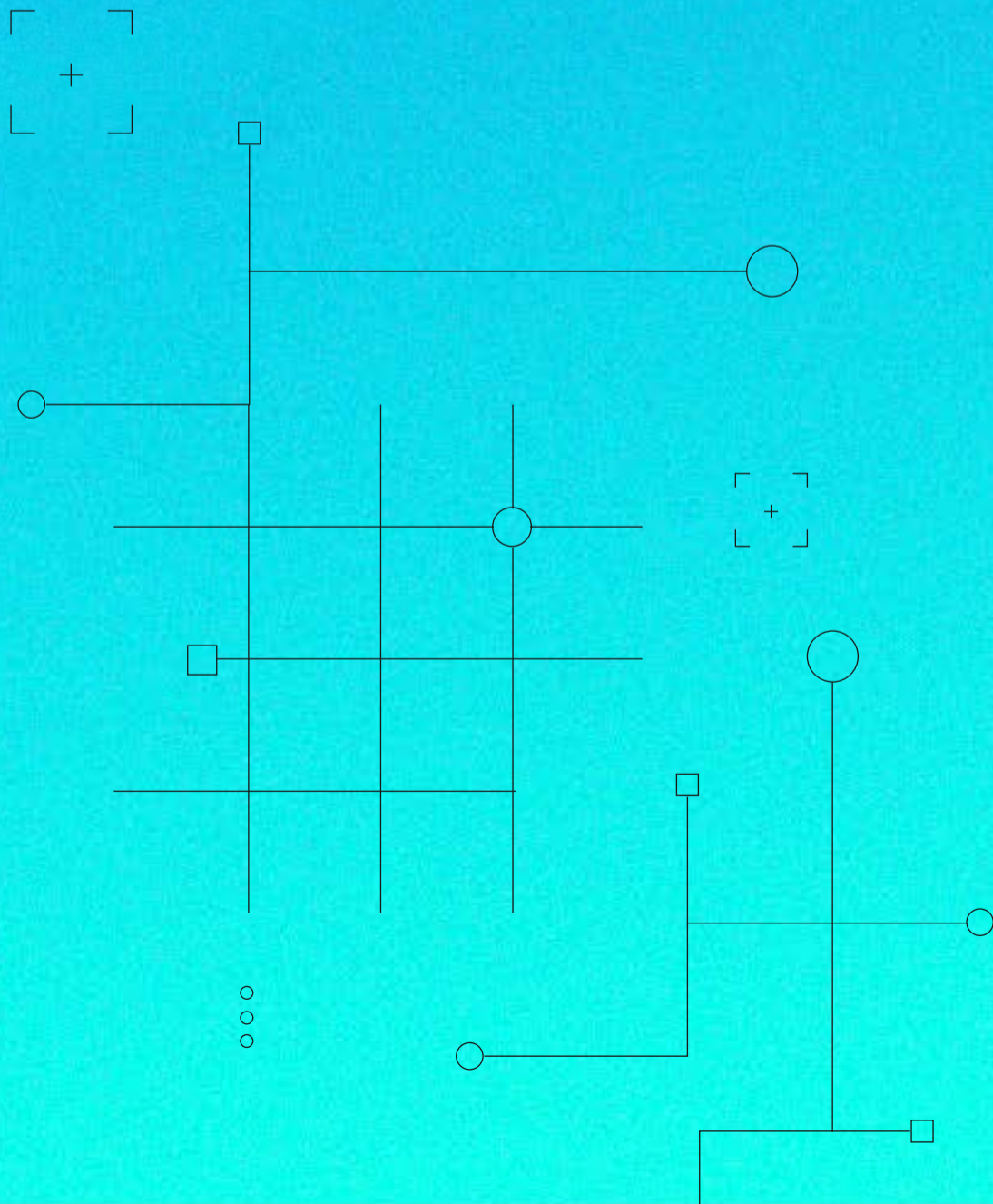
ZACHARIADIS, Markos. OZCAN, Pinar. *The Api Economy and Digital Transformation in Financial Services: The Case of Open Banking*. SWIFT Institute Working Paper NO. 2016-001: Reino Unido, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199. Acesso em 17 abr. 2022.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

15

Tributação de Software: uma análise sobre incidência do ICMS e do ISS

BÁRBARA MILANESE PIMENTEL



Sumário: Introdução. 1. Software, conceito e natureza jurídica. 1.1. *Clouding Computing*, conceitos e características. 2. Tributação. 2.1. ICMS – Imposto sobre a Circulação de Mercadorias e Serviços. 2.2. ISS – Impostos sobre Serviços de qualquer natureza. 3. Supremo Tribunal Federal e o atual entendimento sobre tributação de Software. Considerações finais. Referências.

Introdução

As questões envolvendo o enquadramento jurídico e tributário da licença e/ou cessão de uso de programas de computador (software) é antiga, mas vem tomando força, na medida em que o avanço da tecnologia impacta nos conceitos e premissas utilizadas no passado para definir o enquadramento jurídico e tributário desses negócios jurídicos.

Em razão do enorme potencial arrecadatório, atualmente é possível localizar normas estaduais e municipais que pretendem justificar a tributação de softwares padronizados, customizados e/ou em computação em nuvem, tanto pelo ICMS quanto pelo ISS, em uma tentativa estressante de enquadramento das novas tecnologias em conceitos trazidos pela Constituição Federal de 1988 e ainda com pouca regulação em Lei Complementar.

Pretendemos neste estudo estudar os conceitos jurídicos de software e as hipóteses de incidência do ICMS e ISS para verificar qual seria o melhor modelo de tributação (longe de esgotar as discussões sobre o tema).

1. Software, conceito e natureza jurídica

Segundo Roberto Chacon de Albuquerque (2006), *Software* é um conjunto de elementos lógicos que controla e gerencia o funcionamento do *hardware* que, por sua vez, é o corpo físico do computador. O software pode ser subdividido em duas espécies: (i) softwares básicos, responsáveis pelas operações fundamentais da máquina (correspondendo aos sistemas operacionais); e os (ii) softwares aplicativos, desenvolvidos para atender tarefas específicas e determinadas de acordo com o interesse do usuário final.

1. Advogada graduada (2009) e especialista em Direito Tributário (2012) pela Pontifícia Universidade Católica de São Paulo, e pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro, em parceria com a Universidade do Estado do Rio de Janeiro-UERJ.

Em outras palavras, software é todo programa presente nos computadores e demais dispositivos eletrônicos, como celulares, televisores, *tablets* e outros.

No Brasil, a primeira norma específica a tratar de software ou programa de computador foi a Lei 7.646/1987, revogada em 19 de fevereiro de 1998 pela Lei 9.609/1998. A intenção do legislador foi conceder ao software um regime de proteção de direitos autorais, adotando o entendimento de que o software é obra imaterial, resultante do esforço intelectual e criativo do programador.

O artigo 1º da Lei 9.609/1998, ainda vigente, manteve a definição de programa de computador trazida pela Lei 7.646/1987 como:

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

Além de manter o conceito de computador, a Lei 9.609/1998 também manteve, em seu artigo 9º, a previsão de que o uso de programa de computador deve ser objeto de contrato de licença.

A licença de uso de programas de computador ou a licença de uso de software consiste em uma autorização de uso dada pelo licenciante ou licenciado sobre determinadas condições pré-fixadas em contrato pelas partes (licenciante e licenciado). Vale dizer que a licença de uso do software não altera a titularidade dos direitos patrimoniais sobre o software, apenas concede ao licenciado o direito de utilização do software.

Portanto, podemos concluir que a essência do software é algo intangível e decorre da criatividade, do esforço intelectual de seu autor, de forma que o tratamento jurídico dado ao software é de direito autoral, seja ele classificado como software de “prateleira”, software encomendado, software customizado e software em nuvem.

1.1 “Clouding Computing”: conceitos e características

Com o avanço tecnológico e a disseminação da internet, que contribuiu para uma crescente inovação, não apenas em termos de funcionalidades e acesso aos softwares, mas também nas formas de exploração de seu uso, houve o surgimento *do cloud computing*, traduzido como computação em nuvem).

A computação em nuvem é o fornecimento de serviços de computação, incluindo servidores, armazenamento, banco de dados, rede, software, análise e inteligência, pela Internet (denominada como “a nuvem”) para oferecer ao consumidor inovações mais rápidas, recursos flexíveis e economias de escala.

O *National Institute of Standards and Technology* (NIST), pertencente ao Departamento de Comércio dos Estados Unidos, em estudo sobre *Clouding Computing*, definiu computação em nuvem como um modelo de rede compartilhada de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que pode ser provisionado e liberado com o mínimo de esforço de gerenciamento ou interação do provedor de serviços. Este modelo é composto por cinco características essenciais, sendo elas:

Autoatendimento sob demanda: permite o consumo de recursos computacionais (como tempo do servidor e armazenamento de rede), automaticamente, sob demanda e sem interação com o provedor desses recursos;

Amplo acesso à rede: os recursos estão disponíveis na rede (internet) e podem ser acessados por dispositivos como computadores, celulares, *tablets* e outros;

Agrupamento de recursos: reunião de recursos de computacionais, físicos e virtuais para atendimento, sob demanda, das necessidades de vários consumidores, que não possuem controle ou conhecimento sobre a localização do provedor do serviço;

Elasticidade rápida: permite que os recursos sejam liberados rapidamente e automaticamente, de acordo com a demanda. Ao consumidor os recursos disponíveis muitas vezes parecem ilimitados e que podem ser disponibilizados a qualquer tempo; e

Serviço medido: sistemas que possibilitam o controle/monitoramento e a medição dos recursos utilizados, trazendo transparência para o consumidor e para o provedor dos recursos.

Ainda de acordo com o NIST, a computação em nuvem pode ser dividida em três modelos de serviços:

Software as a Service (SaaS) (traduzido software como serviço) - recurso que possibilita ao consumidor o uso de aplicativos executados em nuvem. Os aplicativos podem ser acessados pelo consumidor por vários dispositivos por meio de interface com um navegador web;

Plataform as a Service (PaaS) (traduzido como plataforma como servi-

ço) – recurso que possibilita ao consumidor a implantar na nuvem aplicativos criados ou adquiridos pelo consumidor, desenvolvidos utilizando linguagem de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor; e

Infrastructure as a Service (IaaS) (traduzido como infraestrutura como serviço) – recurso que possibilita ao consumidor o processamento, armazenamento, comunicação de rede e outros recursos computacionais fundamentais, em que o consumidor é capaz de implementar e executar o software, incluindo sistemas operacionais e aplicações.

Assim, com o surgimento da computação em nuvem foi possível tornar o acesso ao software, que antes era conhecido apenas como software com processamento em suporte físico ou em ambiente virtual por meio de *download*, de forma remota e sob demanda, diretamente pela internet, denominada *software as a service* (SaaS).

No modelo SaaS, o software é suportado e executado em nuvem, ou seja, o usuário mediante licença de uso acessa o programa de computador pela internet (mediante *login* e senha), sem a necessidade de instalar o programa em dispositivo físico. Neste modelo é necessário a contratação de serviços de infraestrutura, processamento e armazenamento de dados e outros recursos computacionais pelo provedor/fornecedor do software, necessários para utilização do software.

Portanto o SaaS, ao combinar a licença de uso de software com a oferta de recursos informáticos e soluções tecnológicas pelo fornecedor, proporcionados pela infraestrutura em nuvem, alterou não só a forma de acesso do usuário ao software, mas também o modelo de negociação (licença temporária e por assinatura).

Apesar de toda evolução tecnológica e as diversas evoluções dos softwares disponíveis hoje no mercado, conforme acima explanado (software *on premises* e softwares em nuvem – SaaS, IaaS, PaaS) ainda temos, aqui no Brasil, dificuldade para solucionar a questão da tributação incidente sobre os programas de computadores, conforme será analisado a seguir.

2. Tributação

Após a análise do conceito de software e características, podemos analisar se há ou não subsunção entre as operações/relações jurídicas envolvendo software com as hipóteses de incidência do ICMS e ISS previstas na legislação.

2.1 ICMS – Imposto sobre a circulação de mercadorias e serviços

O art. 155, inciso II, da Constituição Federal de 1988 atribui competência aos Estados e ao Distrito Federal para a instituição de imposto sobre “operações relativas à circulação de mercadorias e sobre prestações de serviços de transportes interestadual e intermunicipal e de comunicação, ainda que as operações e as prestações se iniciem no exterior”, o chamado ICMS. Sua regulamentação está prevista na Lei Complementar 87/1996 (a chamada “Lei Kandir”).

A referida Lei Kandir, seu artigo 2º, elege cinco hipóteses de incidência do ICM, sendo elas (i) “operações relativas à circulação de mercadorias”, (ii) “serviços de transporte interestadual intermunicipal”; (iii) serviços de “comunicação”; (iv) produção, importação, circulação, distribuição ou consumo de energia elétrica; e (v) extração, circulação, distribuição ou consumo de minerais.

Assim, para que haja a incidência do ICMS sobre as relações jurídicas que envolvem softwares é necessário que haja uma das cinco hipóteses de incidência acima elencadas. No caso em questão, a hipótese de incidência que será estudada concerne às operações relativas à circulação de mercadorias, tendo em vista que interessa a tributação do SaaS.

Portanto, para fins de entendimento da tributação do ICMS é necessário entender os conceitos de “operação”, “circulação” e “mercadoria”, isto porque são conceitos interligados e necessários para determinar se haverá ou não a incidência do imposto (a subsunção do fato a norma).

Nesse sentido, podemos dizer que (i) “operação” deve ser entendido como ato negocial necessário para a ocorrência da circulação, (ii) “circulação” deve ser entendida como a passagem das mercadorias de uma pessoa para a outra, com a conseqüente mudança de patrimônio; e (iii) “mercadoria” deve ser entendida e definida como bem corpóreo destinado a atividade empresarial do produtor industrial e comerciante, cujo objetivo é a distribuição para consumo.

Os conceitos acima são importantes para entender que não há tributação pelo ICMS sem que haja “operação relativa à circulação de mercadoria”, ou seja, não é possível tributar somente a mercadoria.

Em que pesem os conceitos acima representarem o entendimento de parte da doutrina tributária brasileira (entendimentos compartilhados pelos professores José Eduardo Soares de Mello (2012), Roque Antônio Carrazza (2009) e Paulo de Barros Carvalho (2015), há uma outra parte da doutrina que entende que não há necessidade de efetiva transferência de propriedade da mercador-

ria para fins de incidência do ICMS e que o que define uma coisa como mercadoria é o aspecto subjetivo daquele que a criou, se a coisa foi criada para uma finalidade mercantil, de modo que ela será considerada uma mercadoria, independentemente de ser corpórea ou não.

Para o presente estudo, a premissa que será adotada é a mesma dos professores José Soares de Mello, Roque Antônio Carrazza e Paulo de Barros Carvalho, que em uma interpretação sistemática da Constituição Federal, entendem que mercadoria é todo bem móvel, corpóreo e que tenha finalidade mercantil (se não fosse este o entendimento de mercadoria adotado pela Constituição, não seria necessário incluir ressalva em lei sobre a incidência do ICMS sobre a energia elétrica). No que concerne à “circulação” o entendimento é de que a circulação decorre de operação jurídica, com efetiva transferência de sua titularidade.

Corroborando o entendimento adotado neste estudo, o Supremo Tribunal Federal (STF) no julgamento do Recurso Extraordinário com Agravo nº 1.255.885, em 15 de agosto de 2020, pacificou o entendimento de que “não incide ICMS no deslocamento de bens de um estabelecimento para outro do mesmo contribuinte localizados em estados distintos, visto não haver a transferência da titularidade ou a realização de ato de mercancia”.

Deste modo, resta sedimentado pelo STF e por relevante parte da doutrina, o entendimento no sentido de que apenas a circulação jurídica de mercadoria, com fim de mercancia, e que acarreta a efetiva transferência de titularidade da mercadoria estará sujeita ao ICMS.

Neste mesmo sentido, importante analisar que em softwares transacionados por *download* ou por acesso em nuvem (mediante *login* e senha) não há a transferência de titularidade, ou seja, o consumidor/usuário se sujeita às limitações de uso impostas pelo provedor/proprietário do software. Portanto, resta claro que se não há transferência de titularidade do software não há que se falar em circulação de mercadoria e incidência do ICMS.

Em relação ao conceito de mercadoria, o STF ainda não pacificou o entendimento sobre se seriam apenas bens corpóreos ou se seria possível evoluir o conceito de mercadoria para bens incorpóreos tendo em vista a evolução da tecnologia e a necessidade de uma possível evolução do conceito de mercadoria para fins tributários.

De todo modo, em que pese o conceito de mercadoria não estar pacificado na doutrina ou na jurisprudência, entendemos que, sob os alicerces da Constituição, será passível de incidência do ICMS apenas o ato negocial que acarre-

ta transferência de titularidade de bem móvel corpóreo, destinado à mercancia. Caso o STF entenda necessário atualizar o conceito de mercadoria para inserir os bens incorpóreos, em especial o software, esta mudança deve ser realizada por meio de lei e não por uma interpretação dinâmica e extensiva da Constituição Federal.

Portanto, tendo em vista que software é algo incorpóreo e com uso licenciado por prazo determinado ao consumidor (sem efetiva transferência de titularidade e sem a intenção de mercancia), concluímos que não deverá haver incidência de ICMS sobre as operações envolvendo softwares.

2.2 ISS - Imposto Sobre Serviços de qualquer natureza

O artigo 156, III, da Constituição Federal, outorgou aos Municípios a competência para instituir e regulamentar o imposto sobre serviços de qualquer natureza, não compreendidos no art. 155, II, definidos em lei complementar”. Assim, tem-se que o fato gerador do ISS é a prestação de um serviço de qualquer natureza, não compreendido no âmbito de incidência do ICMS e definido por Lei Complementar.

Na doutrina há o entendimento predominante de que o conceito de serviço apontado pelo constituinte é aquele adotado no direito privado, ou seja, “é o esforço humano que se volta para outra pessoa; é fazer desenvolvido para outrem. O serviço é, assim, um tipo de trabalho que alguém desempenha para terceiros”.

Segundo o entendimento de Aires Fernandino Barreto (2009), serviço, para fins de incidência do ISS, deve ser compreendido como o esforço humano, do qual decorrerá um bem material ou imaterial passível de mensuração econômica, em favor de um terceiro – tomador do serviço. É o desprendimento de esforço com intuito de cumprir uma obrigação de fazer.

Por outro lado, parte da doutrina sustenta que o conceito de serviço deve se basear na classificação econômica entre bens materiais e imateriais, de modo que todas as atividades que não constituam circulação de bens corpóreos (que seriam tributados pelo ICMS), devem ser tributadas pelo ISS.

Apesar do entendimento acima veiculado, entendemos que a divisão entre bens materiais e imateriais pouco importa para fins de incidência do ISS, eis que esse imposto possui como fato gerador a “prestação” do serviço, sendo irrelevante o resultado dessa prestação se traduzir em um bem material ou imaterial.

Portanto, para o presente estudo, adotamos o entendimento de que a prestação de serviço é caracterizada pela efetiva obrigação de fazer consistente em esforço humano, que vise a produção de bem material ou imaterial em favor de terceiro, a título oneroso e que não configura relação trabalhista.

No âmbito do ISS, o legislador passou a delimitar a incidência pela Lei Complementar nº. 116, de 31 de julho de 2003 e, portanto, trouxe uma lista taxativa dos serviços que incidem o imposto. Neste ponto, importante destacar que o legislador incluiu na lista de serviços da referida lei complementar (item 1.05) “o licenciamento ou cessão de direito de uso de programas de computação” como serviço/atividade sujeito ao ISS.

Superado o conceito de serviços trazido acima e a informação de que o licenciamento ou cessão dos direitos de uso do software é considerado pelo legislador como atividade sujeita ao ISS, cabe analisarmos se a previsão legal está de acordo com o conceito constitucional de serviço.

Rememorando os conceitos dos itens anteriores, temos que a licença do uso de software consiste em uma autorização do criador do software para o usuário utilizar o programa de computador, de acordo com algumas condições previamente fixadas. Nesse sentido, não há uma obrigação de fazer pelo criador do software, mas tão somente uma obrigação de dar.

Em outras palavras, quando um usuário celebra um contrato de licença de uso de software padronizado seu interesse é apenas acessar as funcionalidades do software e, portanto, não haveria uma obrigação de fazer, como ocorre, por exemplo, nas contratações envolvendo desenvolvimento de software específico para as necessidades do contratante/usuário.

Nesse ponto, cabe ressaltar que o legislador incluiu na lista de serviços anexa a LC 116/2003, em item diferente a licença de uso e desenvolvimento de software (item 1.01), reconhecendo assim a sua distinção.

Importante deixar claro que ainda que haja um esforço intelectual humano na criação de um software padronizado, que será licenciado para diversos usuários, o esforço humano por si só não é objeto da licença de uso, pois esse esforço ocorre antes de disponibilizada a licença e não possui relação direta com os usuários licenciados, que desejam única e exclusivamente utilizar um software pronto.

Portanto, no contrato de licença de uso de software padronizado não há uma obrigação de fazer que possibilite a incidência do ISS, de modo que, apesar de a licença de uso de software cumprir com os requisitos necessários para incidência do ISS (definida em Lei Complementar e não compreendido no

campo de incidência do ICMS), falta a essa atividade a característica de prestação de serviço necessária à incidência do ISS.

Após a análise do software padronizado e a não incidência do ISS, faz-se necessária também a análise dos softwares desenvolvidos e/ou customizados e se estes envolvem prestação de serviços passível de tributação pelo ISS.

O contrato de desenvolvimento de software tem como objetivo a elaboração de programa para atender as necessidades específicas do usuário/contratante, seja para fins de uso próprio ou comercialização. Para esse tipo de software, de acordo com o artigo 4º da Lei 9.609/1998, como regra geral, os direitos patrimoniais relativos ao software desenvolvido pertencerão exclusivamente ao contratante do desenvolvimento, sendo possível, todavia, estipular em contrato que o software desenvolvido pertença ao desenvolvedor ou mesmo a ambas as partes.

O contrato de customização de software, por sua vez, tem como objetivo a adaptação de softwares ofertados ao mercado, de modo a adaptá-los às necessidades do usuário/contratante. Diferente do contrato de desenvolvimento, por ser apenas uma adaptação a um software já existente, em regra, os direitos patrimoniais sobre a adaptação pertencerão ao customizados/contratada (salvo se disposto de forma diferente em contrato).

Nesse sentido, em razão das atividades de desenvolvimento e customização de software envolverem um esforço humano para produção de um bem imaterial, mediante pagamento, podemos dizer que elas se enquadram no conceito de prestação de serviços sujeitos à incidência do ISS. Porém, importante reforçar que não deverá ser tributado o software, mas sim a prestação de serviços de desenvolvimento e/ou customização, sob pena de tributar o bem imaterial e não a prestação de serviços em si.

Por fim, também é necessário analisar o negócio jurídico envolvendo o *software as a service* (SaaS).

Conforme já estudado, no modelo SaaS, o software é executado em nuvem, razão pela qual é necessária a contratação pelo fornecedor do software serviços de infraestrutura, processamento, armazenamento de dados e recursos computacionais necessários para a utilização do SaaS.

Assim, podemos dizer que o SaaS não se limita a um contrato típico de licença de software, conforme previsto na Lei 9.609/1998, pois é composto por diversos elementos negociais indissociáveis (atualização e manutenção do software, serviço de backup, infraestrutura em nuvem, etc.), de modo que deve ser considerado como um contrato misto (único em complexo).

Em contratos mistos há uma grande dificuldade em determinar quais as normas que serão aplicáveis, inclusive para fins de definição da tributação do negócio jurídico.

Parte da doutrina e também da jurisprudência defende que a definição do tratamento tributário aplicável a um determinado negócio jurídico deve se dar a partir da verificação da finalidade específica preponderante em referido negócio.

Desta forma, partindo da premissa que só haverá incidência do ISS sobre a finalidade preponderante do negócio jurídico, temos que no caso do SaaS, cuja finalidade preponderante é a licença de uso do software (obrigação de dar) não há que se falar na incidência do ISS.

Uma alternativa que nos parece plausível para tributação do SaaS e/ou do direito de uso do software (já que vimos que não incidiria ICMS ou ISS), seria o exercício da competência residual da União Federal, prevista no artigo 154, inciso I, da Constituição Federal.

Cabe ressaltar, todavia, que a instituição de imposto específico pela União para tributação sobre a atual economia digital e, por consequente para as operações de licença de uso de software, incluindo SaaS, pode não se mostrar suficiente para resolver um problema que temos hoje e que, por ora, possui uma decisão do STF que entende pela tributação da licença de software pelo ISS, conforme veremos a seguir.

Em relação à possibilidade de ampliação do critério matéria, seja do ICMS ou do ISS, por meio de emenda constitucional, não nos parece a alternativa mais viável, visto que pode acarretar reflexos na tributação de outras operações distintas.

3. Supremo Tribunal Federal e o atual entendimento sobre tributação de Software

O Supremo Tribunal Federal (STF), no julgamento de duas Ações Diretas de Inconstitucionalidade (ADIs 1.945/MT e ADI 5.695/MG) decidiu, por maioria de votos, que o tributo que deve incidir sobre o licenciamento e a cessão de direito de uso de softwares é o Imposto Sobre Serviços (ISS), descartando, assim, a possibilidade de incidência do Imposto sobre Circulação de Mercadorias e Serviços (ICMS) sobre essas operações.

A ADI 1.945/MT, protocolada pelo Movimento Democrático Brasileiro, questionava a legislação do Estado do Mato Grosso, a qual previa a tributação

pelo ICMS nas operações envolvendo softwares. A ADI 5.695/MG, proposta pela Confederação Nacional de Serviços (CNS), por sua vez, contestava um decreto do Estado de Minas Gerais, que também previa que as vendas de programas de computador fossem tributadas pelo ICMS.

Como resultado do julgamento, as referidas leis estaduais foram declaradas inconstitucionais, isto porque, se reconhecida a cobrança do ICMS e do ISS, ocorreria bitributação. Desta forma, por maioria, o STF decidiu que as vendas de softwares, sejam eles padronizados, customizados ou por encomenda, ficam sujeitas ao Imposto sobre Serviços (ISS).

Para facilitar a análise dos votos e entendimentos dos Ministros, segue abaixo a tabela comparativa.

Ministros	Incidência do ICMS	Incidência do ISS
Dias Toffoli	NÃO	SIM
Alexandre de Moraes	NÃO	SIM
Luis Robeto Barroso	NÃO	SIM
Rosa Weber	NÃO	SIM
Ricardo Lewandowski	NÃO	SIM
Luiz Fux	NÃO	SIM
Edson Fachin	SIM	NÃO
Carmen Lucia	SIM	NÃO
Nunes Marques	SIM	NÃO
Gilmar Mendes	SIM	SIM
Marco Aurélio	NÃO	NÃO

A votação totalizou 7 (sete) votos a favor da incidência do ISS, contra 4 (quatro) votos a favor da incidência do ICMS sobre o licenciamento e cessão de uso de programas de computador.

O Ministro Dias Toffoli, relator de uma das ações, julgou pela incidência exclusiva do imposto municipal (ISS) para o licenciamento e cessão de direito de uso de programas de computador. Segundo o ministro, os programas de computador não são mercadorias, eis que são utilitários e imateriais, o que excluiria a incidência do ICMS.

Embora os ministros Alexandre de Moraes, Luís Roberto Barroso, Rosa Weber, Ricardo Lewandowski e Luiz Fux tenham seguido o voto do relator, ministro Dias Toffoli, cada um dos ministros apresentou seus argumentos.

O ministro Alexandre de Moraes julgou pela incidência do imposto municipal, para ele os softwares são pacotes de serviços e, portanto, não poderia incidir ICMS.

O ministro Luís Roberto Barroso em seu voto explicou que, na disponibilização online, sem cessão definitiva do programa de computador, o usuário remunera o detentor da licença, mediante pagamentos periódicos em regime de assinatura, de modo que não há transferência da titularidade do bem. O programa de computador não é vendido, portanto não há tecnicamente circulação de mercadoria que possibilite a incidência do ICMS.

A ministra Rosa Weber entendeu que o licenciamento do uso de computador não se confunde como uma operação de circulação de mercadoria, em especial na condição de artefato intelectual, regido pelo mesmo regime às obras literárias (legislação de direitos autorais e conexos).

O ministro Ricardo Lewandowski em seu voto, para afastar o ICMS e justificar a incidência do ISS, trouxe como exemplo os programas que vêm instalados nos smartphones e disse que quando os consumidores adquirem um software não estão adquirindo uma mercadoria, um bem corpóreo, mas estão comprando um serviço, que pode ser objeto de diversas atualizações.

O ministro Luiz Fux julgou, assim como o ministro Dias Tofolli, julgou pela incidência exclusiva do ISS nas operações com software. O ministro em seu voto rememorou julgados de sua relatoria sobre a incidência de ISS nos planos de saúde.

Para o ministro Edson Fachin, os programas de computador são mercadorias, e, portanto, o ICMS deve incidir. O ministro entendeu que os softwares são produtos de criação intelectual e que, quando esta criação é produzida em série (em massa) para ser comercializada, a destinação e o objetivo da operação passam a ser a circulação, a venda e o lucro, incidindo o ICMS.

A ministra Cármen Lúcia entendeu pela tributação pelo ICMS nas operações mercantis que façam circular licença ou cessão de uso de programas de computador e afirmou que os programas de computador não são equivalentes a uma prestação de serviços.

O ministro Nunes Marques entendeu que o software se configura como um bem (mercadoria), ainda que seja virtual e, por isso, o ICMS deve incidir. “É um produto pronto e acabado (...) colocado em circulação”.

O ministro Gilmar Mendes entendeu pela incidência dos dois tributos, sendo a tributação pelo ISS sobre softwares desenvolvidos de forma personalizada e pelo ICMS sobre software padronizado.

O ministro Marco Aurélio, por sua vez, adotou um posicionamento diferente dos demais ministros, pois além de afastar o licenciamento e a cessão do direito de uso de software do campo de incidência do ICMS, também afastou o licenciamento e a cessão do direito de uso de software do campo de incidência do ISS, visto que não há prestação de serviço em si (obrigação de fazer).

Em sessão realizada em dezembro de 2021 o STF finalizou o julgamento do RE 688.223/PR, em sede de repercussão geral (Tema 590), e reafirmou o entendimento de que incide o ISS sobre contratos de licenciamento ou cessão de usos de programas de computador (software) desenvolvidos para clientes personalizados.

Apresentadas as decisões acima e os votos dos ministros do STF, importante esclarecer que esta análise possui somente o condão de analisar a hipótese de incidência dos tributos (ICMS e ISS) e verificar se seria possível a tributação dos negócios jurídicos envolvendo software. Apesar do posicionamento do STF, reiteramos nosso entendimento no sentido de que os negócios jurídicos envolvendo software (seja ele de qualquer modalidade, incluindo SaaS) não estão sujeitas à incidência do ICMS e do ISS, pelos motivos expostos acima, cabendo à União Federal em sede de competência residual tributar os negócios jurídicos atuais envolvendo tecnologia.

Considerações finais

O tema relativo à tributação da licença de uso de *software* em todas as suas modalidades é complexo e controverso, sendo que, apesar de referido negócio jurídico não possuir as características necessárias tanto à incidência do ICMS quanto do ISS, fato é que o STF recentemente assentou o entendimento que incide ISS sobre os contratos que envolvem licenciamento e/ou cessão de uso de programa de computador.

Conforme vimos ao longo do presente texto, entendemos que as operações de licença e/ou cessão de uso de programas de computador (software) não configuram “operações relativas à circulação de mercadorias” e/ou “serviços de qualquer natureza”, conforme definidos em lei complementar e, portanto, não estão sujeitas à incidência do ICMS ou do ISS.

Diante das alternativas para sanar tal problema, que hoje se vê em tese solucionado pelo STF por uma premissa equivocada de que já existe previsão de tributação de licença e/ou cessão de uso de programa de computador pelo ISS (conforme lista de serviços da LC 116/2001, temos que o exercício da com-

petência residual da União, alinhada a uma reforma tributária mais ampla, visando simplificar o modelo de tributação de bens e serviços, olhado de uma forma mais apurada para as novas tecnologias e o impacto na economia, é a melhor alternativa para mitigar as discussões que existem e que estão por vir, geradas pela era digital que estamos vivendo e que só tem a crescer.

Enquanto não implementadas eventuais alterações legislativas, todavia, o contribuinte continuará sujeito à tributação do software como se serviço fosse.

Referências

ALBUQUERQUE, Roberto Chacon de. A propriedade informática. 1ª edição. Campinas: Russel Editores, 2006.

MELL, Peter; GRANCE, Timothy. *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Special Publication 800-145. Gaithersburg, MD, US: NIST. National Institute of Standards and Technology, Sept. 2011.* <<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial-publication800-145.pdf>> (tradução livre).

MELO, José Eduardo Soares de. ICMS: Teoria e prática. 12ª edição. São Paulo: Dialética, 2012.

CARRAZZA, Roque Antônio. ICMS. 14ª edição, São Paulo: Malheiros, 2009.

CARVALHO, Paulo de Barros. Direito tributário: Linguagem e Método. 6ª edição. São Paulo: Noeses, 2015.

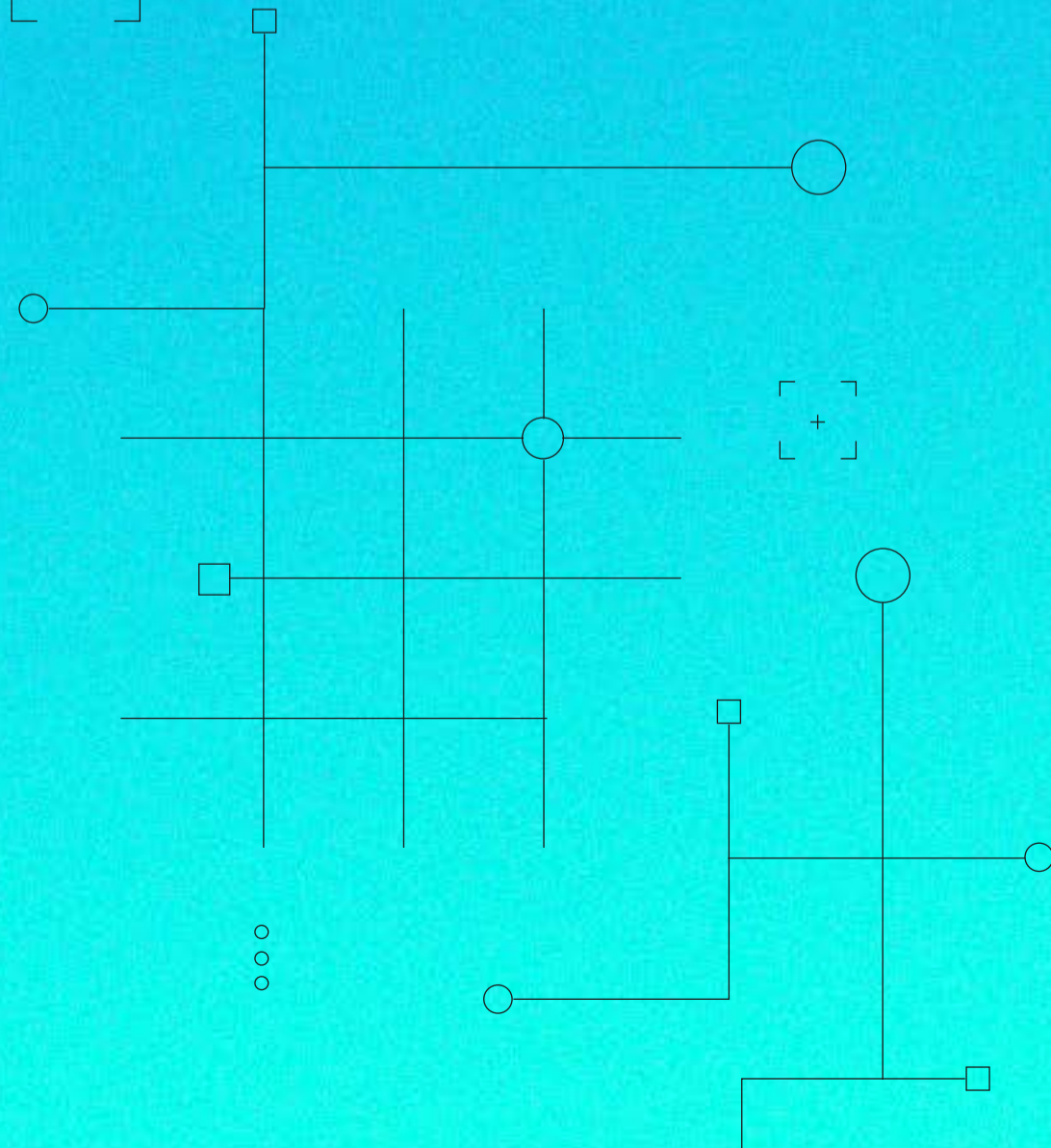
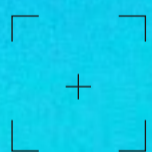
BARRETO, Aires Fernandino. *ISS na Constituição e na Lei*. 3ª edição. São Paulo: Dialética, 2009.

MACHADO, Hugo de Brito. *Curso de Direito Tributário*. 33ª edição. São Paulo: Malheiros, 2012.

HARADA, Kyioshi. ICMS: doutrina e prática. 1ª edição. São Paulo: Atlas, 2017.

Os criptojogos “pay-to-play-to-earn” enquanto valores mobiliários carentes de regulação no Brasil

MARCELO BATISTA GOMES DA CRUZ



Sumário: Introdução. 1. Jogos e criptojogos. 2. Os criptojogos “pay-to-play-to-earn” enquanto valores mobiliários. 3. Necessidade de regulação. Considerações finais. Referências.

Introdução

Em obra publicada no ano de 2004, James Newman destacou o desinteresse da comunidade acadêmica pelos jogos eletrônicos, atribuindo-o ao fato de que o objeto de estudo em questão era comumente visto como mero produto infantil ou mídia inferior e destacando que até parte da indústria de *games* à época se mostrava envergonhada quanto a seu ramo de atuação (NEWMAN, 2004, p. 5). Por certo, o tratamento atribuído aos jogos eletrônicos ganhou contornos de maior seriedade desde então, na medida em que, por um lado, o propósito lúdico dos *games* se mostrava aplicável a diversas idades² e, por outro lado, novos aspectos do fenômeno passaram a receber maior atenção pública³. Dentre tais aspectos, destaca-se a exploração econômica.

Em 2021, a indústria de jogos eletrônicos apresentou receita superior a 180 bilhões de dólares (NEWZOO, 2021), valor que, considerando a cotação da moeda no início de 2022, equivale, aproximadamente, a um trilhão de reais. Essa métrica fez da indústria de softwares de entretenimento a sexta mais lucrativa do mundo no período (TOTTOC, 2021), superando setores como o imobiliário e o alimentício.

Ainda assim, é de se notar que o desinteresse inicial pela indústria não desapareceu por completo, sobretudo no campo estatal, tendo em vista a ausência ou insuficiência de regulamentações específicas para os diversos desdobramentos do fenômeno dos “*games*” no Brasil. O Projeto de Lei nº 2.796/2021 é uma tentativa de criação do “marco legal para a indústria dos jogos eletrôni-

1. Bacharel em Direito pela Universidade de São Paulo (USP). Pós-graduando em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ), Instituto de Tecnologia e Sociedade (ITS Rio) e Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Assistente jurídico na 12ª Câmara de Direito Criminal do Tribunal de Justiça do Estado de São Paulo (TJSP).

2. Pesquisa publicada na plataforma Statista e baseada em dados de treze países demonstrou que 43% dos jogadores, em 2017, possuíam mais de trinta e cinco anos de idade. Disponível em: <https://www.statista.com/statistics/722259/world-gamers-by-age-and-gender/>. Acesso em: 04/01/2022.

3. Em tese publicada em 2014, Fabiano Alves Onça selecionou matérias jornalísticas da década de 2010 que demonstravam a subdivisão da visibilidade social dos jogos eletrônicos em cinco categorias: estranhamento quanto aos comportamentos dos jogadores; fascínio em relação aos benefícios dos *games* para a vida humana; interesse econômico; interesse pelas aplicabilidades não-lúdicas e apreciação cultural. (ONÇA, 2014, pp. 16-22).

cos”, mas além de não haver previsão quanto à aprovação da medida, seu conteúdo mostra-se excessivamente generalista e de abrangência insuficiente, sobretudo no que tange às novas tendências tecnológicas do mercado.

Como comumente ocorre ante o surgimento ou crescimento de novas tecnologias, o afloramento de questões inéditas para os operadores do Direito também se faz presente na indústria dos *games*. Dentre referidas inovações, interessa ao presente artigo a expansão dos “criptojogos”, termo que, doravante, designará os jogos eletrônicos que fazem uso da tecnologia *blockchain*⁴.

Conforme será demonstrado, a adoção de criptoativos como “moeda corrente” do jogo eletrônico conduz à integração entre a economia virtual dos criptojogos e a economia real do mundo físico, transformando os jogos em um produto economicamente explorável não apenas por seus desenvolvedores e distribuidores, mas também pelos próprios usuários. Simultaneamente, esse novo interesse no jogar desperta a atenção tanto de atores consolidados da indústria dos *games* como também de novos desenvolvedores, os quais concentram na promessa do lucro ao usuário sua principal estratégia de captação de recursos.

Nesse âmbito, o jogo *Axie Infinity* se tornou um fenômeno em 2021, de modo que, em julho do referido ano, registrava receita anual de mais de um bilhão de dólares a partir de uma base de usuários de seiscentos mil jogadores (YAP, 2021). Não à toa, cada vez mais jogos de semelhante estratégia se tornam populares: a plataforma de monitoramento de criptoativos, *CoinMarketCap*, registra, no início de 2022, mais de trezentas criptomoedas voltadas a jogos eletrônicos⁵.

O fenômeno impressiona pelos números, mas também por suscitar expressiva quantidade de questões jurídicas ainda pouco exploradas no Direito brasileiro e, em sua maioria, carentes de regulação estatal. Dentre elas, o presente trabalho dará destaque à possibilidade de enquadrar parte dos criptojogos “*play-to-earn*” (modelo por meio do qual o jogador obtém ganhos financeiros ao jogar o *game*) como espécie de contrato de investimento coletivo, sujeito à regulação da Comissão de Valores Mobiliários (CVM). Em seguida, serão abor-

4. Em uma definição mais detalhada: “Criptogames são jogos eletrônicos com uma arquitetura de banco de dados distribuído (distributed ledger) total ou parcialmente, que opera em uma rede de criptomoedas, dando aos jogadores a propriedade comprovada dos bens virtuais que eles controlam. Isso também permite aos jogadores trocar bens virtuais por criptomoedas, as quais podem ser trocadas por moeda real”. (SCHOLTEN et al., 2019, p. 379, tradução livre).

5. Informação disponível em: <https://coinmarketcap.com/pt-br/view/gaming/>. Acesso em 05/01/2021.

dados os problemas da ausência de regulação estatal do assunto, bem como eventuais caminhos para solucioná-los.

1. Jogos e criptojogos

Em relação à interação econômica entre produto e usuário, os jogos eletrônicos podem ser divididos em três categorias: *pay-to-play* (P2P), *free-to-play* (F2P) e *play-to-earn* (P2E). A primeira classificação designa o que se poderia chamar de “modelo tradicional” da indústria de *games*, tendo em vista que, conforme o próprio nome sugere, o usuário paga pela aquisição de uma cópia ou pela permissão de acesso ao jogo. Trata-se da mera compra e venda de produto ou serviço de entretenimento, praticada largamente por empresas gigantes do mercado como Nintendo, Sony e Microsoft. A modalidade *pay-to-play* também pode incluir a venda de DLC’s (downloadable content)⁶ e de serviços que permitem ao usuário “jogar online”, como o “PlayStation Network” ou o “Xbox Game Pass”. Um clássico exemplo dessa categoria de jogos seria a franquia “Grand Theft Auto (GTA)”.

Os jogos *free-to-play* ou “gratuito para jogar”, por sua vez, não exigem, à primeira vista, nenhum dispêndio financeiro por parte do usuário que deseje desfrutar de seu conteúdo (OLIVEIRA, 2017, p. 21). Referidos jogos podem ser concebidos sob diversas formas: jogos que disponibilizam gratuitamente parte do conteúdo e cobram pelo acesso ao conteúdo completo (por exemplo: “Angry Birds”); *games* que ofertam uma versão gratuita com funções limitadas e uma versão paga com funcionalidade completa (por exemplo: “Cartola FC”); jogos que se monetizam através de propagandas e oferecem a possibilidade de o usuário pagar para removê-las (por exemplo: inúmeros jogos para celular); *games* gratuitos que se monetizam através de microtransações para aquisição de itens (por exemplo: “League of Legends”), etc.

Por fim, os *games play-to-earn*, ou “jogue para ganhar”, se caracterizam pela possibilidade de obtenção de lucro por parte do usuário em troca de seu tempo de jogo. A página “Play to Earn Online Magazine”, que se descreve como sendo formada por “cidadãos do metaverso que promovem notícias e conteúdo editorial sobre jogos *blockchain*, criptoarte e tokens não-fungíveis” (PLAY TO EARN MAGANIZE, 2020), explica que o modelo de negócios *play-to-earn*

6. Trata-se de conteúdo “extra” de determinado jogo que pode ser acessado pelo jogador que, após ter adquirido o produto principal, pagar um preço adicional.

se baseia na ideia de permitir ao jogador participar da economia do jogo para criar valor aos outros jogadores e aos desenvolvedores. A ideia é premiar o tempo gasto no jogo com ativos *in-game*⁷, cuja possibilidade de comercialização lhes atribui valor econômico.

Essa dinâmica não é inédita. O jogo “Everquest”, lançado em 1999, já apresentavam um mundo virtual (“Norrath”) com economia própria e interconectada informalmente à economia real por meio de transações intermediadas por plataformas de leilão online, como o Ebay (CASTRONOVA, 2001, pp. 27-28). Conforme pesquisa realizada por Edward Castronova quando o jogo era o mais popular de seu segmento, Everquest proporcionava aos seus jogadores uma renda de aproximadamente três dólares e meio por hora, valor que, considerando o tempo que os usuários mais assíduos despendiam no *game*, poderia somar mais de mil dólares por mês (CASTRONOVA, 2001, p. 30).

Significativas diferenças, no entanto, separam Everquest dos criptojogos *play-to-earn* da atualidade.

Em primeiro lugar, a venda de ativos digitais por dinheiro real, por parte dos jogadores, não era funcionalidade do jogo, mas sim iniciativa dos próprios usuários, tendo em vista que a própria desenvolvedora (Sony) buscava refrear a prática (CASTRONOVA, 2001, p. 19). Parte do incômodo decorria do fato de que a empresa enxergava os ativos de Norrath como sua propriedade intelectual, aspecto que perde sentido ante a ascensão dos jogos que fazem uso da tecnologia NFT (*non-fungible token* ou tokens não fungíveis).

Nesse ponto, a fim de discorrer brevemente acerca da importância do NFT nos criptojogos, necessário despende algumas linhas para elucidar o funcionamento desse recurso⁸.

Grosso modo, *blockchain* “constitui uma tecnologia descentralizada de registro de dados (*distributed ledger* ou *decentralised ledger technology*)” (FONSECA, 2021, pp. 743) ou “um banco de dados de transações organizado cronologicamente em uma rede de computadores” (DIVINO, 2018, pp. 2776-2777 apud NALIN, 2021, p.756). Conforme Chittenden (2016, p. 10 apud BARBOSA, 2021, p.798):

7. O termo se refere àquilo que existe ou ocorre apenas dentro do universo virtual de um jogo eletrônico.

8. Características mais técnicas e detalhadas quanto ao funcionamento dos *blockchains* em jogos eletrônicos fogem ao escopo do presente artigo, no entanto, informações mais detalhadas podem ser encontradas em: MIN, Tian; WANG, Hanyi; GUO, Yaoze; CAI, Wei. *Blockchain Games: A Survey*. Shenzhen: School of Science and Engineering, The Chinese University of Hong Kong: 2019.

[...] *blockchain* é, então, um livro de registros (*ledger*), no qual se inscreve anonimamente informação, que é multiplicada ao longo de um ambiente digital (*network*), que liga os computadores de todos os participantes (*nodes*), e é regularmente atualizada, de tal modo que cada um que participe nesse *network* pode confiar que partilha os mesmos dados que o *ledger*, sem necessidade de um terceiro centralizado a validar.

A partir de tal tecnologia, o NFT surge como uma espécie de certificado que, por meio da criptografia do *blockchain*, individualiza determinado ativo, real ou digital, a fim de lhe conferir exclusividade, criar escassez e, consequentemente, permitir que se exerça sobre tal ativo o direito de propriedade (ANTE, 2021, pp. 01-02). Com o NFT, mesmo ativos de fácil acesso e reprodução, como arquivos digitais, tornam-se escassos e únicos, na medida em que possuem uma espécie de registro que suas cópias não têm.

Desse modo, um dos ativos *in-game* mais populares dos jogos eletrônicos *play-to-earn* é justamente o NFT, que assume a forma de itens ou personagens. No entanto, diferentemente do que ocorria em Everquest, a descentralização da rede *blockchain* confere ao jogador a propriedade do criptoativo, ao mesmo tempo em que o diferencia de outros ativos semelhantes do mesmo jogo.

Assim, a tecnologia afasta questionamentos sobre a impossibilidade de comercialização dos itens e personagens obtidos pelo usuário e, simultaneamente, atribui a eles, por meio de sua exclusividade, maior potencial de valor⁹. Ademais, uma vez que a possibilidade de obtenção de lucro pelo jogador faz parte do modelo de negócios dos criptojogos, os próprios desenvolvedores buscam incentivar as práticas comerciais entre usuários, tanto para atrair novos jogadores e manter os atuais quanto para cobrar taxas operacionais sobre as transações.

Outra contribuição do *blockchain* para os criptojogos é a utilização de criptomoedas como recurso de intermediação de trocas no ambiente *in-game* (CLOAD MAGANIZE, 1980, p. 02). A existência de moedas fictícias no ambiente virtual de um jogo eletrônico não possui nada de novo. Em 1980, a versão do jogo “Dungeons & Dragons” para microcomputadores já possuía um sistema

9. Não se ignora a possibilidade de questionamentos acerca da efetiva independência do jogador em relação aos desenvolvedores do jogo, tendo em vista que estes são responsáveis pela manutenção do ambiente digital que confere valor ao NFT e, ao mesmo tempo, podem tomar medidas de banimento do usuário.

de compra de itens por meio de “gold pieces”¹⁰. Por sua vez, a interação entre as moedas fictícias e os recursos financeiros reais também já se mostrava presente, como visto, na década de 1990, em jogos como Everquest. Contudo, não havia grande praticidade técnica para que o usuário desfrutasse dessa interação, tendo em vista a necessidade de recorrer a plataformas intermediárias.

Essa dificuldade, entretanto, é sanada por uma característica comum dos criptojogos, qual seja: o fato de operarem conectados a uma rede *blockchain* que lhes permite adotar como moeda virtual *in-game* uma criptomoeda, isto é, uma “moeda digital descentralizada que usa um banco de dados distribuído (*distributed ledger*) para registrar e provar sua propriedade” (SCHOLTEN et al., 2019, p. 380). Assim, os criptojogos costumam apresentar conectividade com uma carteira digital de criptoativos de titularidade do jogador, permitindo-lhe armazenar e transferir as criptomoedas obtidas por meio das transações que realiza no jogo.

Portanto, uma vez que referidas moedas estejam listadas em alguma corretora de criptoativos ou plataforma de função semelhante, os recursos obtidos pelo jogador no mundo virtual do jogo estão a poucos “cliques” de serem trocados por moeda real. Referida corretora, ademais, pode ser uma *exchange* descentralizada (DEX), permitindo negociações diretas entre os usuários através da rede *blockchain*, sem a necessidade, portanto, da intervenção direta de atores intermediários. Ademais, a própria criptomoeda do jogo (*gamecoin*) está sujeita a variações de valor atreladas à demanda pelo ativo, de modo que até mesmo não-jogadores que adquiram uma *gamecoin* podem obter lucros indiretos de determinado criptojogo.

Por fim, outro aspecto que afasta os criptojogos de outros jogos *play-to-earn* do passado são os significativos crescimentos do número de usuários. Quando Castronova desenvolveu sua pesquisa sobre Everquest, o jogo contava com 400 mil usuários (CASTRONOVA, 2001, p. 08), já o criptojogo “Thetan Arena” possuía, no final de 2021, três milhões de jogadores (THETAN ARENA OFFICIAL, 2022). Números como esse, somados à maior difusão de referidos jogos¹¹ em um mundo muito mais conectado, demonstram que os jogos *play-*

10. CLOAD MAGAZINE INC. *Dungeons and Dragons*. Califórnia: 1980, p. 02. Disponível em: [http://www.gametronek.com/site/rubriques/tandy/FAQs/CLOAD%20Magazine%201980-05%20\(1980\)\(CLOAD%20Magazine%20Inc\).pdf](http://www.gametronek.com/site/rubriques/tandy/FAQs/CLOAD%20Magazine%201980-05%20(1980)(CLOAD%20Magazine%20Inc).pdf). Acesso em: 08/01/2022.

11. Veja-se os números de criptoativos “*gamer*” mencionados no início deste artigo.

-to-earn não são mais um mero nicho de difícil geração de valor, mas sim uma tendência da contemporaneidade.

Assim, estando definido o escopo do trabalho e a relevância do tema, passa-se a abordar as questões jurídicas que o permeiam.

2. Os criptojogos “pay-to-play-to-earn” enquanto valores mobiliários

Embora a função tradicional de jogos seja o propósito lúdico, não há qualquer prejuízo em atribuir-lhes objetivos adicionais que proporcionem maiores benefícios à vida humana. É cada vez mais comum a utilização de jogos eletrônicos como instrumentos de ensino, seleção de profissionais, tratamento de saúde etc. No entanto, a partir do momento em que determinada atividade passa por reconfigurações que lhe transformem em fenômeno diverso, também é passível o questionamento sobre as novas implicações dessa atividade e a eventual necessidade de alterar o estatuto jurídico que lhe é atribuído. Visto isso, passa-se a questionar se os criptojogos podem ser vistos como forma de investimento financeiro e as implicações de tal concepção.

Sendo assim, no que tange à função econômica dos criptojogos *play-to-earn*, observa-se que o jogador que desejar obter ganhos financeiros pode, em geral, fazê-lo de três formas: (i) comprando *gamecoins* e apostando em sua valorização; (ii) obtendo NFT's *in-game* que possam ser trocados por criptomoedas (como ocorre em jogos como “Cryptokitties”) e (iii) recebendo criptomoedas ao jogar, seja em razão de suas habilidades (como no jogo “Town Star”) ou simplesmente como prêmio pelo tempo despendido no jogo (como no *game* “Bomb Crypto”).

Não há dúvidas de que a primeira modalidade supracitada configura típica atividade de investimento (ou de especulação) financeiro, mas poder-se-ia argumentar que o mesmo não se aplica às outras duas modalidades. Não se confundem as operações do mercado de valores mobiliários com a mera compra e venda de um bem que gere obtenção de lucro e menos ainda com a obtenção de recursos em troca do tempo e das habilidades do jogador.

Todavia, é necessário pontuar que muitos criptojogos não se enquadram na modalidade *free-to-play*, pois apenas permitem que o usuário comece a jogar se possuir determinado item ou personagem, em regra concebidos em forma de NFT's. Tais ativos, por sua vez, apenas podem ser obtidos mediante pagamento da criptomoeda atrelada ao *game*. Em referidos jogos, portanto,

não há um simples sistema *play-to-earn*, mas, na verdade, uma modalidade *pay-to-play-to-earn (P2P2E)*.

Em suma, as etapas mais comuns de implementação de um criptojogo *P2PE2* na comunidade “*gamer*” são as seguintes: após criarem o jogo total ou parcialmente, os desenvolvedores geram uma *gamecoin* específica e a produzem em determinada quantidade; em seguida, o projeto é anunciado publicamente por meio de um “*white paper*”¹², como forma de atrair os jogadores-investidores, em uma espécie de captação de recursos; a seguir, a aquisição da criptomoeda é disponibilizada aos interessados, o que pode ocorrer sob diferentes modalidades de oferta pública, quais sejam: *Initial Coin Offering (ICO)*; *Initial Exchange Offering (IEO)*; *Initial Farm Offering (IFO)* e *Initial DEX Offering (IDO)*.¹³.

Caso a meta de captação seja atingida a partir da venda das *gamecoins*, o desenvolvimento do jogo prossegue; por fim, após o lançamento do *game*, os usuários podem utilizar as criptomoedas adquiridas para obter os personagens ou itens necessários para começar a jogar e a lucrar (ou a perder os valores investidos)¹⁴.

O que chama atenção, contudo, é que não há qualquer notícia de que referido processo, ao atingir potenciais investidores brasileiros, esteja sujeito ao controle da Comissão de Valores Mobiliários e às regras impostas pela Lei 6.385/76.

Com efeito, a lei em questão define como valores mobiliários sujeitos a regime legal específico: “quando ofertados publicamente, quaisquer outros títulos ou contratos de investimento coletivo, que gerem direito de participação, de parceria ou de remuneração, inclusive resultante de prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros”¹⁵.

12. *White paper*, no universo dos criptoativos, é um documento que visa elucidar as bases de determinado projeto e atrair potenciais investidores, ao “explicar qual é o problema a ser resolvido, como será resolvido, o financiamento e a quantidade de token que estará disponível. Além de um roteiro de implantação do projeto, entre outros detalhes dignos de nota” (BIT2ME ACADEMY. 2022).

13. Uma análise aprofundada das diferenças e aspectos técnicos de tais modalidades foge ao escopo do presente artigo. O que importa, contudo, é compreender que todos tratam da oferta pública de criptoativos através da rede *blockchain*, seja por meio de *exchanges* centralizadas ou descentralizadas (ROCHA, 2021).

14. Um exemplo do processo descrito pode ser observado no *white paper* dos critojogos Mouse Haunt (disponível em: <https://whitepaper.mousehaunt.com/universe/>. Acesso em: 08/01/2022), CryptoGuards (disponível em: <https://whitepaper.cryptoguards.me/roadmap>. Acesso em: 08/01/2022), Zodiacs (disponível em: <https://s.ladcdn.com/60d5ad345932a600139ca4b2/zodiacs-whitepaper--20211011100244.pdf>. Acesso em: 08/01/2022), Guild of Guardians (disponível em: <https://whitepaper.guildofguardians.com/>. Acesso em: 08/01/2022) e Space Crypto (disponível em: <https://docs.spacecrypto.io/guides/readme>. Acesso em: 08/01/2022).

15. Lei 6.385/76. Artigo 2º, inciso IX.

A norma em comento foi incluída no diploma legal citado por meio da Lei 10.303/01, que visava “alargar o conceito de valores mobiliários para hipóteses que, embora não expressamente previstas em lei, deveriam se submeter à regulação da CVM em função de sua substância” (RABELLO; MAFRA, 2019, p. 224). O regramento foi inspirado no chamado “*Howey Test*”, desenvolvido pela Suprema Corte dos Estados Unidos para verificar o enquadramento de determinado título na categoria de valor mobiliário. Conforme Rabello e Mafra (2019, p. 224), referido teste determinava que o valor mobiliário (*security*) seria assim considerado caso fosse “um investimento em dinheiro (“*investment of money*”) por investidor no contexto de investimento coletivo (“*commom enterprise*”) que gerasse expectativa de ganho (“*expectation of profits*”) derivados unicamente do esforço de terceiros (“*solely from the effort of others*”)”.

Ao adaptar o “*Howey Test*” para o contexto do direito brasileiro, a CVM propôs o enfrentamento dos casos práticos a partir de cinco indagações: (a) Buscou-se captar recursos de investidores por meio de uma oferta pública? (b) Os investidores aportaram (ou foram chamados a aportar) dinheiro ou outro bem suscetível de avaliação econômica? (c) Os recursos captados na oferta (ou que se buscava obter com a oferta) foram (ou seriam) aplicados em um empreendimento coletivo? (d) O aporte foi (ou seria) feito na expectativa de lucros, decorrentes de um direito de participação, de parceria ou alguma forma de remuneração (inclusive resultante de prestação de serviços)? (e) Os resultados esperados do investimento adviriam, exclusiva ou preponderantemente, dos esforços do empreendedor ou de terceiros? (CVM, 2020).

Visto isso, ao submeter-se os criptojogos *P2P2E* às indagações acima, percebe-se, de pronto, que a primeira e a segunda pergunta podem ser respondidas de forma afirmativa. Com efeito, o art. 3º, inciso IV, da Instrução CVM 400/2003 define como oferta pública:

Utilização de publicidade, oral ou escrita, cartas, anúncios, avisos, especialmente através de meios de comunicação de massa ou eletrônicos (páginas ou documentos na rede mundial ou outras redes abertas de computadores e correio eletrônico), entende-se como tal qualquer forma de comunicação dirigida ao público em geral com o fim de promover, diretamente ou através de terceiros que atuem por conta do ofertante ou da emissora, a subscrição ou alienação de valores mobiliários.

Tendo em vista o processo de captação de recursos acima enunciado, observa-se que não raras vezes o *white paper* do jogo cita explicitamente mencio-

na o modelo de oferta pública adotado (como o IDO)¹⁶ ou simplesmente anuncia a data aproximada em que serão disponibilizados para venda do público em geral as criptomoedas. Portanto, não restam dúvidas de que haja oferta pública que chama investidores a aportarem dinheiro no projeto.

Por sua vez, quanto à existência de empreendimento coletivo ou comum (terceira indagação proposta pela CVM), faz-se necessário verificar se o valor mobiliário foi oferecido a “diversas pessoas, que partilham um mesmo conjunto de ativos, com a expectativa de auferir lucros decorrentes dos esforços do promotor do negócio ou do instrumento que está sendo ofertado” (EIZIRIK et al., 2019, pp. 72-73 apud CVM, 2020). Nesse aspecto, tendo em vista que o modelo de jogos *play-to-earn* visa justamente o maior envolvimento dos jogadores na economia do jogo, prometendo-lhes expectativa de lucro por meio, dentre outras causas, da maior demanda da *gamecoin* ofertada pelos desenvolvedores, parece que há a existência de empreendimento comum.

É de se ponderar o argumento de que, embora haja processos de oferta públicas de criptoativos para lançamentos de critojogos, tratar-se iam de meros *utility tokens*, isto é, um ativo virtual que “confere ao investidor acesso à plataforma, projeto ou serviço, nos moldes de uma licença de uso ou de créditos para consumir um bem ou serviço” (CVM, 2017). No entanto, a CVM não descarta que, a depender de sua configuração, os *utility tokens* podem também ser considerados como valores mobiliários (CVM, 2017), análise que há de ser feita caso a caso.

Quanto à quarta indagação proposta pela CVM, não se pode afirmar que todo o jogador que aloque recursos financeiros para acessar um critojogo *P2P2E* o faça com intenção de lucro, tendo em vista que, a despeito de suas peculiares características, tais jogos preservam, ainda que parcialmente, seu caráter lúdico. No entanto, também não se pode ignorar que os *white papers* de referidos critojogos enfatizam a preocupação com a economia do *game* e com as formas de obtenção de lucro por parte do jogador¹⁷.

Por outro lado, a CVM (2019) já entendeu que:

[...] para a caracterização do contrato de investimento coletivo, o lucro esperado pode estar associado tanto aos resultados do em-

16. É o que se observa no *white paper* do critojogo Space Crypto (disponível em: <https://docs.spacecrypto.io/guides/readme>. Acesso em: 08/01/2022).

17. Como exemplo, cita-se o *white paper* do critojogo Star Atlas, disponível em: <https://staratlas.com/white-paper.pdf>. Acesso em: 10/01/2022.

preendimento a ser desenvolvido, quanto à valorização do título ou contrato que representa o investimento. Nessa segunda hipótese, não se pode falar em contrato de investimento coletivo quando a expectativa de valorização é associada a fatores externos, que fogem do controle do empreendedor, mas apenas quando o promotor do empreendimento ou um terceiro indicam que envidarão esforços com o objetivo de – ou tendentes a – valorizar o investimento inicialmente realizado.

Sendo assim, poder-se-ia argumentar que os rendimentos obtidos pelos jogadores de criptojogos estão sujeitos meramente à lei da oferta e demanda, não havendo que se falar na intervenção intermediária dos desenvolvedores. Contudo, como demonstrado e conforme o entendimento acima citado, os *white papers* exibem um projeto de desenvolvimento do *game* que muitas vezes traz planejamento de longo prazo a fim de atrair novos jogadores ao longo do tempo e de manter o jogo interessante e lucrativo para seus usuários. Portanto, ainda que prevaleça a necessidade de avaliação casuística, não parece irrazoável compreender que a quarta indagação acima proposta também merece resposta afirmativa.

Por fim, no que tange à última indagação proposta pela CVM (“Os resultados esperados do investimento adviriam, exclusiva ou preponderantemente, dos esforços do empreendedor ou de terceiros?”), é necessário avaliar os esforços dos jogadores-investidores em contrapartida aos dos desenvolvedores-empresendedores para determinar se há ou não preponderância dos últimos em relação aos primeiros. Portanto, a análise se torna, mais uma vez, casuística.

Ainda assim, algumas considerações merecem ser tecidas a esse respeito. Ao acompanhar entendimento da jurisprudência norte-americana, a CVM determinou que “uma participação pouco expressiva do investidor não descaracteriza o contrato de investimento coletivo, desde que os esforços de terceiros sejam os predominantes” (CVM, 2019).

Nesse sentido, é certo que o usuário de criptojogos possui o papel tanto de financiar parte do projeto quanto de, principalmente, mantê-lo “vivo”, isto é, financeiramente interessante para novos e atuais investidores. O valor da *gamecoin* atrelada ao criptojogo é o cerne de sua atratividade econômica, tendo em vista que ao jogador-investidor não interessa possuir criptoativos que não possa trocar por expressiva quantia de moeda real. Tal valor, por sua vez, depende da demanda pela *gamecoin* no mercado secundário, de modo que um criptojogo *P2P2E* que não suscita a procura de novos jogadores ou o reinves-

timento de jogadores antigos tende a sobreviver apenas do fator lúdico. Esse fator, no entanto, é secundário para jogadores-investidores e pode ser facilmente superado por outros jogos *free-to-play* do mercado ou *games* “não-cripto”, que prescindem dos trâmites de conectividade mediante carteira de ativos digital.

Portanto, embora o interesse e envolvimento dos jogadores seja fundamental para a manutenção do jogo, cabe aos desenvolvedores o total controle dos fatores que influenciam referido interesse. Além de serem os responsáveis pela criação e oferta da *gamecoin*, bem como pela produção do jogo e conexão com rede *blockchain*, os desenvolvedores possuem poder de adotar medidas como a implementação de novos recursos, correção de *bugs*, banimento de práticas nocivas, promoção do jogo e adoção de medidas que sustentem a economia do *game* a longo prazo.

Assim sendo, há que se repetir a necessidade de análise casuística para aferição da distribuição de esforços entre desenvolvedores e jogadores, contudo, não se pode ignorar que os fatores acima listados conferem aos criptojogos *P2P2E* todas as características necessárias para constituí-los como modalidade de contratos de investimento coletivo sujeitos ao controle regulatório da CVM.

3. Necessidade de regulação

Parece desejável que os operadores do direito que se debruçarem sobre temas relacionados a novas tecnologias busquem equilibrar a ânsia de regular o não-regulado e o medo da intervenção regulatória excessiva. Por um lado, os criptojogos parecem ocupar papel relevante no desenvolvimento e popularização da tecnologia *blockchain*, além de constituírem interessante modelo de negócios que, a despeito de inseguranças e volatilidades, pode atrair a atenção de diversos investidores. Por outro lado, a preocupação com o desenvolvimento dessa atividade à margem de qualquer regulação estatal não é mero capricho. Os criptojogos são fenômeno recente, mas que já suscita uma série de questões problemáticas, algumas das quais serão brevemente mencionadas a seguir.

Como visto no capítulo anterior, os criptojogos *P2P2E* prescindem da aquisição inicial de itens ou personagens, os quais, em regra, são disponibilizados de forma aleatória ao jogador, em sistema idêntico ao da *lootbox*, isto é, um “item de *videogame* comprado com dinheiro real e que possui conteúdo aleatório” (SCHOLTEN et al., 2019, p. 380). Em outras palavras, a *lootbox* se baseia na

dinâmica de vender ao jogador a chance de obter, com maior recorrência, itens comuns e, com menor recorrência, itens raros, de acordo com probabilidades definidas pelo algoritmo dos desenvolvedores.

Contudo, uma questão recorrente que tem sido levantada em relação a referida tecnologia é a sua aproximação aos jogos de azar, proibidos no Brasil por meio do artigo 50 da Lei das Contravenções Penais¹⁸. Embora não haja precedente de que referida proibição tenha sido levantada contra o sistema de lootbox (presente também em muitos jogos que não usam da tecnologia *blockchain*), há histórico de diversos países que já se preocuparam em regular o instituto, como Japão, China e Coréia do Sul (KOEDER; TANAKA; MITOMO, 2018, pp. 15-16). Portanto, parece sensato que as autoridades públicas ao menos se debrucem sobre o assunto, visando aferir o potencial aditivo do jogo, exigir a disponibilização do algoritmo para conferir as probabilidades de acerto e evitar manipulações, etc.

Outro ponto relevante atinente aos criptojogos é a utilização de robôs (bots) que podem ser usados para o inflacionamento artificial de preço de *gamecoins* através da compra massiva dos ativos (MCCONNEL, 2021) ou para garantir indevidas vantagens competitivas de um jogador em relação a outros (P2NEWS, 2021). Referidas práticas vão de encontro à atribuição conferida à CVM pelo art. 4º, inciso V, da Lei 6.385/76 (“evitar ou coibir modalidades de fraude ou manipulação destinadas a criar condições artificiais de demanda, oferta ou preço dos valores mobiliários negociados no mercado”), sendo desejável que haja algum tipo de controle e fiscalização nesse sentido.

Por fim, o crescimento dos criptojogos foi acompanhado pelo crescimento de novas formas de estelionato (*scams*), como: o uso de artifício ou ardil para obtenção de senhas de acesso às carteiras digitais do usuário, a emissão de tokens falsos que confundam o jogador que pretende investir em *gamecoin* semelhante e até mesmo a captação fraudulenta de recursos para investimento em jogo inexistente (REES, 2021). Tais práticas poderiam ser amenizadas, por exemplo, mediante iniciativas de regulação quanto à emissão de novas criptomoedas e de ofertas públicas de criptoativos ou por meio de exigências quanto à adoção de medidas educativas aos jogadores-investidores.

18. LCP. Art. 50. Estabelecer ou explorar jogo de azar em lugar público ou acessível ao público, mediante o pagamento de entrada ou sem ele: Pena – prisão simples, de três meses a um ano, e multa, de dois a quinze contos de réis, estendendo-se os efeitos da condenação à perda dos móveis e objetos de decoração do local. § 3º Consideram-se, jogos de azar: a) o jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte; b) as apostas sobre corrida de cavalos fora de hipódromo ou de local onde sejam autorizadas; c) as apostas sobre qualquer outra competição esportiva.

Apesar do quanto exposto, a CVM, já em 2017, emitiu nota demonstrando estar ciente da ocorrência de *ICO's* voltados a investidores brasileiros, alertando-os quanto aos riscos do procedimento e alegando que monitoraria o mercado em relação a práticas desse tipo (CVM, 2017). Em 2020, a autarquia chegou a autorizar, para investidores qualificados, o lançamento de fundo de investimento voltados a *NFT's* e *gamecoins*¹⁹, mas não se pronunciou, até o momento, em relação à regularidade dos critojogos.

Não obstante, o assunto não deve ser encarado de forma simplista, pois os critojogos não o são. Trata-se de atividade que ocorre exclusivamente em ambiente virtual e por meio de redes de registro criptografadas e descentralizada, bem como promovida por agentes que podem residir e atuar em jurisdição estrangeira, emitindo ativos ofertados a usuários em todo o mundo. Ademais, a simples imposição das regras já existentes no âmbito da CVM pode ser inadequada, tendo em vista a possibilidade de criação de custos regulatórios que inviabilizem a atividade, a desnecessidade de agentes intermediários na rede *blockchain*, o conflito de competência entre jurisdições diversas, etc (RABELLO; MAFRA, 2019, p. 224).

Ainda, a carência de regulação estatal não se confunde com a carência de mecanismos autorregulatórios que visem conferir credibilidade ao critojogo face aos jogadores-investidores. É comum que os *white papers* demonstrem a realização de auditorias privadas sobre os códigos de *smartcontracts*²⁰ do jogo, bem como que referidos contratos prevejam medidas que direcionem parte das vendas de criptoativos a um fundo de liquidez ou que bloqueiem as carteiras digitais dos desenvolvedores por determinado período, garantindo que permanecerão cumprindo com o prometido.

De qualquer forma, parece possível buscar instrumentos normativos formais que ofereçam maior segurança jurídica ao jogador-investidor e mesmo aos desenvolvedores que buscarem empreender no ramo, proporcionando medidas como a obrigatoriedade de transparência algorítmica, a padronização de *white papers*, a verificação dos processos de auditoria, dentre outras.

19. Trata-se do fundo “Vitreo Cripto NFT FICFIM IE”, disponível em: <https://www.vitreo.com.br/investir/fundos-de-investimento/cripto-nft/>. Acesso em: 08/01/2022.

20. O funcionamento prático dos critojogos usualmente se utiliza de *smartcontracts* ou contratos inteligentes, os quais “podem ser programados para implementar transações mais complexas entre partes, atuando como um “agente independente” que obedecerá às vontades determinadas em seu código-fonte. Dito de outra forma, os *smart contracts* são programas executados em um *blockchain* que, uma vez iniciados, agem de forma independente das partes, obedecendo aos comandos dispostos em seu código-fonte” (RABELLO; MAFRA, 2019, p. 229).

Também merecem ser citadas as propostas de Nathalia Rabello e Ricardo Mafra à regulação de *ICO'S*, as quais, com as devidas adequações, poderiam se aplicar ao mercado de criptoativos. Tais propostas sugerem: a elaboração, pela CVM, de uma Instrução própria para as ofertas públicas de criptoativos no setor e de outra para bolsas de criptoativos; a facilitação e padronização do procedimento de dispensa de registro da oferta de criptoativos e a instituição de regulamentação voluntária que permita o desenvolvimento de um mercado regulado, em paralelo ao não regulado (RABELLO; MAFRA, 2019, p. 224). Também é digna de nota a possibilidade de estímulo aos desenvolvedores de criptoativos para que se inscrevam no programa de sandbox regulatório²¹ promovido pela CVM por meio da Instrução nº 626/2020²².

Por fim, independentemente da solução adotada, é necessário que haja maior difusão do presente debate, a fim de que todos os atores interessados se manifestem na arena pública para pensar conjuntamente sobre a elaboração dos mecanismos mais adequados ao fenômeno, visando atingir o ponto de equilíbrio entre inovação e regulação.

Considerações finais

Este estudo teve como objetivo demonstrar que os criptoativos *play-to-earn* constituem fenômeno carente de regulação pelo direito brasileiro, apesar das crescentes e relevantes questões jurídicas que suscita. Desse modo, inicialmente, explorou-se a diferença entre os diferentes modelos econômicos de jogos eletrônicos, enfatizando as diferenças entre os *games play-to-earn* do passado e os criptoativos da atualidade.

Em seguida, demonstrou-se que parte desses jogos se utiliza do modelo *pay-to-play-to-earn*, que se aproxima, conforme demonstrado, de contrato de investimento coletivo sujeito à regulação da CVM. Após, foram abordados os problemas relacionados à difusão desregulamentada dos criptoativos e sugeridos, em linhas gerais, alguns caminhos para solucioná-los.

21. Sandbox regulatórios ou “ambientes de testes” são um “instrumento regulatório de fomento, baseado em incentivo regulatório por meio de experimentalismo estruturado, tendo como pilar indutivo a isenção normativo-regulatória temporária. Ele se dá através da instituição de programas que objetivam disponibilizar às empresas um espaço propício ao teste e à experimentação de inovações em condições reais, por meio da implementação de um ambiente regulatório mais flexível e menos restritivo, sob a contrapartida de obediência a parâmetros de supervisão do regulador e constante monitoramento e fiscalização” (BRUZZI; KNOB; OBREGON, 2020, pp. 181-201.).

22. Trata-se de sandbox regulatório do mercado de capitais instituído pela CVM.

É necessário ressaltar, contudo, que fenômenos recentes os quais se manifestam de diferentes formas e atingem diversas áreas da vida em sociedade (como é o caso dos criptojogos) suscitam inúmeras questões em diversos ramos do direito, de modo que o presente artigo não buscou assumir a tarefa pretensiosa de esgotar o assunto e todos os seus desdobramentos. Na realidade, parece pouco frutífero que profissionais do direito busquem isoladamente por soluções regulatórias adequadas, tendo em vista a complexidade do tema e o veloz desenvolvimento tecnológico que o permeia. Entretanto, é igualmente infrutífero que os juristas se mantenham alheios a relevantes discussões contemporâneas.

Por tal razão, este trabalho buscou, sobretudo, fomentar o debate sobre questão pouco explorada pelos principais agentes regulatórios do país. Os jogos eletrônicos há muito não são mais enxergados como tema infantil e parece necessário que essa visão também seja abandonada pelo Direito brasileiro.

Referências Bibliográficas

ANTE, Lennart. *Non-fungible token (NFT) markets on the Ethereum blockchain: temporal development, cointegration and interrelations*. Hamburgo: Blockchain Research Lab, 2021

BARBOSA, Mafalda Miranda. Blockchain e responsabilidade civil. In: NETTO, Felipe Braga et al. (Coord.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. Indaiatuba, SP: Editora Foco, 2021, pp. 797-827.

BIT2ME ACADEMY. *O que é um white paper?* Disponível em: <https://academy.bit2me.com/pt/o-que-%C3%A9-um-whitepaper/>. Acesso em: 08/01/2022

BRASIL. Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm. Acesso em 08/01/2022.

_____. Lei 6.385 de 7 de dezembro de 1976. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6385compilada.htm. Acesso em 08/01/2022.

BRUZZI, Eduardo; KNOB, Yasmin; OBREGON, Fernanda. Sandbox Regulatório no Brasil: os modelos CVM, SUSEP e Banco Central. In: BECKER, Daniel (Coord.); FERREARI, Isabela (Coord.). *Regulação 4.0: vol. II: Desafios da regulação diante de um novo paradigma científico*. São Paulo: Thomson Reuters Brasil, 2020, pp. 181-201.

CASTRONOVA, Edward. *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier*. Califórnia: CESifo, 2001

YAP. Jack. Axie Infinity's \$1.2 Billion Annualized Revenue Overtakes Candy Crush's 2020 Total Revenue. *Chaindebrief*, 24 de julho de 2021. Disponível em: <https://chaindebrief.com/axie-infinitys-1-2-billion-annualized-revenue-overtakes-candy-crushs-2020-total-revenue/>. Acesso em 08/01/2022

CLOAD MAGAZINE INC. *Dungeons and Dragons*. California: 1980, p. 02. Disponível em: [http://www.gametronek.com/site/rubriques/tandy/FAQs/CLOAD%20Magazine%201980-05%20\(1980\)\(CLOAD%20Magazine%20Inc\).pdf](http://www.gametronek.com/site/rubriques/tandy/FAQs/CLOAD%20Magazine%201980-05%20(1980)(CLOAD%20Magazine%20Inc).pdf). Acesso em: 08/01/2022.

COMISSÃO DE VALORES MOBILIÁRIOS. *FAQ da CVM a respeito do tema Initial Coin Offerings (ICOs)*. Disponível em: <https://www.gov.br/cvm/pt-br/assuntos/noticias/initial-coin-offerings--icos--88b47653f11b4a78a276877f6d877c04>. Acesso em: 08/01/2022.

_____. Instrução CVM nº 400, de 29 de dezembro de 2003. Disponível em: <http://conteudo.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/400/inst400.pdf>. Acesso em: 08/01/2022

_____. Instrução CVM nº 626, de 15 de maio de 2020. Disponível em: <http://conteudo.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/600/inst626.pdf>. Acesso em: 08/01/2022

_____. *Nota a respeito do tema Initial Coin Offering (ICO)*. Disponível em: <https://www.gov.br/cvm/pt-br/assuntos/noticias/initial-coin-offering--ico--a0e4b1d10e5a47aa907191d5b6ce5714>. Acesso em: 08/01/2022.

_____. Processo Administrativo Sancionador CVM nº 19957.009524/2017-41. Diretor Relator: Gustavo Machado Gonzales. São Paulo, 22 de abril de 2019. Disponível em: http://conteudo.cvm.gov.br/export/sites/cvm/decisoes/anexos/2019/20190422/0832__DGG.pdf. Acesso em: 08/01/2022.

_____. Processo Administrativo Sancionador CVM nº 19957.003406/2019-91. Diretor Relator: Gustavo Machado Gonzales. São Paulo, 26 de outubro de 2020. Disponível em: http://conteudo.cvm.gov.br/export/sites/cvm/noticias/anexos/2020/20201027_PAS_CVM_19957_003406_2019_91_voto_diretor_gustavo_gonzalez.pdf. Acesso em: 08/01/2022.

ROCHA, Luciano. IDO, ICO, IEO e IFO: saiba o que são e quais as diferenças. *Criptofácil*, 16 de agosto de 2021. DeFi 101. Disponível em: <https://www.criptofacil.com/ido-ico-ieo-e-ifo-saiba-o-que-sao-e-quais-as-diferencas/>. Acesso em: 08/01/2022

CRYPTOGUARDS. *White paper*. Disponível em: <https://whitepaper.cryptoguards.me/roadmap>. Acesso em: 08/01/2022.

FONSECA, Ana Taveira. Smart Contracts. In: NETTO, Felipe Braga et al. (Coord.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. Indaiatuba, SP: Editora Foco, 2021, pp. 743-753.

GUILD OF GUARDIANS. *White paper*. Disponível em: <https://whitepaper.guildofguardians.com/>. Acesso em: 08/01/2022.

MIN, Tian; WANG, Hanyi; GUO, Yaoze; CAI, Wei. *Blockchain Games: A Survey*. Shenzhen: School of Science and Engineering, The Chinese University of Hong Kong: 2019

KOEDER, Marco Josef; TANAKA, Ema; MITOMO, Hitoshi. "Lootboxes" in digital games -A gamble with consumers in need of regulation? An evaluation based on learnings from Japan. In: THE 22ND BIENNIAL CONFERENCE OF THE INTERNATIONAL TELECOMMUNICATIONS SOCIETY. *Beyond the boundaries: Challenges for business, policy and society*. Seul, 2018.

MOUSE HAUNT. *White paper*. Disponível em: <https://whitepaper.mousehaunt.com/universe/>. Acesso em: 08/01/2022.

REES, Katie. The 5 biggest nft scams and how to avoid them. *MUO*, 21 de outubro de 2021. Technology explained. Disponível em: <https://www.makeuseof.com/biggest-nft-scams-how-to-avoid/>. Acesso em: 08/01/2022.

NALIN, Paulo; NOGAROLI, Rafaella. Inteligência artificial, blockchain e smart contracts: breves reflexões sobre o novo desenho jurídico do contrato na sociedade da informação. In: NETTO, Felipe Braga et al. (Coord.). *Direito digital e inteligência artificial: diálogos entre Brasil e Europa*. Indaiatuba, SP: Editora Foco, 2021, pp. 753-775.

MCCONNEL, Alex. How bots are being used to skew nft prices for big profit. *NETACEA*. Disponível em: <https://www.netacea.com/blog/how-bots-skew-nft-prices-for-big-profit/>. Acesso em: 08/01/2022.

NEWMAN. James. *Videogames*. Londres: Routledge, 2004, p. 5

NEWZOO. *2021 Global Games Market*. Disponível em: <https://newzoo.com/insights/articles/the-games-market-in-2021-the-year-in-numbers-esports-cloud-gaming/>. Acesso em: 04/01/2022.

OLIVEIRA. Ruy Guilherme Silva Gomes de. *Aplicação de meta-modelos à monetização de jogos free-to-play*. São Luís: TEDE UFMA: 2017.

ONÇA. Fabiano Alves. *A era dos games na sociedade da escolha*. São Paulo, Teses USP: 2014.

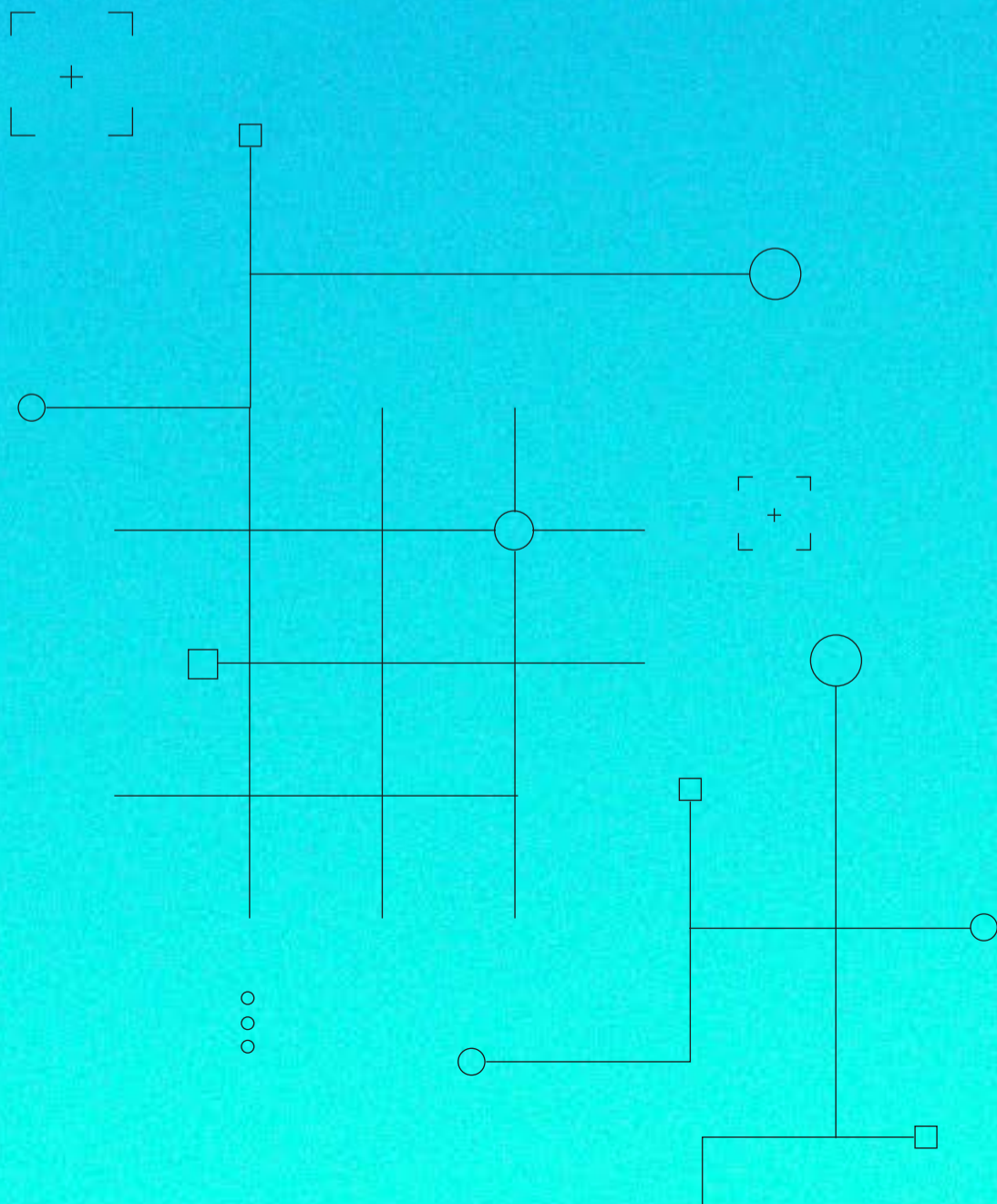
- P2ENEWS. *Bot farming will get you banned!* Disponível em: <https://p2enews.com/news/bot-farming-will-get-you-banned-p2enews/>. Acesso em: 08/01/2022.
- PLAY TO EARN ONLINE MAGAZINE. *What's the Play-to-Earn Business Model?* Disponível em: <https://www.playtoearn.online/whats-the-play-to-earn-business-model/>. Acesso em: 08/01/2022.
- RABELLO, Nathalia; MAFRA, Ricardo. Regulação das initial coin offerings no direito brasileiro: as dificuldades práticas e algumas recomendações para a construção de um marco regulatório adequado. In: BECKER, Daniel (Coord.); FERRARI, Isabela (Coord.). *Regulação 4.0: Novas tecnologias sob a perspectiva regulatória*. São Paulo: Thomson Reuters Brasil, 2019, pp.211-247.
- SCHOLTEN, Oliver James *et al.* Ethereum Crypto-games: mechanics, prevalence and gambling similarities. In: CHI PLAY '19: THE ANNUAL SYMPOSIUM ON COMPUTER-HUMAN INTERACTION IN PLAY. *Paper Session 6: Broader Reflections*. Barcelona: 2019.
- SPACE CRYPTO. *White paper*. Disponível em: <https://docs.spacecrypto.io/guides/readme>. Acesso em: 08/01/2022.
- STATISTA. *Distribution of video gamers worldwide in 2017, by age group and gender*. Disponível em: <https://www.statista.com/statistics/722259/world-gamers-by-age-and-gender/>. Acesso em: 04/01/2022.
- STAR ATLAS. *White paper*. Disponível em: <https://staratlas.com/white-paper.pdf>. Acesso em: 10/01/2022.
- THETAN ARENA OFFICIAL. *3 million players reached as thetan arena breaks multiple records in nft gaming*. Disponível em: <https://medium.com/@ThetanArena/3-million-players-reached-as-thetan-arena-breaks-multiple-records-in-nft-gaming-19e247d70c8a>. Acesso em: 08/01/2022.
- TOTTOC. Jose Karlo Mari. 5 Most Profitable Industries in the World in 2021. *Insider Monkey*, 18 de junho de 2021. News. Disponível em: <https://www.insidermonkey.com/blog/5-most-profitable-industries-in-the-world-in-2021-946645/>. Acesso em: 08/01/2022.
- VITREO CRIPTO. *Cripto NFT*. Disponível em: <https://www.vitreo.com.br/investir/fundos-de-investimento/cripto-nft/>. Acesso em: 08/01/2022.
- ZODIACS. *White paper*. Disponível em: <https://s.ladicdn.com/60d5ad345932a600139ca4b2/zodiacs-whitepaper--20211011100244.pdf>. Acesso em: 08/01/2022.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

17

As implicações penais da prática de scanlation

LARISSA FERNANDA DE MESQUITA BARALDO



Sumário: Introdução. 1. Da origem à globalização dos mangás. 2. Da prática de *scanlation*. 3. Da violação dos direitos autorais. 4. Das complicações e possíveis soluções cibernéticas. Considerações finais. Referências Bibliográficas.

Introdução

A pirataria digital de mangás, conhecida como *scanlation*, é um dos meios mais recorridos de se consumir mangás no Brasil. Esta prática, mesmo que ilegal, acarretou na popularização e consolidação do mercado nacional de publicação de quadrinhos japoneses e ganha força no contexto atual de alta demanda por mangás que não possuem seu material físico licenciado. Entretanto, a cultura de *scanlation* é considerada prejudicial pelas editoras japonesas. Este argumento é embasado em levantamentos como a da Associação de Distribuição de Conteúdo no Exterior (*Content Overseas Distribution Association*), organização que procura proteger os direitos autorais da indústria de entretenimento japonesa, que no ano de 2019 estimou-se um prejuízo financeiro de 6 bilhões a 7 bilhões² de reais devido a distribuição ilegal de mangás online. Portanto, a pesquisa visa apresentar o contexto brasileiro da distribuição de mangás ilegais, discutir as implicações jurídicas sobre o tema e refletir sobre as complicações e soluções tecnológicas para esta problemática.

1. Da origem à globalização dos mangás

Através da etimologia da palavra, entende-se “mangá” como desenhos humorísticos, definição que se afilia com a origem destes quadrinhos japoneses oriundos da mistura de tradições artísticas japonesas como os *emakimono* e da influência estrangeira. Como influência, pode-se pontuar especificamente a criação e popularização da revista de humor, *Japan Punch* do inglês Charles Wirgman em 1859 que elaborava charges de cunho político. A impressão da revista inspirou artistas japoneses a desenharem sátiras e ampliarem os seus conhecimentos de narrativas sequenciais, que na época ainda seguia o estilo norte-americano sem balões de diálogo.

1. Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio (ITS) com a Universidade do Estado do Rio de Janeiro (UERJ). Graduada em Direito pela Universidade Federal Fluminense (UFF).

2. Valor referente à cotação do iene de R\$0,048 em 11 de janeiro de 2022.

Destaca-se que o termo mangá é a nomenclatura utilizada para se referir a histórias em quadrinhos no Japão, enquanto nos Estados Unidos os quadrinhos são conhecidos pelo seu teor cômico e por causa deste fator se utiliza a nomenclatura *comics* para se referir a estes. Já no Brasil, o termo é gibi devido a influência de uma revista infantil.

Entretanto, o formato adotado para a produção de mangás veio a ser consolidado apenas após as publicações de Osamu Tezuka, que recebeu o apelido de “Deus do Mangá” entre os japoneses. Segundo Luyten (2005), Tezuka, fortemente influenciado pelo teatro japonês, cinema europeu e Walt Disney se valeu de técnicas cinematográficas para ambientar suas obras de forma mais expressiva, com close-ups nos rostos de seus personagens, onomatopeias para representar sons e desenhos de linhas para indicar movimento o que resultava em uma leitura mais dinâmica. É importante destacar que o traço característico dos quadrinhos japoneses de personagens com olhos grandes é também trabalho de Tezuka, inspirado pelo filme *Bambi* da Disney. Além destas inovações gráficas, Tezuka ampliou as temáticas abordadas nos quadrinhos e consolidou as animações na mídia televisiva japonesa onde adaptava suas obras mais populares. Como resultado de suas contribuições, os mangás tiveram destaque na indústria do entretenimento japonesa.

O mangá se diferencia em vários aspectos das produções de quadrinhos ocidentais, desde o detalhe mais simples como a forma em que são lidos até a metodologia de publicação. Sua leitura deve ser realizada da direita para a esquerda, respeitando a estrutura gramatical oriental. Quanto à publicação, a indústria de quadrinhos japonesa adota uma estratégia voltada a segmentar públicos-alvo através de critérios como gênero e faixa etária. Por exemplo, a maior editora japonesa, *Shūeisha* publica a *Shounen Jump*, revista que publica narrativas esportivas e heróicas que buscam atrair rapazes como o mangá mais vendido no mundo, *One Piece* (publicado desde 2012 e em andamento pela editora brasileira Panini). Na mesma editora tem a revista voltada para o público feminino que divulgam histórias dramáticas e de romance, a *Margaret* que publicou mangás famosos como *Rosa de Versalhes* (publicado pela editora brasileira JBC em 2019). No geral, existem cinco grupos demográficos respeitados pelas editoras no Japão: *Shoujo* que visa o público jovem feminino, *shounen* que é voltado para os meninos, *josei* para mulheres maduras, *seinen* para homens adultos e *kodomo* para crianças.

Também é interessante comentar que os capítulos de um mangá são publicados semanalmente ou mensalmente em revistas, onde dependendo do

gênero e idade de seu público irá atrelar outros conteúdos que venham à agrada-los, como reportagens sobre negócios ou ensaios fotográficos de cantores populares. Se a série for popular esta poderá vir a ser compilada e publicada em volumes encadernados, como é feito no Brasil.

1.1 Cool Japan e a importância dos mangás

No início dos anos 2000 os mangás passaram de um passatempo japonês para uma forma de mídia consumida em escala global, se tornando ferramenta importantíssima para relações diplomáticas e produto de exportação do Japão. Não só os licenciamentos de quadrinhos como a de animações, música e jogos eletrônicos, se caracterizando como um verdadeiro tsunami cultural no Ocidente. Este *boom* dos mangás auxiliou o Japão a sobreviver às crises econômicas a partir da década de 1990 que bloquearam a produção do setor industrial.

Na mesma década, ao reconhecer a expansão da cultura nipônica pelo mundo, o governo japonês adotou a campanha do *Cool Japan* - termo extraído de uma reportagem da revista americana *Foreign Affairs* em 2002 sobre o crescimento da influência cultural japonesa no globo - que consiste em uma modalidade de *soft power* para abeirar relações diplomáticas, ou seja, um poder de convencimento sob a aptidão de influenciar a perspectiva dos jovens do mundo inteiro sobre o Japão e convencê-los a consumir. Afinal, os quadrinhos japoneses afastam a imagem de país tradicional advinda das épocas de xogunato e apresenta uma realidade atual de país *high-tech*. Aliado com o seu *hard power* da exportação de produtos de alta tecnologia, o Japão tem uma grande variedade de produtos tanto caros quanto baratos que são cobiçados mundialmente.

1.2 O mercado de mangás no Brasil

Ao estudar a consolidação do mercado nacional de publicação de quadrinhos japoneses, observa-se três ondas. A primeira movimentação de mangás no Brasil foi na primeira metade do século XX e se deu por conta da imigração japonesa. É abordado por Ramos (2018) que os imigrantes e descendentes japoneses se valiam da leitura dos mangás era uma forma de manter contato com as suas raízes nipônicas, para exercer a língua natal e continuar atrelado à sua cultura.

Por outro lado, a primeira publicação nacional de um mangá só veio em 1988 pela editora Cedibra com a obra *Lobo Solitário* de Koike Kazuo e Kojima Goseki. Esta história narra sobre a vida de um samurai, sendo um conteúdo

voltado para um público adulto. Sendo elogiada pela crítica, a primeira edição brasileira de *Lobo Solitário* que possuía a peculiaridade de ser traduzido a partir da edição americana e não da japonesa original. Dois anos depois da impressão da história sobre a filosofia samurai e historicidade nipônica, a editora Globo distribuiu a famosíssima obra *Akira* de Katsuhiro Otomo, se aproveitando do sucesso do longa-metragem homônimo que revolucionou a forma em que se faz animações. No entanto, todas as obras divulgadas nesta segunda onda da invasão cultural japonesa não tiveram boas vendas, mesmo sendo elogiadas pelos críticos, resultando em um tumulto editorial para finalizar os títulos no Brasil.

A consolidação do mercado nacional de mangás se iniciou somente em 2000 quando a editora Conrad distribuiu *Dragon Ball* e *Cavaleiros do Zodíaco*, dois mangás já conhecidos pelo público brasileiro devido ao grande sucesso de suas animações transmitidas na televisão. A estratégia de pesquisar quais mangás que possuíam apelo popular por conta de suas versões animadas foi certeiro, visto que o público que consumia também tinha interesse em ler o material de origem. Esta metodologia foi aplicada em outros lançamentos e unido com estrutura padrão ocidental resultou em um maior investimento neste nicho por parte das editoras. Nesta terceira onda de expansão da cultura japonesa no Brasil, as editoras já tinham restabelecido o molde oriental de leitura que é conhecido atualmente, visto que em consenso constataram que a antiga forma de publicação era onerosa e morosa para se trabalhar.

Atualmente, pode-se constatar que a cultura de consumo de mangás é um fenômeno bastante popular no país. O embasamento de tal afirmação é de que apenas uma das setes editoras que publicam mangás no Brasil, a NewPOP, anunciou trinta obras licenciadas no primeiro mês do ano de 2022 e com a promessa de revelar mais títulos no futuro.³ Logo, é palpável a alta demanda.

A estrutura editorial da publicação de um mangá no Brasil sofre empecilhos como a morosidade da aprovação de seu conteúdo pelas editoras nipônicas – que muitas vezes exigem o envio físico do exemplar para averiguar a qualidade do produto – e de distribuição homogênea pelo território nacional, sendo normal queixas de brasileiros não residentes da região sudeste de falta de acesso aos exemplares. Também há a problemática do encarecimento dos

3. **Confira os anúncios do NewPOP WEEKEND!** NewPop, Notícias, 31 de janeiro de 2022. Disponível em: <https://www.newpop.com.br/confira-os-anuncios-do-newpop-weekend/> Acesso em: jan. 2022

exemplares já que os insumos como papel sofreram uma alta considerável de preços.⁴

2. Da prática de *scanlation*

Como foi explanado no capítulo anterior, o mercado nacional de mangás demorou para arrecadar investimentos e uma estrutura para publicar títulos diversos. Ademais, é necessário comentar que a estratégia, ainda vigente para a maioria dos títulos anunciados no Brasil, de imprimir mangás que tem uma animação de sucesso limita ainda mais a variedade de obras nipônicas. Comparando com o acervo japonês torna o cenário brasileiro ainda pior, este com um número exorbitante de histórias lançadas de todos os gêneros e públicos-alvo possíveis, além de outros formatos e *merchans* relacionados com a série cartunizada, como *action figure* – esculturas detalhadas de personagens populares - e *artbook*, livros que exploram a parte artística da obra como detalhes sobre o processo criativo e ilustrações exclusivas dos personagens. Além disso, mesmo quando um quadrinho japonês é licenciado no Brasil, devido ao processo de publicação peculiar asiático, há atrasos nos lançamentos. Outros problemas enfrentados por mangás licenciados no Brasil são a rigidez gráfica das editoras japonesas que dificultam a periodicidade da publicação e o risco recorrente da história vir a ser cancelada por causa do fracasso de vendas.

Diante este cenário, os consumidores de mangás recorrem ou à aquisição de volumes estrangeiros – o que é bastante oneroso e limita o público para aqueles que têm conhecimento de outras línguas - ou à grupos de *scanlation* para manter contato com suas histórias favoritas e descobrir novos títulos que podem encantá-los.

O *scanlation* é um termo referente a distribuição da tradução de capítulos ou volumes de mangás digitalizados gratuitamente nas plataformas digitais. Este trabalho é realizado por um grupo de fãs, que devido ao seu amor pelas obras asiáticas aprendem línguas diferentes e obtém conhecimentos de programas editores de imagens para promover o mangá que gosta para um público maior. É uma forma alternativa de consumir mangás que só é viável devido à cultura participativa desta comunidade, que dispõe de horas de seus dias para administrar um site ou blog de *scans*.

4. GAGLIONI, Cesar. **Como o preço do papel pressiona o mercado editorial**. Nexo, Expresso, 01 de março de 2022. Disponível em: <https://www.nexojornal.com.br/expresso/2022/03/01/Como-o-pre%C3%A7o-do-papel-pressiona-o-mercado-editorial> Acesso em: mar. 2022

Por exigir várias habilidades e dependendo dos títulos que buscam disponibilizar em sua plataforma, os grupos de *scanlation* possuem um recrutamento em comunidades virtuais ou engajam em formas de capitalizar a fim de manter o seu trabalho. As maneiras populares de adquirir dinheiro é através de links de doações feitas pela comunidade ou a veiculação de links patrocinados em sua plataforma. É crucial deixar claro que a prática de *scanlation* não almeja fins lucrativos, é um exercício feito de fãs para fãs.

Em suma, é uma forma de suprir a demanda de mangás que se tem em seu país de origem e graças aos adventos da tecnologia, a distribuição da digitalização de mangás traduzidos por fãs é facilitada. Como foi abordado pela pesquisadora Lee (2009), os motivos centrais para a prática de *scanlation* é a paixão dos fãs à obra, contendo um forte sentimento de zelar pelo seu mangá favorito. Desse modo, os *scanlators* – nome que se dá para os membros da equipe – se devotam à ampla divulgação do quadrinho a fim que este venha a ser conhecido pelo grande público.

Logo, observa-se que esta prática é importante também para a leitura de mangás mais desconhecidos, mas que podem vir a ser interessantes para a comunidade já que o licenciamento de mangás no mercado nacional é baseado em sua popularidade. Afinal, os *scans* auxiliam as editoras de mangás brasileiras nas pesquisas de mercado visto que a popularidade de certos *scans* atenta as editoras há buscar o licenciamento dessas obras por terem previsões de boas vendas. Por exemplo, conforme é apontado por Hirata (2012), o mangá *Fruits Basket*, o qual foi publicado no Brasil graças ao trabalho dos *scanlators*, que por conta de seu ofício, resultou em uma legião de leitores assíduos que vieram a se mobilizar para demonstrar seus interesses em ter acesso à obra fisicamente diante as editoras nacionais.

2.1 A diferença do scan para o doujinshi

Assim como os *scans*, os *doujinshis* também auxiliam no crescimento da indústria de mangás. Cabe salientar em primeira análise que tanto o *scanlation* quanto o *doujinshi* violam os direitos autorais, afinal, ambos não têm a prática de solicitar permissão formal dos criadores das obras para alterá-las ou divulgá-las. Visto isto, destaca-se que o *doujinshi* não é necessariamente virtual como os *scans* e estes divergem quanto ao seu conteúdo.

O *doujinshi* é um quadrinho que copia elementos de uma obra popular como narrativa ou personagens e introduzem transformações da história ori-

ginal. Por exemplo, altera-se levemente o *plot* ou modifica a aparência dos personagens. É um mercado alimentado por fãs que buscam conteúdos diferenciados dos seus mangás favoritos e que naturalmente beneficia a comercialização dos mangás, visto que a competição gerada pelos *doujinshi* impacta na alta produtividade e qualidade dos mangás. Além disso, vários mangakas aprenderam a desenhar ou começaram as suas carreiras produzindo *doujinshi*, como o autor do mangá *Ijiranaide, Nagatoro-san*, Nanashi. Dessa forma, é do costume japonês autorizar a circulação destas obras adulteradas mesmo sendo juridicamente ilegal. Como é citado por Lessing (2004), outro motivo da permanência dos *doujinshi* a dificuldade nipônica de frear o seu avanço por conta da falta de recursos e advogados para denunciar estes casos.

Outra diferença é que os grupos de *scans*, mesmo sendo divulgação ilegal, possuem um certo código de ética do qual consiste no término da prática quando a obra for licenciada e manter ao máximo, a integridade da obra. No fim das contas, o cerne da questão que envolve o *scanlation* é promover o licenciamento dos mangás. Entretanto, há casos em que o trabalho de *scan* não é finalizado mesmo com publicação nacional, alegando que nem todos os leitores possuem condições financeiras para ter acesso à obra. Nestas ocasiões, a equipe de *scan* promove a compra dos exemplares a fim de incentivar o mercado nacional e o artista da obra.

3. Da violação dos direitos autorais

Por sua definição, o *scanlation* é uma violação direta aos direitos autorais, na medida que tanto na legislação nacional quanto japonesa, a aquisição de um mangá não permite que o consumidor venha a divulgá-lo sem autorização do autor.

A seguir serão abordadas as implicações jurídicas penais que envolvem o ofício de *scans* à luz do ordenamento japonês e nacional.

3.1 Perspectiva japonesa

A terra natal dos mangás se vale do regime de *copyright* para assegurar os direitos do autor. Ou seja, o seu foco é viabilizar a proteção material da obra – artística, literária, científica, entre outras – e a sua capacidade de reprodução. Em tradução livre, o “direito da cópia” tem um forte viés de exploração econômica da obra e desse modo, se preocupa com a captação de lucro do autor e encomendador da obra pelo uso comercial que vem a ser utilizado. Ao discutir sobre os direitos morais abordados na lei japonesa, nota-se que estes

são mais extensos do que os disponíveis na lei americana e buscam manter a integridade da obra. Já na exploração econômica, os direitos patrimoniais, diferentes dos morais, são transferíveis e se atrelam ao direito de reprodução, performance, distribuição e derivações de sua obra, vide art. 21-28 da *Japanese Copyright Act*, lei japonesa que versa sobre os direitos do autor.

As únicas exceções presentes no regime japonês são as de *fair use*, quando a utilização da obra envolve motivações educacionais e de material crítico, a fim de promover a acessibilidade à cultura e progresso artístico. No geral, o uso da cópia é legal quando não tem intenções de lucratividade ou ferir a integridade da obra.

Ao que se refere ao *scanlation*, a tipicidade se encontra no artigo 113, I, (ii) da *Japanese Copyright Act*, que aborda sobre a violação do direito autoral na prática da distribuição com o propósito de distribuição de uma obra através de um meio que venha a infringir os direitos do autor, de impressão, entre outros tutelados pela lei. A pena penal para tal atividade ilegal é expressa no artigo 119 da lei supracitada, que pode acarretar o aprisionamento de até 10 anos do infrator e multa de 10 milhões de ienes, cerca de 482 mil reais.

Não só viola o direito patrimonial da distribuição indevida como pode vir a infringir o direito moral do autor, por conta da tradução indevida. Tal direito é garantido pelo artigo 20 da lei que versa sobre o direito do autor de preservar a integridade de sua obra, a qual não poderá vir a sofrer quaisquer modificações ou recortes que venham a ser contrários à intenção do autor. Esta infração moral prejudica a reputação do criador, pois uma tradução malfeita pode vir a alterar totalmente a mensagem da obra. É interessante salientar que este dispositivo também permite que as penalidades da tradução equivocada possam vir a ser aplicadas para obras licenciadas também.

Entretanto, como será discursado adiante, os esforços japoneses não conseguem frear o avanço do *scanlation*, levando a implementação de novas leis quanto à proteção intelectual. Em junho de 2020 foi sancionada uma emenda à *Copyright Act* japonesa⁵, que revisou segmentos expressos pelo direito autoral japonês vigente, resultando na tutela sobre sites que divulgam *hyperlinks* de material pirateado e os *downloads* ilegais do conteúdo desses *hyperlinks*.

5. “Act to Revise Part of the Copyright Act and the Special Provisions on the Registration of Works of Computer Programming”, em tradução livre, ‘Lei de Revisão da Parte da Lei de Direitos Autorais e das Disposições Especiais sobre o Registro de Obras de Programação de Computadores’

Antes desta emenda, a prática destes sites de distribuir *hyperlinks* para obras pirateadas não era considerada infração ao direito autoral, logo, os administradores desses sites não sofriam penalidades criminais. O argumento utilizado para incriminar estes sites veio do pensamento de que ao prover os *hyperlinks*, estaria ocorrendo um incentivo ao consumo de material pirateado. E a punição é extensiva para tanto os administradores deste site quanto usuários que vierem a divulgar os *hyperlinks* nas interações disponíveis neste servidor. Dessa forma, desde outubro de 2020, para os provedores do site, a penalidade é de até 3 anos de prisão, multa de até 3 milhões de ienes (equivalente a 144 mil reais) ou ambas as opções. Já para os operadores do mesmo site a pena é de até 5 anos de prisão, multa de no máximo 5 milhões de ienes (241 mil reais) ou ambas as opções.

O outro segmento da reforma, a infração quanto a aquisição de obra ilegal por download, veio a ter o exercício de sua sanção posteriormente. A lógica da violação se baseia no cenário de que o usuário estaria usufruindo de material pirateado conscientemente. Os usuários enquadrados recorrentemente neste crime são punidos em até 2 anos de prisão e em multa de até 2 milhões de ienes (96 mil reais), ou ambos.

Desde janeiro de 2021 está em vigor esta parte da emenda, que possui exceções em casos de *download* e *print* de pequenas partes de conteúdo pirateado, o *download* feito sem intenção, *download* de paródias e derivações da obra, e sob circunstâncias especiais onde a obra pirateada não vem a prejudicar os direitos autorais. Estas exceções vieram como contraponto à proposta inicial da penalidade dos *downloads*, que em 2019 eram mais rigorosas, onde tipificavam quaisquer conteúdos pirateados.

Sem as exceções estipuladas, o uso da internet no Japão enfrentaria novas dificuldades como a caducidade da ferramenta de pesquisa, que poderia prejudicar o próprio *mangaka* já que a propagação de *prints* e paródias auxiliam na popularização de sua obra. A proposta inicial também afetaria o direito de liberdade de expressão dos usuários, que não poderiam postar sobre passagens de suas obras favoritas ou se expressarem artisticamente, influenciados por uma obra específica. Além disso, como foi citado anteriormente, a cultura de mangás no Japão possui um grande impacto na circulação de derivações das obras originais e diante à este fato, Landers (2021) afirma que a permissiva de baixar conteúdo de obra parodiada ou derivada é relacionada com o mercado de *doujinshi* no Japão.

3.2 Perspectiva nacional

Em 2020, o Brasil liderava o ranking mundial de países que consumiam pirataria online, conforme pesquisa organizada pela empresa Nagra/Kudelski Group⁶. No quesito de consumo de mangás de forma ilegal não é diferente, sendo uma problemática recorrente pelas editoras brasileiras. Por exemplo, em 2017, a editora JBC precisou solicitar a um site de *scanlation* que retirasse os títulos que são licenciados pela editora.⁷

Diferente do *copyright* japonês, o ordenamento nacional adota o modelo de direito do autor -do francês, *droid d' auteur* – é de tradição romano-germânica e está voltado para a proteção da integridade do autor, a criatividade da obra e assegurar os direitos morais que envolvem a relação autor-obra. O mercado nacional de mangás, além de ter que assegurar os direitos autorais japoneses das obras licenciadas, deve zelar pelo regimento nacional já que a prática de *scanlation* também vêm a ser tipificada como violação ao direito autoral.

Há tanto possibilidade de responsabilização civil quanto penal para a violação dos direitos autorais. Conforme pensamento de Santos (2009), as obras intelectuais não perdem a sua tutela mesmo quando são digitalizadas, logo, o enquadramento penal da distribuição de *scans* - mesmo nos casos em que não há intuito de lucro direto ou indireto - é configurado como conduta típica por vir a violar direitos de autor, vide artigo 184 do Código Penal. Expressamente, as sanções do crime variam de detenção de até 1 ano ou multa na sua modalidade mais simples para reclusão de até 4 anos e multa quando há motivação financeira.

Todavia, esta violação aos direitos autorais ocasionada pela pirataria digital é questionada pelo pesquisador Túlio Vianna (2006). Em seu raciocínio, a digitalização de propriedade intelectual é principalmente prejudicial para a empresa – no caso, editora – dado o argumento de que “todo aquele que pirateia uma obra intelectual, caso fosse impedido de fazê-lo, necessariamente compraria o produto” (VIANNA, 2006, p.11). A consequência da prática ilegal não afetaria financeiramente o autor visto que sua remuneração é majoritariamente pela “alienação deste trabalho aos detentores dos meios de produção

6. FELTRIN, Ricardo. **Brasil é 1º do mundo em consumo de pirataria online, diz estudo**. UOL, Splash Uol, 21 de dezembro de 2020. Disponível em: <https://www.uol.com.br/splash/noticias/ooops/2020/12/21/brasil-e-do-mundo-1-em-consumo-de-pirataria-online-diz-estudo.html> Acesso em: jan. 2022

7. **Representantes da JBC falam sobre a polêmica com scanlation que cobrava assinaturas**. Geekdama, notícias, 18 de julho de 2017. Disponível em: <https://geekdama.com.br/noticias/anime-friends-2017-jbc-polemica-scanlation/> Acesso em: jan. 2022

que irão consubstanciá-lo em meio físico e vendê-lo no livre mercado” (VIANNA, 2006, p.12). Desse modo, a criminalização da pirataria teria o viés de garantir um monopólio do direito de reprodução da obra, intuito contrário aos direitos de autor que focam na ampla divulgação do trabalho intelectual.

Outrossim, a violação do direito patrimonial da pirataria é configurada erroneamente na esfera penal visto que ocorre apenas uma falta de correspondência com a remuneração estimada pelo proprietário dos meios de produção, logo, a infração contra os direitos autorais seria mais bem tutelada na esfera civil por se tratar de uma dívida civil. Dessa maneira, a sanção penal seria inconstitucional visto que não é vedada a prisão civil por dívida à luz do art. 5º, LXVII.

Cabe salientar que no cenário de *scanlation*, pode-se valer de princípios limitadores constitucionais para evitar penalidade em esfera criminal. Por se tratar de uma cultura, a leitura de *scans* é tanto difundida quanto aceita pela sociedade brasileira que engaja positivamente nas redes sociais incentivando o consumo e se voluntariando para participar nas traduções e edições necessárias para a distribuição. Logo, a conduta deixa de ser considerada injusta, podendo se valer do princípio da adequação social.

Compreende-se que o *scanlation* tem benefícios tanto para o autor quanto para o público. “Do ponto de vista de lucro, para o próprio autor da obra, muitas vezes a sua reprodução inclusive é mais benéfica do que o monopólio de exploração pelas empresas” (ROSA, 2014, p. 8). Por parte do criador, sua obra terá uma maior visibilidade, o que acarreta em outras oportunidades de trabalho que geram um lucro maior do que o percentual que ganha em relação à distribuição física de sua obra. Para os leitores, o acesso para uma vasta variedade de mangás é facilitado. Desse modo, mesmo que se classificando como ilegal, os *scans* apresentam lesividade mínima para a sociedade, instaurando o princípio da insignificância.

Por fim, enxerga-se a aplicação do princípio da intervenção mínima, o qual garante que o direito penal deve ser aplicado apenas quando os demais ramos do direito não forem capazes de proteger os bens de maior importância. Segundo Greco (2017, p.127):

O princípio da intervenção mínima, ou *ultima ratio*, é o responsável não só pela indicação dos bens de maior relevo que merecem a especial atenção do Direito Penal, mas se presta, também, a fazer com que ocorra a chamada descriminalização. Se é com base

neste princípio que os bens são selecionados para permanecer sob a tutela do Direito Penal, porque considerados como os de maior importância, também será com fundamento nele que o legislador, atento às mutações da sociedade, que com a sua evolução deixa de dar importância a bens que, no passado, eram da maior relevância, fará retirar do nosso ordenamento jurídico-penal certos tipos incriminadores.

A partir deste ensinamento, observando não só a lesividade mínima para a sociedade, como a aceitação da prática de *scanlation* por parte dela, conclui-se que o bem jurídico tutelado não necessita de uma aplicação penal neste caso de infração. Também argumentado anteriormente, os *scans* podem ser tratados como dívida civil, sendo matéria tutelada pelo Direito Civil e consequentemente, dispensando medidas penais. Portanto, é viável a aplicação do princípio da intervenção mínima.

4. Das complicações e possíveis soluções cibernéticas

Mesmo com o agravamento das penalidades que envolvem a pirataria virtual, as versões ilegais das obras continuam de fácil acesso nas comunidades virtuais, através da tecnologia *peer-to-peer*, discussões privadas em fóruns de mangás e por publicação dos *scans* de leitores que possuíam cópias dos arquivos. Esta profunda cadeia de cibercultura só é possível devido aos mecanismos encontrados em âmbito virtual. Ademais, a tecnologia necessária para identificar os infratores dos direitos autorais é limitada tanto em sua funcionalidade e onerosa demais para ser mantida pelas editoras de mangás, resultando na impunidade da prática de *scanlation*.

Há casos também em que serviços de hospedagem de certas empresas facilitam a propagação dos *scans*. Por exemplo, o *Cloudflare* disponibiliza um serviço de CDN –rede de distribuição de conteúdo– em que resulta no velamento do endereço IP do servidor provedor. Por causa desta ferramenta e por conta da falta de identificação do operador no *Cloudflare*, muitos grupos de *scan* se utilizam da plataforma para publicar suas traduções, evitando serem identificados e consequentemente, penalizados. A utilização de *Cloudflare* para esta prática é tão popular que 4 editoras japonesas processaram a empresa no va-

lor de, aproximadamente, 12,3 bilhões de reais⁸ por infringir os seus direitos de *copyright* por contribuir com a pirataria de suas obras.⁹

Contudo, o ciberespaço não só criou complicações como também possibilita soluções para o embate do *scanlation* exacerbado. A opção de assinatura à leitura de mangás via streaming é bastante utilizada, sendo uma forma de facilitar o acesso às obras legalmente, respeitando os direitos autorais dos autores. Um dos serviços de streaming mais populares no Brasil deste nicho é o Mangamo¹⁰, que possui mais de 300 títulos. Porém, é importante frisar que estes aplicativos de assinatura possuem pouquíssimas obras traduzidas para português e como já foi dito, não consegue acompanhar a circulação de mangás publicados no Japão e com isso, acaba selecionando títulos mais populares e ignorando certos gêneros que não são buscados pelo leitor comum. Dessa forma, mesmo sendo uma boa iniciativa, o aplicativo não supre a demanda dos leitores de nicho e nem facilita o acesso à leitura para os indivíduos que não tem fluência em inglês.

Considerações finais

A expansão global do consumo de mangás só foi possível devido à quebra das barreiras físicas e linguísticas que as traduções feitas por fãs realizaram ao divulgar seu trabalho no ciberespaço. Como é abordado por Lessig (2004), a prática de *scans* não se equivale ao prejuízo provocado por outras modalidades de cópias, visto que sua motivação não é financeira. Afinal, o mercado brasileiro de mangás só consegue se expandir devido ao aumento de suas vendas e a divulgação online das obras não impede de que há a sua aquisição em formato físico. Pelo contrário, a leitura digitalizada cria uma base de fãs que solicitam o licenciamento do produto para vir a consumir a obra legalmente.

Fica claro que a perspectiva japonesa é de se considerar o *scanlation* como uma problemática e que a sua estratégia de aplicar penas mais severas não é uma solução viável, visto que os meios eletrônicos inviabilizam a retirada total do conteúdo pirateado no ciberespaço e/ou dificultam a identificação dos

8. Valor referente à cotação do iene de R\$0,037 em 16 de abril de 2022.

9. LUSTER, Joseph. **Japanese Publishers to Sue Cloudflare for Hosting Servers for Pirated Manga Sites**. Crunchyroll, News, 02 de fevereiro de 2022. Disponível em: <https://www.crunchyroll.com/pt-br/anime-news/2022/02/02-1/japanese-publishers-to-sue-cloudflare-for-hosting-servers-for-pirated-manga-sites> Acesso em: mar. 2022

10. YUGE, Claudio. **App de assinatura de mangás Mangamo chega ao Android com investimento da Sony**. Canaltech, Entretenimento, Quadrinhos, 25 de novembro de 2020.

infratores. As editoras nipônicas, mesmo observando os obstáculos tecnológicos para responder o avanço do *scanlation* através de medidas legais, continuam investindo no agravamento de sua legislação penal invés de procurar meios de suprir a demanda internacional como facilitar o licenciamento de obras ou permitir a realização de publicações simultâneas pelo globo. Uma outra proposta viável para retardar a circulação de scans no âmbito virtual seria a criação de aplicativos de assinatura de mangás pelas revistas japonesas e através desta plataforma publicar todas as obras que possuem reprodução física, disponibilizando a tradução da obra para todas as línguas.

Na perspectiva brasileira, se for analisar pela solução asiática, se encontra em um ambiente jurídico de incertezas quanto à penalização dos *scans*. Afinal, sua tipificação é entrelaçada pela ofensa aos direitos autorais de cunho moral do autor e como foi explanado, os *scans* são realizados somente para divulgar e incentivar a compra da obra, o que é de maior interesse para o autor. Logo, não há infração moral e por não ter o intuito de lucro, as traduções não podem ser consideradas condutas que venham a ofender o direito autoral patrimonial do autor. Além disso, as editoras nacionais se encontram com dificuldades de morosidade de suas traduções, problema estrutural de emissão dos volumes pelo Brasil e preços exorbitantes, ocasionando o *scanlation* uma fonte de leitura recorrente para os admiradores de quadrinhos japoneses. Desse modo, se instaura uma cultura de *scans*, fazendo com que a prática seja adequadamente legal na sociedade, implicando em uma baixa lesividade da infração do bem tutelado e buscando solucionar o impasse em esferas jurídicas divergentes da penal.

Em suma, é preciso que se enxergue a prática de tradução feita por fãs de outra maneira, buscar incentivos para que os leitores adquirirem a obra física e não os amedrontar por consequências jurídicas.

Referências

BARBOSA, Rômulo Oliveira. **Os mangás e a prática de scanlation no context de convergência midiática**. Monografia. Universidade Federal do Ceará, Instituto de Cultura e Arte, Fortaleza, 2019. Disponível em: https://repositorio.ufc.br/bitstream/riufc/49785/1/2019_tcc_robarbosa.pdf Acesso em: jan. 2022

CAZAROTI, Tatiane Martins Barros. **Crimes Cibernéticos**. Monografia. Centro Universitário Várzea Grande, 2016. Disponível em: <https://www.repositoriodigital.univag.com.br/index.php/rep/article/view/203/235> Acesso em: jan. 2022

COPYRIGHT RESEARCH AND INFORMATION CENTER (CRIC). **Copyright Law of Ja-**

pan. Disponível em: <https://www.cric.or.jp/english/clj/cl2.html> Acesso em: jan. 2022

GRECO, Rogério. **Código Penal: comentado**. – 11. ed. – Niterói, RJ: Impetus, 2017.

HIRATA, Tatiane. **Mangá: do Japão ao mundo pela prática midiática do scanlation**. Dissertação (mestrado) Universidade Federal de Mato Grosso, Instituto de Linguagens, Programa de Pós-Graduação em Estudos de Cultura Contemporânea. Cuiabá, 2012. Disponível em: https://ri.ufmt.br/bitstream/1/550/1/DISS_2012_Tatiane%20Hirata.pdf Acesso em: jan. 2022

HIRATA, Tatiane; GUSHIKEN, Yuji. **Scanlation: reprodução e consumo subalterno de mangá na cibercultura**. Revista Líbero, n.30, p. 127 -137. Dezembro de 2012. Disponível em: <https://casperlibero.edu.br/wp-content/uploads/2014/05/9-Scanlation.pdf> Acesso em: jan. 2022

JENKINS, Henry. **Why Participatory Culture is not Web 2.0: Some Basic Distincts** Disponível em : <[http:// henryjenkins.org/2010/05/why_participatory_culture_is_n.html](http://henryjenkins.org/2010/05/why_participatory_culture_is_n.html) > Acesso em: jan. 2022

LANDERS, Sydney. **Gotta Catch ‘Em All!: The National Diet’s Inadequate Attempt to Control Manga Pirates**, 76 U. MIA L. Rev. 251. Disponível em: <https://repository.law.miami.edu/umlr/vol76/iss1/6> Acesso em: jan. 2022

LEE, Hye-Kyung. **Between fan culture and copyright infringement: manga scanlation**. In: Media Culture & Society. 2009 ; Vol. 31, No. 6. pp. 1011 -1022. Disponível em: <https://kclpure.kcl.ac.uk/portal/files/4682147/lee%2520between.pdf> Acesso em: jan. 2022

LESSIG, Lawrence. **Cultura Livre**. São Paulo: Editora Trama, 2005. Disponível em: <https://www.ufmg.br/proex/cpinfo/educacao/docs/10d.pdf> Acesso em: jan. 2022

LUYTEN, Sonia Bibe (org). **Cultura Pop Japonesa – Mangá e anime**. São Paulo: Hedra, 2005.

MUSSARELLI, F. **A análise de quadrinhos japoneses sob a ótica de Bakhtin : o mangá como material de referência para a cultura japonesa / Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2013. 165 f.** Disponível em: <https://repositorio.ufscar.br/bitstream/handle/ufscar/1116/5074.pdf?sequence=1> Acesso em: jan. 2022

NETO, Osmar Marques. **Pirataria Digital à luz do Princípio da Intervenção Mínima e a aplicabilidade do Direito Civil visando a proteção dos Direitos Autorais**. Monografia. Universidade do Extremo Sul Catarinense, UNESC. Criciúma, 2019. Disponível em: <http://repositorio.unesc.net/handle/1/7574> Acesso em: jan. 2022

PARANAGUÁ, Pedro; BRANCO, Sérgio. **Direitos Autorais**. Rio de Janeiro: Editora FGV, 2009. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2756/Direitos%20Autorais.pdf> Acesso em: jan. 2022

RAMOS, A. A. **Aspectos da cultura japonesa representados no herói do mangá One Piece: análise dos conceitos de hierarquia, yakuza, on e giri**. Tese (doutorado)-Faculdade de filosofia, Letras e Ciências Humanas da Universidade de São Paulo. São Paulo, 2018. Disponível em: <https://www.teses.usp.br/teses/disponiveis/8/8157/tde-07052018-113226/pt-br.php> Acesso em: jan. 2022

ROSA, P. N. M. . **Crimes relativos aos direitos autorais: uma análise a partir das perspectivas de racionalidade legislativa e bem jurídico**. In: CONPEDI/UFPB. (Org.). Direito penal, processo penal e constituição II. 1ed. Florianópolis: CONPEDI, 2014, v. 02, p. 420-445. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=77ebef784ecdb4ce> Acesso em: jan. 2022

SANTOS, Manuella. **Direito autoral na era digital: impactos, controvérsias e possíveis soluções**. São Paulo: Saraiva, 2009. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp063159.pdf> Acesso em: jan. 2022

VIANNA, Túlio Lima. **A ideologia da propriedade intelectual: a inconstitucionalidade da tutela penal dos direitos patrimoniais de autor**. Revista dos Tribunais. São Paulo, v. 95, n. 845, p. 443-456, mar. 2006. Disponível em: http://www.inf.ufsc.br/~jose.lucca/A_ideologia_da_propriedade_intelectual.pdf Acesso em: jan. 2022



Acesse nossas redes



itsrio.org

Este livro foi composto nas fontes Termina,
FreightSans Pro e Public Sans e lançado pelo Instituto
de Tecnologia e Sociedade, em outubro de 2022.