DIREITO E INOVAÇÃO

Volume 1

Criptoativos, Fintechs, Online Disput Resolution (ODR), Análise de Dados e Inteligência Artificial e a Lei Geral de Proteção de Dados e Privacidade

OAB PARANÁ
COMISSÃO DE INOVAÇÃO E GESTÃO
CAIXA DOS ADVOGADOS DO PARANÁ
ESA ESCOLA SUPERIOR DE ADVOCACIA

EXPEDIENTE

Direito e Inovação
Criptoativos, Fintechs, Online Disput Resolution (ODR), Análise de Dados e Inteligência Artificial e a Lei Geral de Proteção de Dados e Privacidade

Ordem dos Advogados do Brasil – Seção do Paraná Diretoria OAB/PR – Gestão 2019-2021
Cassio Lisandro Telles (Presidente)

Marilena Indira Winter (Vice-Presidente)

Rodrigo Sanchez Rios (Secretária-Geral)

Christhyanne Regina Bortolotto (Secretário-Geral Adjunto)

Henrique Gaede (Tesoureiro)

Alexandre Salomão (Diretor de Prerrogativas)

Escola Superior de Advocacia
Adriana D´Avila Oliveira (Coordenadora Geral da ESA-PR)

Marília Pedroso Xavier (Coordenadora de Direito Privado da ESA-PR)

Francisco Zardo (Coordenador de Direito Público da ESA-PR)

Conselho Editorial
Rhodrigo Deda Gomes

Editor
Rafael Aggens Ferreira da Silva

Revisão
Rhodrigo Deda Gomes

Rafael Aggens Ferreira da Silva

Mariana Pereira Faria

Diagramação
Rafael Alvares

Endereço postal
Ordem dos Advogados do Brasil – Seção do Paraná

Escola Superior de Advocacia

Rua Brasilino Moura, 253 – Ahú

80.540-340 – Curitiba - Paraná

Distribuição

Gratuita

Versão eletrônica disponível para download

SUMÁRIO

1. PREFÁCIO 05
2. A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA NA PRÁTICA EMPRESARIAL 06
3. A CRIAÇÃO DA AUTORIDADE NACIONAL DA PROTEÇÃO DE DADOS NO ÂMBITO DA LGPD: análise ontológica da experiência brasileira 21
4. FINTECHS E MEIOS DE PREVENÇÃO AO CRIME DE LAVAGEM DE DINHEIRO 39
5. FUTUROS POSSÍVEIS NO SISTEMA FINANCEIRO BRASILEIRO: arranjos de pagamento, fintechs e pagamentos instantâneos 57
6. EXCHANGES DE CRIPTOMOEDAS X BANCOS: uma questão de direito concorrencial? 73
7. SOBRE A CONSULTA PÚBLICA Nº 06/2018, DA RECEITA FEDERAL DO BRASIL E SEUS PONTOS POLÊMICOS 89
8. A TUTELA DAS INSTITUIÇÕES FINANCEIRAS BRASILEIRAS EM FACE AOS RISCOS ENVOLVIDOS NO INVESTIMENTO EM CRIPTOMOEDAS E DAS INITIAL COIN OFFERINGS (ICO'S) 102
9. ANÁLISE PREDITIVA DE DADOS E SUAS APLICAÇÕES NO DIREITO 114
10. INTELIGÊNCIA ARTIFICIAL E O DIREITO: CASES ATUAIS E CENÁRIOS FUTUROS 139
11. INTELIGÊNCIA ARTIFICIAL: MITOS E REALIDADE 154
12. ONLINE DISPUTE RESOLUTION (ODR) EM PERSPECTIVA INTERNACIONAL E ANÁLISE CRÍTICA 173

PREFÁCIO

Este livro temático de nossa Escola Superior de Advocacia – ESA representa parte do esforço da OAB-PR em construir de forma colaborativa conhecimento jurídico aprofundado envolvendo direito, tecnologia e inovação. Os artigos apresentados são fruto de reflexões e debates que ocorreram nos Grupos Permanentes de Discussão, um formato de trabalho e estudo que foi aprendido com a Comissão da Advocacia Iniciante – CAI e que tem trazido bons resultados para a nossa comunidade.

O avanço tecnológico é inexorável, mas será a forma como os advogados lidam com ele que fará toda a diferença. Isso não quer dizer que os operadores do direito precisam sair desenvolvendo teses sobre direito e tecnologia de forma tresloucada toda vez que surge uma novidade legislativa no horizonte. No afã de acreditar que os mais rápidos levam tudo, acabam por gastar a energia que poderiam aplicar de forma incisiva e com a intensidade adequada em iniciativas que farão significativa transformação em suas carreiras.

Lidar com tecnologia e direito, neste final da segunda década do Século XXI, é antes de tudo fazer parte de uma comunidade que busca incessantemente a excelência, trabalhando de forma colaborativa para que todos possam se desenvolver juntos. A opção por um arranjo dessa natureza advém das questões que a inovação e a transformação digital impõem ao mundo do direito – é preciso aprender muitos temas, rapidamente e com profundidade.

Mesmo quando é possível fazer tudo isso sozinho, o que é uma tarefa enorme, não é sensato. A sociedade vem aprendendo a se relacionar em rede, o que significa fragmentação e individualismo, mas, também, comunhão de propósitos e solidariedade. E é com essa visão, de que a reflexão em grupo sobre o direito, a tecnologia e a inovação tornou-se uma abordagem poderosa para desenvolver conhecimento jurídico, que são apresentados os trabalhos dessa primeira edição.

Isso não seria possível sem o integral apoio da ESA e a confiança da Diretoria da OAB-PR nesta gestão e na anterior. A aprovação dos Grupos Permanentes de Discussão pela diretoria, o fornecimento de estrutura e apoio para a realização das reuniões, a publicação de trabalhos deles decorrentes pela ESA são, sem dúvida nenhuma, prova de que boas coisas acontecem quando todos partilham de um propósito comum.

A advocacia paranaense tem demonstrado estar comprometida com a ideia de desenvolver profundo conhecimento jurídico em toda a sorte de áreas em que a tecnologia adentra. Os artigos que compõem esta publicação são prova disso. Contudo, talvez, a evidência mais clara do compromisso da comunidade seja o apoio da CAI, parceira de primeira hora em todas as iniciativas que a Comissão de Inovação e Gestão vem realizando.

A publicação desta revista jurídica online, dada a quantidade de pessoas envolvidas para a sua realização, requer especiais agradecimentos à Diretoria da OAB-PR e à ESA, mas, também à CAI, aos setores de Eventos, de Comissões e de Comunicação, além dos demais funcionários da Ordem, que diuturnamente colaboram para a realização das atividades dos Grupos Permanentes de Discussão. Um especial agradecimento também aos coordenadores desses grupos, que desenvolvem as atividades com ânimo e disposição, por acreditar que o Paraná pode contribuir no âmbito nacional e internacional com conhecimento de qualidade sobre direito, tecnologia e inovação.

Rhodrigo Deda Gomes – Presidente da Comissão de Inovação e Gestão da OAB-PR

Rafael Aggens Ferreira da Silva – Secretário da Comissão de Inovação e Gestão da OAB-PR

Mariana Pereira Faria – Diretora de Comunicação da Comissão de Inovação e Gestão da OAB-PR

A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA NA PRÁTICA EMPRESARIAL

THE BRAZILIAN GENERAL DATA PROTECTION LAW ON BUSINESS ACTIVITY

ANA PAULA DE OLIVEIRA
Advogada, pós-graduanda em Direito Civil e Direito Processual Civil pela Unicuritiba, pós-graduanda em Direito do Trabalho e Direito Previdenciário pela UNISC; Membro da Comissão de Compliance da OAB/PR, Membro do Comitê Brasileiro de Compliance e Membro da Comissão de Processo Disciplinar da Federação Paranaense de Futebol.

DÂNTON ZANETTI
Advogado, pós-graduado em Direito Processual Civil pela PUC-PR, pós-graduado em Direito e Processo do Trabalho pela Unicuritiba, Professor na Faculdade de Direito Santa Cruz. Membro da Comissão de Inovação e Gestão da OAB/PR.

FLÁVIO SANTOS LIMA
Advogado, Membro da Comissão de Inovação e Gestão da OAB/PR. Advogado e Consultor na Oystr Robôs Inteligentes.

THEMIS ORTEGA SAMPAIO
Advogada, pós-graduada em Direito Contemporâneo pela FEMPAR, pós-graduada em Direito Civil e Direito Processual Civil pela Unicuritiba, Membro da Comissão de Inovação e Gestão da OAB/PR e Membro do Comitê Brasileiro de Compliance.

RESUMO:

A Nova Lei Geral de Proteção de Dados, que passa a ter vigência em agosto de 2020, surgiu como um desafio para as empresas que lidam com dados pessoais. Diante disso, nasce a necessidade de entender quais serão os caminhos para a adaptação dessas instituições. Assim, o objetivo do artigo consiste em apresentar medidas que devem ser observadas pelos empresários para estar em conformidade (*Compliance)* com a lei e proteger os usuários efetivamente. Outrossim, observou-se questões como a função do termo de uso e das políticas de privacidade, e o papel do DPO, que recai sobre a figura do encarregado.

Palavras-chave: Proteção de Dados; *Compliance*; Atividade Empresarial.

Sumário: 1.Introdução; 2. A Lei Geral de Proteção de Dados Brasileira em *Compliance*; 3. O Novo Papel dos "Termos de Uso" e das "Políticas de Privacidade" de Acordo com a LGPD; 4. A Figura do *Data Protection Officer (DPO);* 5. Conclusão; 6. Referências Bibliográficas.

Abstract:

The new Brazilian General Data Protection Law, which will become effective in August of 2020, has emerged as a challenge for companies that deal with data personal. In this scenario, arises the need to understand the ways of adapting these institutions. Thus, the purpose of this paper consists in presenting measures that should be observed by entrepreneurs to comply with the law and protect users effectively. As measures to be taken in the adapting process, relevant questions such as the function of the "Terms of Use" and "Privacy Policies" and the role of the DPO, which falls on the person in charge of personal data treatment are being presented in this study.

Keywords: Data Protection, Compliance, Business Activity;

Summary: 1.Introduction; 2. The New Brazilian General Data Protection Law in Compliance; 3. The New Paper of the Terms of Use and Privacy Policies; 4 The Data Protection Officer (DPO) Figure; 5. Conclusion; 6. Bibliographic References.

1. INTRODUÇÃO

O desenvolvimento tecnológico experimentado pela sociedade nas últimas décadas, ofusca o fato de que um longo percurso histórico teve de ser percorrido até que a privacidade pudesse ser reconhecida como um bem jurídico digno de tutela Estatal, atribuindo-se aos juristas norte-americanos Samuel D. Warren e Louis D. Brandeis o primeiro artigo científico dedicado ao tema, intitulado *"The Right to Privacy"*, do ano de 1890.[5]

No referido escrito os autores sustentam que os direitos individuais derivariam da proteção da *pessoa* ou da *propriedade*, e, de tempos em tempos, alterações no cenário político, social e econômico fariam necessário reavaliar a natureza e extensão de tais bens jurídicos. Nesta esteira, ressignificando o direito à vida em face da mais nova ameaça tecnológica da época – as câmeras fotográficas instantâneas utilizadas pela imprensa – Warren e Brandeis reconhecem a privacidade como "o direito de ser deixado só".

Desde então, com a evolução das tecnologias, paulatinamente a privacidade, foi ganhando importância e reconhecimento jurídico no cenário internacional, valendo citar, exemplificativamente, documentos expressivos como a Convenção Americana dos Direitos e Deveres do Homem, de 1948, cujo artigo V estatui que "Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar"[2], e a Declaração Universal dos Direitos Humanos, do mesmo ano, que no artigo 12 expressa que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".[3]

A preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela "Quarta Revolução Industrial", cujo tom é dado pelo fenômeno da "informacionalização da sociedade", iniciado na década de 1970. Seus reflexos impactam diretamente tanto a atividade econômico-empresarial, quanto a atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações.[4]

Diante dessa transformação exsurge a necessidade de regulamentar o uso dos dados, fenômeno que vem inspirando a edição de leis e regulamentações específicas sobre a matéria a nível global.

No Brasil, o acesso à internet é garantido por força da Lei 12.965/2014 (o "Marco Civil da Internet"), que em seu artigo 7º prevê que o "O acesso à internet é essencial ao exercício da cidadania". Mais recentemente, em 14 de agosto de 2018, foi promulgada a Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGDP), responsável por aprofundar a regulamentação das questões relativas ao tratamento de dados pessoais no cenário nacional.

Os impactos desta nova norma são expressivos, tanto no aspecto da tutela da privacidade e proteção dos dados pessoais de seus respectivos titulares, quanto, naturalmente, para a

---

[5] WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, Vol. 4, Nº. 5. 1890, p. 193-220.

[2] Disponível em: <https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm>; Acesso em 07.01.2019.

[3] Disponível em: <https://www.unicef.org/brazil/pt/resources_10133.html>; Acesso em 07.01.2019.

[4] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2018, p. 13-15.

atividade empresarial, considerando que a LGPD impõe uma série de diretrizes para que o tratamento de dados seja realizado de forma lícita.

No presente estudo, sem a pretensão de esgotar o tema, serão abordadas algumas medidas consideradas necessárias para a adaptação das empresas diante deste novo cenário. Inicialmente, trata-se da instauração de Programas de *Compliance*, com observância de boas práticas, incluindo os princípios fundamentais, gestão de risco e até mesmo a aplicação da ISO 27001.

Em seguida, passa-se a analisar a tessitura de documentos como os "Termos de Uso" e "Políticas de Privacidade", largamente utilizados em serviços *online*. Por fim, analisa-se a figura do *Data Protection Officer (DPO)*, que recai na pessoa que exerce a função de encarregado.

2. A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA EM COMPLIANCE

A nova Lei Geral de Proteção de Dados, publicada em agosto de 2018, trouxe novos desafios para as empresas que lidam com dados pessoais. Até a sua entrada em vigor, as pessoas naturais e jurídicas que estejam sob sua abrangência devem se adequar às novas exigências legais.

Inicialmente, o empresário que usa, coleta ou armazena dados de qualquer pessoa deve observar, além da boa-fé, os princípios trazidos pela Lei 13.709/2018, no art. 6º, para se manter em *compliance*[5]. Tais princípios apresentam-se discriminados com sua aplicação prática, o que facilita a sua incorporação pelas políticas de proteção de dados.

Pode-se dizer que esses princípios foram desenvolvidos por meio de instrumentos internacionais e transnacionais, a partir do novo contexto da privacidade ligada à proteção dos dados pessoais[6] e trazidos para a legislação brasileira. Tratam-se de princípios fundamentais dos cidadãos e devem ser efetivados pelas instituições que manipulam dados. Diante disso, busca-se aqui demonstrar a concretização dos princípios mais relevantes, que servem de base para a efetividade dos demais princípios, sendo eles o princípio da finalidade, da transparência, da qualidade de dados e da segurança.

O princípio da finalidade determina que é necessária uma correlação entre o uso dos dados pessoais e o fim comunicado aos titulares quando do momento da coleta. Assim, é possível limitar o acesso de terceiro às informações coletadas. Outrossim, também serve para definir a adequação e razoabilidade do uso de dados. Para o cumprimento deste princípio, deve a instituição estabelecer de forma expressa e limitada "a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas"[7].

Já o princípio da transparência, para se tornar efetivo, precisa que os bancos de dados sejam de conhecimento público. Esta ideia reafirma o preceito democrático de incompatibilidade de bancos de dados sigilosos com um Estado Democrático de Direito. Ademais, a transparência também permite o combate de práticas abusivas a partir do uso dos dados. Para estar em conformidade com esse relevante princípio, as empresas devem publicar seu nome, sede e conteúdo juntamente com o banco de dados. Essas publicações podem ser feitas em "registros públicos, diários oficiais ou meios de grande circulação sob pena de ineficácia desse direito"[8].

Ainda, importante ressaltar o princípio da qualidade dos dados. Este exige que as informações tenham tratamento leal e lícito, além de estarem adequados à finalidade declarada e possuindo conteúdo objetivo, exato e atualizado. Para isso, as empresas que tratam dados devem ter cautela com a sua gestão[9], mantendo-os sempre atualizados. Assim, é necessário que se disponha de instrumentos para garantir os direitos de acesso, retificação e cancelamento dos dados[10].

---

[5] Conformidade (tradução livre).

[6] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. p. 70.

[7] Ibidem, p. 71

[8] Idem.

[9] "A Gestão de Identidades e Acessos compreende um conjunto de processos para gerenciar todo o ciclo de vida dos acessos dos usuários, internos ou externos, dentro de uma organização" (SILVA, Felipe. **Gestão de Identidades e Acessos.** In. In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p.73).

[10] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. p. 72

Ademais, imperioso comentar acerca do princípio da segurança, que para ser efetivo precisa de meios que possibilitem a proteção dos dados pessoais contra extravios, destruições, modificações e desvios não autorizados por seus titulares. Decorrente disto, surge o princípio da responsabilização e prestação de contas, "que visa assegurar a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade"[11]

Nesse panorama, os Programas de Integridade (C*ompliance*) têm se mostrado como um ótimo caminho para superar todos os desafios de adequação, revelando-se, ainda, como estratégia para minimizar os riscos reputacionais e legais das empresas[12].

Diante da necessidade de uma atuação multidisciplinar especializada, que demanda estrutura tecnológica de segurança da informação, governança normativa e contratual, e ainda capacitação de equipes, há a exigência de ação imediata por parte das empresas.

Importante observar que o programa ou sistema a ser adotado, poderá ser proporcional ao porte da corporação, bem como aos riscos que ela enfrenta.

Sobre esse aspecto, a Portaria Conjunta da CGU e do Ministério da Micro e Pequena Empresa n. 2279/2015 aponta medidas de integridade com um rigor formal mais simples, a fim de garantir o comprometimento com a ética e a integridade entre as microempresas e empresas de pequeno porte[13]. Desmistifica-se assim o preceito de que "*compliance tem um custo elevado demais*" para estas empresas, tendo em vista que é possível adequá-lo às necessidades especiais de cada companhia.

Em linhas gerais, quanto maior a corporação, e maiores os riscos a que a esta estará submetida, mais complexa é a tarefa de incorporar um sistema de cumprimento normativo[14].

Em se tratando de riscos, as penalidades provenientes do descumprimento da Lei podem ser bastante danosas. São os casos, por exemplo, da publicização da infração, da aplicação de multa diária única, ou ainda de multa de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Estima-se assim que a adequação, de fato, não será tarefa fácil[15], porém a falta dela poderá importar em prejuízos incomensuráveis. Ponderando-se que o c*ompliance* tem objetivos tanto preventivos, quanto reativos[16], tais danos podem ser consideravelmente reduzidos.

Neste ínterim, tratando-se em definitivo das diretrizes de um Programa de Integridade, é possível defini-lo sob três etapas: A primeira, correspondente à formulação, ou seja, análise e valoração de riscos, definição de medidas de prevenção e a criação de uma estrutura de *compliance*. A segunda, implementação, ou seja, comunicação e detalhamento do programa, consistente em medidas organizacionais para criação de processos de *compliance*. A terceira,

---

[11] Idem.

[12] VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017. p.104.

[13]Ibidem. p.174.

[14]VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.p.276.

[15] FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial**, 2018. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018> Acesso em: 29/09/2018.

[16] VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017. p.91.

por fim, abrangendo a consolidação e aperfeiçoamento, estabelecendo um processo para apuração de violações, critério de sanções e avaliação continuada e aperfeiçoamento do programa[17].

No que tange a gestão dos riscos, consiste num processo estruturado[18]. Levantam-se os ímpetos possíveis do negócio para, em seguida, dar sequência às demais etapas, buscando formas de reduzir ou eliminar seus efeitos como, por exemplo, coibir severos danos à imagem da empresa, no caso de um eventual vazamento de dados.

BARROS aponta que "risco é composto de dois grandes componentes: a probabilidade de ocorrência e a magnitude de perda", sendo que esta última consiste em "impacto"[19]. Nesse contexto, a probabilidade de ocorrência pode ser representada pela frequência do evento danoso – ou ameaça – em determinado período de tempo. Quanto ao impacto, se revela no "comprometimento de uma das propriedades básicas da segurança de informação: confidencialidade, integridade e disponibilidade"[20].

No que tange os mecanismos para desenvolver a conformidade com a Lei Geral da Proteção de Dados, o grupo de normas 27000, publicada pela *International Organization for Standardization (ISO),* pode-se mostrar também como importante e moderna ferramenta de proteção de dados. Estas normas definem requisitos para um sistema de gestão de segurança da informação (SGSI) bem como sua operação, em especial a ISO 27001[21].

Referida normativa trata-se de padrão internacional reconhecido e validado para segurança de informação. Entre outros aspectos, segue um sistema de gestão que avalia riscos de segurança e proteção, adota procedimentos de controle, e monitora o desempenho dos processos, atuando assim em sintonia e reforçando os programas de integridade que visam a proteção de dados e privacidade.

Assim, considerando-se os riscos do negócio e os preceitos basilares dos programas de integridade, como prevenção, processamento de informações sensíveis, e treinamento de colaboradores, pode-se enquadrar a Lei Geral da Proteção de Dados, perfeitamente como um tema de *compliance.*

Diante disso, para se manter em *compliance* efetivamente*,* as instituições ainda devem observar outras questões práticas, a exemplo da elaboração de um adequado Termo de Uso e de Políticas de Privacidade.

---

[17]Ibidem, p.277.

[18] BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p. 38.

[19]BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p. 39.

[20] Ibidem, p. 40.

[21] Ibidem, p. 52.

3. A FUNÇÃO DOS TERMOS DE USO E DAS POLÍTICAS DE PRIVACIDADE

Com o advento da LGPD, quebra-se um verdadeiro paradigma na cultura de proteção meramente formal da privacidade do titular de dados, e inaugura-se uma nova etapa em que se impõe a tutela material dos dados pessoais tratados em ambiente digital ou fora dele.

Isto porque, se mesmo no âmbito das relações digitais estabelecidas via *internet* havia legislação própria para regular o tema da proteção de dados– ainda que de forma incompleta, considerando que a questão da proteção de dados até então era regida pela Lei nº 12.965/2014, conhecida como "Marco Civil da *Internet*" – verificava-se abuso contumaz praticado por empresas na coleta, tratamento e exploração de dados pessoais. O cuidado no tratamento de dados realizados fora do meio digital, então, não se sujeitava a qualquer controle mínimo, mesmo havendo outras normas dispostas em leis esparsas, como o Código de Defesa do Consumidor e as leis do Cadastro Positivo (nº 12.414/2011) e de Acesso à Informação (nº 12.527/2011), sem olvidar da garantia fundamental à vida privada, assegurada no artigo 5º, X, da Constituição Federal.

A referida mudança de paradigma, traz impactos relevantes à atividade empresarial, mormente considerando que nesta "Quarta Revolução Industrial", que tem como traços marcantes a velocidade, amplitude, profundidade e impacto sistêmico (SCHWAB, 2016)[22], as relações sociais cada vez mais se desenvolvem digitalmente, razão pela qual os grandes bancos de dados, atualmente, são mantidos em nuvens (*cloudcomputing*) e outras espécies de bancos de dados exclusivamente digitais, ganhando enorme relevo atividades de '*Data Mining'* (mineração de dados)[23] e o chamado '*Big Data'* (grande volume de dados)[24], por exemplo.

Este fenômeno se deve muito em razão do amadurecimento nas últimas décadas da importância da *informação* como ativo dotado de valor financeiro e de mercado, considerados, sobretudo, os aspectos da 'maleabilidade' e 'utilidade' da informação, que exponenciam sua influência sobre as tomadas de decisão e a vida cotidiana em geral. Na análise de DONEDA, o efeito disso foi uma crescente expansão de atividades empresariais ligadas à exploração de dados, sistematização da informação e formação de bancos de dados.[25]

---

[22] SCHWAB, Klaus. **A quarta revolução industrial**. Tradução por Daniel Moreira Miranda. São Paulo: Edipro, 2016.

[23] Segundo FREITAS e PAMPLONA (2018, p. 8), *"*A Mineração de Dados (*Data Mining*) tem como objetivo atender estas expectativas e pode ser definida por Fayyad, Piatetsky-Shapiro e Smyth (1996, p. 39-40) como *'nontrivialprocessofidentifyingvalid, novel, potentiallyusefulandultimatelyunderstandablepatterns in data'".*

[24] Conforme FRANÇA, "Os dados das redes sociais online podem ser usados para extrair informações sobre padrões de interações interpessoais e opiniões. Esses dados podem auxiliar no entendimento de fenômenos, na previsão de um evento ou na tomada de decisões. Com a ampla adoção dessas redes, esses dados aumentaram em volume, variedade e precisam de processamento rápido, exigindo, por esse motivo, que novas abordagens no tratamento sejam empregadas. Aos dados que possuem tais características (volume, variedade e necessidade de velocidade em seu tratamento), chamamo-los de Big Data."(FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J.. BigSocial Data: Princípios sobre coleta, tratamento e análise de dados sociais. Artigopublicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2014.Curitiba. 2014, p. 8. Disponível em:<http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf>. Acesso em 10/10/2018.

[25] DONEDA, Danilo. **Proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília: SDE/DPDC. 2010, p. 22.

Uma das consequências diretas deste modelo relacional é a proliferação dos documentos intitulados "Termos de Uso" e "Política de Privacidade", que se propõem a reger as relações dos usuários de *sites* e serviços de *internet*, inclusive no que tange às ações ligadas ao tratamento de dados pessoais, desde a coleta, passando pelo armazenamento, até sua eliminação.

Para CAVALCANTI e SANTOS (2018), "Torna-se, portanto, obrigatório adotar, desde a concepção de serviços, produtos e modelos de negócio, a prática de se garantir direitos de proteção à privacidade e aos dados pessoais. São os chamados *privacy by design* e *by default*"[26], em que o primeiro modelo permite uma adequação do formato e níveis de privacidade a ser cedida por determinado usuário, enquanto o segundo não se concebe tal possibilidade.

Com efeito, ainda é insipiente na doutrina e na própria jurisprudência pátria discussões mais aprofundadas a respeito da natureza jurídica e efeitos emanados dos documentos intitulados "Termos de Uso" e "Política de Privacidade".

Nada obstante, é possível amolda-los às ferramentas já existentes no ordenamento jurídico pátrio, em especial às normas pertinentes aos contratos de adesão, cuja principal característica é a existência das figuras do proponente e do aderente. O primeiro é o responsável por estabelecer cláusulas e condições contratuais, enquanto o segundo tem apenas a opção de aceitar ou rejeitar o contrato como um todo, abrindo mão da possibilidade de negociar os termos do contrato. Nas palavras de RIBEIRO e GALESKI JUNIOR (2015):

> "Nos contratos de adesão, a liberdade na fixação do conteúdo contratual, entendida como liberdade privada do contratante e contratado é parcialmente afastada, por não resultarem do livre debate entre as partes, mas provirem do fato de uma delas aceitar tacitamente cláusulas e condições previamente estabelecidas pela outra."[27]

As definições acima são inteiramente aplicáveis aos Termos de Uso e Políticas de Privacidade, eis que um determinado internauta, ao acessar um *site* de seu interesse – e, portanto, estabelecer uma relação com dada empresa, fornecedora de serviços – tem pouca, ou mesmo nenhuma possibilidade de influir na redação e nos efeitos de qualquer das cláusulas dispostas nos documentos mencionados. Resta-lhe apenas aceitá-los nos moldes em que se encontram propostos, ou rejeitá-los e, assim, ter seu acesso a informação, conteúdos, produtos, serviços, etc., limitado ou até mesmo impedido.

De outro lado, a empresa titular de determinado domínio de *internet*, ou aplicativo, mesmo atualmente, enquanto sujeita às disposições legais previstas no Marco Civil da *Internet*, tem o dever de informar àqueles que navegam em seu *site* a respeito dos dados pessoais que pretende tratar, o que, como visto, comumente é disposto nos Termos de Uso e Políticas de Privacidade.

Analisando a natureza desta relação adesiva é bem-vinda a lição de MAGRANI (2014, p. 158) ao afirmar que, "malgrado tratar-se de espaços privados, os usuários não podem sujeitar-se a termos de uso abusivos que restrinjam de forma desproporcional seus direitos garantidos na Constituição"[28], ponderando que o uso da *internet* é manifestação palpável da função social desempenhada pela atividade empresarial, e que os ambientes virtuais não mais podem ser

---

[26] CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo.**A Lei Geral de Proteção de Dados do Brasil na era do Big Data.** *In* Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018, p. 358.

[27] RIBEIRO, Márcia Carla Pereira; GALESKI JUNIOR, Irineu. **Teoria geral dos contratos: contratos empresariais e análise econômica.** 2ª ed. São Paulo: Editora Revista dos Tribunais. 2015, p. 58.

[28] MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático**. Curitiba: Juruá. 2014, p. 158.

enxergados apenas como um espaço para o mero exercício de direitos disponíveis, mas como meio de concretização de diversos direitos sociais e individuais.

Muito embora o dever, em si, quanto à proteção de dados pessoais já existisse sob o pálio do Marco Civil da Internet, a LGPD, no entanto, aprofunda – e muito – as parcas diretrizes estabelecidas naquela norma, impondo às empresas novos desafios para se adequar ao novo estandarte legal.

Como visto, sobretudo para as empresas que hospedam seus serviços na *internet*, para estar em *compliance* com a LGPD, invariavelmente terão que dispor em seus Termos de Uso e Políticas de Privacidade informações claras e transparentes a seu público a respeito da forma como o tratamento de dados pessoais será realizado, sobretudo para dar fiel atendimento aos princípios previstos nos incisos do artigo 6º, em especial quanto à *finalidade* (I), *adequação* (II), *necessidade* (III) e *transparência* (VI).

A transparência talvez seja justamente a tônica da norma, uma vez que a partir do desenvolvimento deste princípio as partes envolvidas estarão em um patamar informacional equivalente. Neste sentido, DONEDA (2010, p. 84) esclarece que para salvaguarda das informações pessoais, estas deverão ser submetidas *"*através de uma política de privacidade clara e precisa e do recurso a outros meios que garantam que sua inscrição não se efetive sem o real conhecimento das suas consequências".[29]

Para traçar um paralelo, os Termos de Uso e Políticas de Privacidade, embora, como visto, ostentem a natureza instrumental própria dos contratos de adesão, são documentos que muito se assemelham a uma 'Carta de Intenções', por meio dos quais se estabelecem premissas acerca dos interesses, direitos, obrigações e demais regras consideradas necessárias para reger uma relação superficial entre as partes, que em muitos casos se limita ao acesso de determinado site, plataforma, aplicativo, etc., adequando tais interesses às balizas legais.

Estas intenções devem refletir fielmente aquilo que se pretende dar e, sobretudo, receber acesso, mormente considerando que tais documentos em regra são concebidos de forma unilateral pela parte que oferece os serviços ou detém a titularidade do ambiente em que a coleta e o tratamento de dados pessoais virá a ocorrer, valendo destacar que os Termos de Uso e Políticas de Privacidade, serão o principal instrumento de comunicação e de registro entre as partes dos moldes da relação entre elas estabelecida, vinculando-os a seus termos.

A título meramente exemplificativo, elencam-se, aqui, algumas disposições possíveis de serem estabelecidas nos Termos de Uso e Políticas de Privacidade como: direitos e deveres dos usuários e clientes; regras para utilização de serviços como *sites*, plataformas, aplicativos, etc., inclusive com relação à proteção de propriedade intelectual sobre conteúdos veiculados pelas partes; responsabilidade e limites de responsabilização, entre outras questões a serem pensadas casuisticamente, de acordo com os interesses envolvidos na consecução da atividade empresarial, que deverão nortear a elaboração dos referidos documentos.

Mais especificamente quanto à privacidade no tratamento de dados, é essencial, por exigência da LGPD, especificar quais serão os dados tratados – cujo tratamento deve se limitar aos dados mínimos necessários –; qual será a finalidade do tratamento, por qual prazo os dados serão tratados e o de que forma será realizada a eliminação dos dados quando do alcance da finalidade proposta, ou do exaurimento do prazo previsto (art. 15, I e II, LGDP); e qual serão os meios disponíveis para que o titular dos dados (art. 5º, V, LGPD) possa exercer o direito de livre acesso aos dados tratados (art. 9º).

[29] Op. cit., p. 84.

Além disso, tão importante quanto dar ao titular dos dados informações precisas a respeito dos pontos acima elencados – e aqui reside um dos grandes desafios para as empresas, sobretudo aquelas que exploram comercialmente os dados que tratam – é justificar o tratamento dos dados através da subsunção do caso concreto às hipóteses legais previstas no artigo 7º da Lei.

A política de privacidade deve dar ciência ao titular dos dados pessoais de que o tratamento de seus dados apenas será realizado em razão de alguma das hipóteses legais previstas nos incisos do artigo 7º, da LGPD.

Em linhas gerais, a LGPD apresenta dez hipóteses que autorizam o tratamento de dados pessoais, fugindo dos objetivos deste breve estudo tecer considerações mais aprofundadas a respeito de cada uma delas. Contudo, dado o tema a que ora nos debruçamos, mais apropriado do que esta abordagem é estabelecer a *necessidade*, em si, de liame entre os Termos de Uso e Políticas de Privacidade e algumas das hipóteses legais.

Sem embargo, abre-se exceção para tecer breves considerações a respeito da especial hipótese legal quanto ao consentimento (art. 7º, I, LGPD), instituto que, na concepção de CAVALCANTI e SANTOS "tem importante papel na autodeterminação informativa, controle e liberdade do titular em relação aos seus dados, configurando-se elemento central para a proteção de dados pessoais".[30]

O consentimento é, notoriamente, uma das principais e mais utilizada das hipóteses, embora seja considerada justamente a mais frágil delas, em razão da possibilidade de sua revogação pelo titular e da possibilidade de considerar-se nula a aquiescência do titular em caso de abuso ou se obtido mediante informações incompletas ou de teor enganoso (arts. 8º, § 5º e 9º, § 1º, LGPD).

A Lei traz em seu artigo 5º todo um rol de definições, conceituando, em seu inciso XII, o 'consentimento' como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", cuja descrição se demonstra relevante por carregar densa carga principiológica, sobretudo no aspecto da autodeterminação informativa, um dos fundamentos da LGPD (art. 2º, II).

É também exigência legal que a obtenção do consentimento para tratamento de dados pessoais seja realizada por escrito ou *"por outro meio que demonstre a manifestação de vontade do titular"* (art. 8º, § 1º), com cláusula em destaque, cabendo ao controlador o ônus da prova quanto à regularidade do consentimento obtido (art. 8º, § 2º). FRAZÃO (2018), sustenta que o consentimento é *qualificado*, ao afirmar que

> "(...) a manifestação de vontade precisa ser (i) livre e inequívoca, (ii) formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados, e (iii) restrita às finalidades específicas e determinadas que foram informadas ao titular dos dados."[31]

Cabe atentar ao fato de que o consentimento se torna ainda mais qualificado, quando se pretende o tratamento de dados pessoais sensíveis (art. 11, I) e de menores de idade, caso em

---

[30] Op. cit., p. 359.

[31] FRAZÃO, Ana. **Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais**; disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018; acesso em 31/10/2018.

que o consentimento deverá ser manifestado por um dos pais ou responsável legal pelo menor (art.14, § 1º).

Com base nestas considerações, conclui-se que esta nova cultura imposta – de maneira ainda mais ostensiva – pela LGPD visa à efetiva proteção, em sentido material, da privacidade dos titulares de dados pessoais e traz grande impacto sobre a atividade empresarial, demandando adequações operacionais no tratamento de dados, mas também providências jurídicas para que as 'regras do jogo' sejam claras e estejam compreendidas e aceitas pelos envolvidos, a fim de prevenir a ocorrência de danos e prejuízos aos usuários e à sociedade em geral, bem como às próprias empresas que realizarem o tratamento de dados pessoais.

Para efetivamente prevenir a ocorrência de danos e prejuízos, importante analisar as funções do controlador e do operador de dados.

4. A FIGURA DO DATA PROTECTION OFFICER (DPO)

Uma das obrigações impostas pela LGPD é a necessidade dos controladores de dados pessoais, sejam eles entes públicos ou privados, terem que indicar um encarregado (DPO - *Data Protection Officer*), pessoa natural ou jurídica, que deverá ser o profissional responsável pela proteção dos dados tratados e atuará como intermediador da comunicação entre o controlador e os titulares e a autoridade nacional[32].

A identidade do encarregado e a forma de comunicação deverão ser publicadas no site do controlador de maneira clara e objetiva, com a finalidade de facilitar requisições e comunicados dos titulares dos dados e da autoridade nacional.

Inicialmente as atividades do encarregado consistirão em receber reclamações e requisições dos titulares de dados, interagir com autoridade nacional de proteção de dados, orientar os funcionários e prestadores de serviços a respeito de boas práticas, bem como adotar as providências necessárias de proteção dos dados tratados.

Desta forma, é fundamental que o encarregado tenha conhecimento, e possa acompanhar e se envolver com todos os fluxos de processos realizados dentro da empresa controladora, bem como auxiliar diretamente no desenvolvimento de produtos e serviços, na elaboração de termos de consentimento, no processo de anonimização dos dados armazenados em bancos de dados, entre outros, de maneira que possa supervisionar todas as práticas de tratamento de dados, e certificar se estão em *compliance* com a Lei Geral de Proteção de Dados.[33]

Para isso, será de suma importância que o encarregado desempenhe suas funções com autonomia e imparcialidade dentro das organizações, podendo ele interferir nos processos internos, e sugerir mudanças e adequações, mesmo que isso afete economicamente a empresa, tendo em vista que sua motivação principal deve ser a de fazer com que a empresa cumpra as normas impostas pela legislação[34].

Além disso, a autoridade de proteção de dados, poderá através de normas complementares incluir novas atribuições ao encarregado, bem como definir sobre as hipóteses de dispensa da necessidade de sua indicação, conforme o tamanho e a natureza da empresa, bem como o volume de tratamento de dados.

Em linhas gerais, o encarregado pela proteção de dados dentro das empresas controladoras, deverá ser um profissional, com expertise em legislação de proteção de dados, tecnologia da informação em especial criptografia, e gestão de processos, que desempenhará um papel muito importante dentro das empresas a partir da vigência da Lei Geral de Proteção de Dados, e deverá estar capacitado para agir em prol do cumprimento da lei.

---

[32] BRASIL. **Lei n. 13.709, 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**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 2 de novembro 2018.

[33] MARCONDES, Juliana. **Quem é o Data ProtectionOfficer?**. Disponível em: <http://www.plmj.com/xms/files/2017_PDF/junho/Quem_e_o_Data_Protection_Officer.pdf>. Acesso em: 2 de novembro 2018.

[34] LEORATTI, Alexandre. **Nova lei de dados cria carreira no Direito com salários de até R$ 50 mil**. Disponível em: <https://www.jota.info/carreira/dados-dpo-carreira-direito-salarios-23102018>. Acesso em: 2 de Novembro de 2018.

5. CONCLUSÃO

Diante da universalidade de dados pessoais existentes no mundo virtual, e das novas consequências impactantes na sociedade, foi necessário a criação de legislações específicas sobre o tema. Nesse panorama, a Lei Geral de Proteção de Dados, Lei n.º 13.709/2018, foi promulgada no Brasil.

Com isso surgiram novos desafios, especialmente para quem manuseia dados pessoais, a exemplo das empresas privadas. Diante disso, surge a importância do presente estudo, que vem com o intuito de encontrar soluções práticas para a adequação à nova legislação por parte das pessoas jurídicas de direito privado.

Inicialmente, foi apresentada a ideia de *Compliance* como meio de garantir a correta aplicação da nova legislação. Para a instituição do Programa de Integridade, além da observância dos princípios que protegem direitos fundamentais, é necessário ter boa governança corporativa, fazer a correta gestão dos riscos, possuir uma boa estrutura tecnológica de segurança da informação e capacitar adequadamente as equipes de funcionários.

Em seguida, restou demonstrada a importância das funções dos Termos de Uso e Políticas de Privacidade, que possuem como finalidade informar sobre a utilização dos dados pessoais, de forma clara e transparente. Apesar de possuírem natureza instrumental de contratos, os Termos de Uso e Políticas de Privacidade se mostram como uma "Carta de Intenções", acerca da coleta e manipulação dos dados pessoais do usuário. Diante disso, foi verificada a importância do consentimento do titular dos dados pessoais para a sua proteção.

Por fim, foi analisada a figura obrigatória do *Data Protection Officer*, que recai sobre o encarregado. Este será sempre pessoa física, responsável pela proteção dos dados pessoais, atuando também como intermediador entre o controlador e os titulares e a autoridade nacional.

Muitos desafios vão surgir para as empresas privadas que manipulam dados pessoais com a futura vigência da Lei Geral de Proteção de Dados. Contudo, os primeiros passos de proteção já se mostram perceptíveis. E, tendo em vista a proximidade da vigência da nova lei, a atuação para a conformidade deve ser imediata.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015.

BRASIL. **Lei n. 13.709, 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**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 2 de novembro 2018.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo.**A Lei Geral de Proteção de Dados do Brasil na era do Big Data.** *In* Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018.

DONEDA, Danilo. **Proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília: SDE/DPDC. 2010.

FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J..**Big Social Data: Princípios sobre coleta, tratamento e análise de dados sociais.** Artigo publicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2014. Curitiba. 2014, p. 8. Disponível em http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf. Acesso em: 29/10/2018.

FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial**, 2018.Disponível em <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018> Acesso em: 31/10/2018.

FREITAS, Cinthia Obladen de Almendra; PAMPLONA, Danielle Anne. **A complexa relação entre negócios e direitos humanos: as violações dos direitos de personalidade por meio de Tracking e Profiling em serviços online.** 2018.

LEORATTI, Alexandre. **Nova lei de dados cria carreira no Direito com salários de até R$ 50 mil**. Disponível em: <https://www.jota.info/carreira/dados-dpo-carreira-direito-salarios-23102018>. Acesso em: 2 de Novembro de 2018.

MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático**. Curitiba: Juruá. 2014.

MARCONDES, Juliana. **Quem é o Data Protection Officer?**. Disponível em: <http://www.plmj.com/xms/files/2017_PDF/junho/Quem_e_o_Data_Protection_Officer.pdf>. Acesso em: 2/11/2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014.

RIBEIRO, Márcia Carla Pereira; GALESKI JUNIOR, Irineu. **Teoria geral dos contratos: contratos empresariais e análise econômica**. 2ª ed. São Paulo: Editora Revista dos Tribunais. 2015.

SILVA, Felipe. **Gestão de Identidades e Acessos.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015.

VENOSA, Sílvio de Salvo. **Direito civil: teoria geral das obrigações e teoria geral dos contratos.** 14ª ed. São Paulo: Atlas. 2014.

VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017.

A CRIAÇÃO DA AUTORIDADE NACIONAL DA PROTEÇÃO DE DADOS NO ÂMBITO DA LGPD: análise ontológica da experiência brasileira

Camila Giacomazzi Camargo

Advogada, Mestre em Propriedade Intelectual pela Universidade de Torino/Academia da Organização Mundial da Propriedade Intelectual.

Amanda Caroline Bissoni

Advogada, Especialista em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários -IBET.

1. RESUMO

O presente trabalho tem por objetivo tratar sobre a criação de uma Autoridade Nacional de Proteção de Dados, tendo em vista a edição da Lei nº 13.709 de 14 de agosto, vulgarmente denominada Lei Geral de Proteção de Dados (LGPD).

Desta forma, o trabalho abordará as experiências internacionais na criação das Autoridades de Proteção de Dados, adicionalmente quais poderiam ser os tipos de atuação da ANPD no Brasil.

Indo adiante, o trabalho discorrerá acerca dos possíveis modelos que o Brasil poderá utilizar para implementar a Autoridade Nacional de Proteção de Dados no país. Ainda, como o modelo que foi sugerido pela Lei Geral de Proteção de Dados, ainda que tenha sido vetado, se encaixaria, de acordo com a experiência brasileira.

2. BREVE HISTÓRICO DA EXPERIÊNCIA INTERNACIONAL

2.1. A AUTORIDADE DE PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA

A revisão na Europa da legislação sobre proteção de dados pessoais teve início quando se constatou que as regras já existentes não estavam em harmonia com as inovações tecnológicas. Deste modo, em 2011, por meio da emissão de um comunicado, recomendou-se que havia a necessidade de edição de uma nova norma, destinada a buscar a padronização na proteção de dados pessoais.

Assim, em virtude da urgência na elaboração de um novo normativo sobre à proteção de dados é que em 24 de maio de 2016, foi editada a *General Data Protection Regulation (GDPR),* estabelecendo que as empresas, o governo, bem como as sociedades civis teriam dois anos para implementar as medidas necessárias para o cumprimento de suas disposições.

Desta forma, para que a GDPR produzisse efeitos e que tornasse possível a verificação do cumprimento das obrigações, foram instituídas as *Data Protection Authorities (DPA),* que dizem respeito à Autoridades Públicas Independentes, que supervisionam, por meio de poderes investigativos e corretivos, a aplicação da Lei de Proteção de Dados. Essas Autoridades, na Europa, fornecem aconselhamento especializado sobre as questões de proteção de dados e lidam com reclamações apresentadas contra violações do Regulamento Geral de Proteção de Dados e das leis nacionais relevantes, vez que deve existir uma em cada Estado-Membro da União Europeia.

De modo geral, as empresas se submetem às Autoridades no Estado-Membro em que sua sociedade está sediada. No entanto, nos casos em que as entidades processem dados em diferentes Estados-Membros da União Europeia, ou faça parte de um grupo econômico que esteja estabelecido em diversos Estados-Membros, a sociedade poderá estar sujeita à Autoridades de Proteção de Dados em cada um destes Estados-Membros[35].

Indo adiante, é possível citar como exemplo de internalização da GDPR, o Reino Unido, onde uma nova Lei de Proteção de Dados foi promulgada, em maio de 2018, para complementar a GDPR, no que diz respeito às seções do Regulamento que foram deixadas para os Estado-Membros, individualmente, interpretassem, implementassem e aplicassem as suas disposições.

Deste modo, sob a GDPR, o Reino Unido criou a sua Autoridade de Fiscalização, denominada *The Information Comissioner's Office (ICO),* em que os titulares dos dados têm o direito de apresentar queixa à autoridade sempre que considerarem que o tratamento de seus dados pessoais infringe o Regulamento, ainda garantido o direito a que o indivíduo ingresse com medida judicial contra os responsáveis pelo tratamento de dados, haja vista que seus direitos foram infringidos em virtude de que seus dados não foram tratados de acordo com o que dispõe a GDPR.

Além disso, o ICO tem o poder de "impor uma limitação temporária ou definitiva, incluindo a proibição do processamento de dados"[36], ou seja, podendo encerrar completamente as atividades que vinham sendo exercidas pelas entidades que violaram a Lei de Proteção de Dados.

---

[35] **WHAT ARE DATA PROTECTION AUTHORITIES (DPAs)?** Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en >. Acesso em: 27 de novembro de 2018.

[36] Article 58 (2f) of the GDPR.

Outrossim, a Autoridade de Fiscalização poderá aplicar penalidades consideravelmente grandes, quando verificado o descumprimento das diretrizes da Lei de Proteção de Dados. Ou seja, o ICO poderá penalizar as sociedades com multas administrativas de até 20 milhões de euros ou 4% do faturamento global anual, o que for maior[37].

Finalmente, vale ressaltar que na Europa há a Autoridade de Proteção de Dados na União Europeia (European Data Protection Supervisor – EDPS), que é uma organização independente com as atribuições de monitorar e assegurar a proteção de dados pessoais e o correto tratamento da informação pelas diversas entidades sujeitas à GDPR, aconselhar, intervir e cooperar com as autoridades nacionais dos Estados-Membro em questões relacionadas ao tema, de forma a garantir o *compliance* das entidades e instituições junto a GDPR.

2.2 AUTORIDADE DE PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS DA AMÉRICA

De acordo com a estrutura política que os Estados Unidos estão constituídos é possível afirmar que eles não possuem uma Autoridade Nacional "oficial' de Proteção de Dados. No entanto, a *Federal Trade Commission (FTC)* tem jurisdição sobre a maioria das entidades comerciais e tem autoridade para emitir e aplicar regulamentos de privacidade em áreas específicas, por exemplo, telemarketing, e-mail comercial e privacidade infantil[38].

A FTC usa sua autoridade geral para evitar práticas comerciais desleais e enganosas, bem como para implementar medidas repressivas contra ações inadequadas de segurança de dados e as práticas inadequadas de coleta, uso e divulgação de informações. Entretanto, os procuradores gerais do estado normalmente têm autoridade semelhante e podem realizar fiscalização, especialmente nos casos de violação de segurança de dados de pessoais de suma importância.

Importante destacar nesse ponto as considerações trazidas pelo artigo "*Data protection in the United States: overview":*

> In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. However, each Congressional term brings proposals to standardize laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators[39].

Portanto, é possível dizer que nos Estados Unidos existem diversas entidades responsáveis pela proteção de dados pessoais. Entre elas, merece destaque as seguintes: *The Federal Trade*

---

[37] **THE GDPR AND THE DPA 2018.** Disponível em: < https://www.itgovernance.co.uk/data-protection >. Acesso em: 27 de novembro de 2018.

[38] **ABOUT FTC.** Disponível em: < https://www.ftc.gov/about-ftc >. Acesso em: 27 de novembro de 2018.

[39] LEUAN JOLLY, LOEB & LOEB. **DATA PROTECTION IN THE UNITED STATES: OVERVIEW.** Disponível em: < https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1 >. Acesso em: 27 de novembro de 2018.

Commission, The Financial Services Modernization Act, The Health Insurance Portability and Accountability Act, The HIPAA Omnibus Rule, The Fair Credit Reporting Act, The Controlling the Assault of Non-Solicited Pornography and Marketing Act, The Electronic Communications Privacy Act.

Há também muitas leis federais de segurança e de aplicação da lei que regulam o uso de informações pessoais. Além das entidades citadas acima, há também muitas diretrizes emitidas por grupos do setor que não são legalmente aplicáveis, mas geralmente são consideradas "práticas recomendadas" nesses setores. Por exemplo, o setor de publicidade continua tentando desenvolver o seu programa de autorregulamentação para publicidade comportamental on-line, que refletem em grande parte as diretrizes da FTC.

A maioria dos estados americanos promulgaram alguma forma de legislação de privacidade. No entanto, a Califórnia lidera o caminho na área de privacidade, tendo editado diversas leis de privacidade, algumas possuem, inclusive, efeitos no âmbito nacional.

A Califórnia foi o primeiro estado a promulga uma lei de notificação de violação de segurança (Código Civil da Califórnia § 1798.82). A lei exige que qualquer pessoa ou empresa que possua ou licencie dados informatizados que inclua informações pessoais para divulgar qualquer violação da segurança do sistema a todos os residentes da Califórnia cujas informações pessoais não criptografadas tenham sido adquiridas por uma pessoa não autorizada.

Em virtude de os Estados Unidos possuírem inúmeras diretrizes e legislações que tratam sobre a proteção de dados é que é possível dizer que eles não têm uma única Autoridade de Proteção de Dados.

3. POSSÍVEIS MODELOS NA PERSPECTIVA DA EXPERIÊNCIA BRASILEIRA

Tendo em vista que os artigos da LGPD que tratavam da forma de criação da ANPD foram vetados, muito se especula sobre qual será o modelo a ser adotado pela legislação brasileira para fiscalizar, orientar e punir as entidades infratoras.

O Projeto de Lei nº 58/2018 determinava a criação de autarquia especial vinculada ao Ministério da Justiça, devido à competência de referido Ministério na tutela dos direitos fundamentais, dotada de independência administrativa e hierárquica e autonomia financeira. Adicionalmente, foram atribuídos à tal autoridade os deveres de orientação e, originalmente, engajamento, assim como os poderes fiscalizador e punitivo.

Não obstante, suprimiu-se das atribuições da ANPD o dever de engajamento, tão relevante para a educação da sociedade nas questões atreladas ao tratamento e proteção de dados. Nesse sentido, sugere-se que – paralelamente à atuação da ANPD - as entidades dos diversos setores da economia afetados pela LGPD reúnam-se com o propósito de suprir referida lacuna e atuar para estimular a adoção de padrões e boas práticas na proteção de dados. Dessa forma, é relevante a atuação de conselhos, institutos, órgãos de classe e outras organizações setoriais.

3.1 MODELO DA DEFESA DA CONCORRÊNCIA – CADE

Dentre os modelos já existentes atualmente no Brasil, o modelo adotado em defesa da concorrência aproxima-se em suas características ao modelo sugerido para uma ANPD pela LGPD, especialmente pela sua atuação transversal – em defesa da concorrência - e não setorial – a favor de setor específico da economia.

De acordo com a Lei nº 12.5429/2011, o CADE é:

> Uma autarquia federal, vinculada ao Ministério da Justiça, que exerce em todo o Território Nacional as atribuições dadas pela lei
> O CADE tem como missão zelar pela livre concorrência no mercado, sendo a entidade responsável, no âmbito do Poder Executivo, não só por investigar e decidir, em última instância, sobre matéria concorrencial, como também fomentar e disseminar a cultura da livre concorrência.[40].

Seus órgãos principais são o Tribunal Administrativo, a Superintendência-Geral e o Departamento de Estudos Econômicos. O CADE, ao lado da SEAE, constitui o SBDC - Sistema Brasileiro de Defesa da Concorrência.

O Tribunal do CADE (TADE) tem o papel de julgar sobre matéria concorrencial os processos encaminhados por sua Superintendência-Geral. Desempenha os papéis preventivo, repressivo e educativo, dentro do mercado brasileiro. Já a SG desempenha principalmente o papel de instruir os processos no controle de condutas e de concentrações e de monitorar o mercado. O DEE, a seu turno, elabora estudos econômicos no intuito de auxiliar o TADE e a SG no desempenho de suas funções precípuas.

---

[40] **CADE.** Disponível em: < http://www.cade.gov.br/acesso-a-informacao/institucional >. Acesso em: 28 de novembro de 2018.

São instituições com funções semelhantes e equivalentes àquelas do CADE, em outros países, o *Federal Trade Commission* (FTC) nos Estados Unidos da América, a *Office of Fair Trade* (OFT) no Reino Unido, a *Autoritá Garante della Concorrenza e del Mercado*, na Itália, a *Australian Competition and Consumer Commission* (ACCC) na Austrália. A Direção-Geral de Concorrência da Comissão Europeia é responsável pela defesa da concorrência Comunitária.

Conforme mencionado o CADE desempenha principalmente três papeis, quais sejam em detalhe:

Preventivo: análise dos atos de concentração (fusão, incorporação, cisão e associação) entre agentes econômicos, ou seja, impor obrigações de fazer, não - fazer, determinar alienações e alteração nos contratos dos agentes;

Repressivo: análise de condutas da Concorrência (gestão anticoncorrenciais, ou seja, reprimir práticas que infrinjam à ordem econômica, tais como cartéis, vendas casadas, preços predatórios, acordos de exclusividade, dentre outras;

Educativo: papel pedagógico, com palestras, cursos, seminários.

Portanto, nesse modelo a ANPD teria tanto autoridade investigativa dentro da autarquia, com independência em relação à instância decisória. Assim, a ANPD exerceria tanto as atividades preventivas quanto as repressivas, que a LGPD atribui à ANPD.

3.2 MODELO DO SETOR PUBLICITÁRIO - CONAR

O Conselho Nacional de Autorregulamentação Publicitária (CONAR) é conselho organizado e mantido pelas entidades e profissionais do setor publicitário e é o maior exemplo brasileiro de modelo de autorregulamentação. Referido modelo caracteriza-se, especialmente, pela iniciativa do setor em estabelecer as diretrizes para o exercício de suas atividades.

O CONAR foi criado no final dos anos 70 em reação à inércia do Estado em regulamentar as atividades do setor de publicidade e propaganda. O CONAR é então uma organização da sociedade civil cujas atribuições incluem orientar, engajar e reprimir práticas contrárias as regras estabelecidas. Apesar de exercer, de certa forma, poder punitivo, não tem competência para aplicação de multas.

Sobre o CONAR, vale destacar as palavras de Luciano Coutinho sobre o CONAR:

> "Isso porque o exemplo da autorregulação eficaz e rigorosa é pedagógico: ele aponta para a consciência do mercado de que é preciso atuar sob determinadas bases, orientado por parâmetros mínimos aceitáveis. É uma boa lição para um momento de crise. Uma crise global que é financeira, mas é, no fundo, também ética, pois só alcançou tamanha gravidade pela falta de seriedade e pela ausência de uma regulação preventiva nas economias desenvolvidas".

O exemplo do setor publicitário não se apresenta, no contexto da LGPD, como uma alternativa ao modelo institucional, todavia pode servir de inspiração aos demais setores da economia como modelo a ser adotado para a regulação setorial no tocante a proteção de dados.

4. A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS NO CONTEXTO DA LGPD

4.1 A TRAJETÓRIA LEGISLATIVA DA CRIAÇÃO DE UMA ANPD: DO PROJETO DE LEI AO VETO PRESIDENCIAL E A MP 869/2019

Dentre os temas que surgem da discussão em voga em relação à proteção de dados, a necessidade de criação de uma autoridade nacional capaz de garantir os direitos previstos na LGPD mediante a regulação e fiscalização das obrigações previstas na lei é eminente.

O texto legislativo submetido à sanção presidencial criava, conforme artigos 55 ao 59, integrantes do Capítulo IX, a ANPD e o Conselho Nacional de Proteção de Dados e definia sua estrutura organizacional e financeira, a forma e limites da atuação de referida autoridade. Contudo, referido capítulo foi vetado pelo então Presidente da República, Michel Temer, sob a justificativa de que "Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao art. 61, §1º, II, "e", cumulado com o artigo 37, XIX da Constituição".[41]

Apesar da discussão quanto às razões do veto – sejam elas de cunho estritamente legal ou de cunho econômico, considerando a disponibilidade orçamentária do atual governo para tanto – não ser o cerne do presente artigo, tomamos a liberdade de tratar do tema diagonalmente com o tímido propósito de informar o leitor quanto ao debate acerca das razões do veto. A questão é se houve de fato um vício formal de iniciativa no processo legislativo para a criação da ANPD no formato proposto pelo Congresso Nacional, na medida em que diferente daquele originalmente proposto pelo Poder Executivo, ou se tal vício seria naturalmente sanado com a sanção presidencial.[42]

Dito de outra forma, nas palavras do ex-ministro do Supremo Tribunal Federal (STF), Ilmar Nascimento Galvão em conjunto com o professor da Universidade de Brasília (UnB), Jorge Octávio Lavocat Galvão[43]:

> "(...) o Congresso Nacional, no exercício da atividade legislativa, modificou a natureza jurídica do agente que realizará a fiscalização da proteção de dados no país, alterando-o de órgão público, previsto no projeto original, para autarquia em regime especial, vinculada ao Ministério da Justiça, dotada de independência administrativa, autonomia financeira, ausência de subordinação hierárquica,

---

[41] BRASIL. PROJETO DE LEI Nº 5.276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em <https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=62B6CCB8D15F03BD169F7421D3CDB6EE.proposicoesWeb1?codteor=1457971&filenamççlvce=Avulso+-PL+5276/2016>. Acesso em 25 de novembro de 2018.

[42] Os questionamentos, em suma, giram ao redor da competência do Poder Legislativo para deliberar sobre a criação de um órgão da Administração Pública indireta na figura de uma autarquia independente, considerando que a proposta originária do Executivo previa a criação de um órgão vinculado a Administração Pública direta. A discussão, enfim, agrava-se na medida em que há um entendimento de que o veto aos referidos artigos de criação de ANPD não seria necessário considerando que o vício formal de iniciativa poderia ter sido sanado com a correspondente sanção presidencial - do Poder Executivo, portanto.

[43] GALVÃO, Ilmar Nascimento; GALVÃO, Jorge Octávio Lavocat. **Parecer sobre a criação de órgão público e/ou de autarquia.** Brasília, 21 de julho de 2018. Disponível em: <https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018>. Acesso em 25 de novembro de 2018.

> mandato fixo e estabilidade de seus dirigentes, conforme §3º, do art. 55 do PLC nº 53/2018."

Nesse sentido, argumentaram os juristas supracitados em defesa às modificações realizadas pelo Congresso Nacional por compreenderem que não há qualquer vício de inconstitucionalidade nos artigos 55 e 56 do Projeto de Lei nº 53/2018 e concluíram que tais alterações ocorreram com o propósito de adequar o projeto de lei à necessária independência e autonomia da autoridade fiscalizadora. Senão, vejamos[44]:

> "1. A reserva de iniciativa do Presidente da República dos Projetos de Lei que alterem a estrutura da Administração Pública é justificada na medida em que cabe ao Chefe de Governo escolher quais políticas públicas pretende implementar e como pretende implementá-las, dentro de sua disponibilidade orçamentária e de seu plano de Governo;
> 2. O Poder Legislativo realiza o crivo democrático das opções do Poder Executivo, sendo-lhe autorizado efetuar emendas ao projeto de iniciativa privativa do Poder Executivo, desde que não implique aumento de despesa nem desvirtuamento da proposta original;
> 3. No caso, o Poder Executivo encaminhou o Projeto de Lei nº 5.276, de 2016, tendo como escopo estabelecer a política nacional de proteção de dados, prevendo um órgão público para fiscalizar a sua observância.
> 4. O Poder Legislativo, no gozo de sua legítima competência, modificou a natureza jurídica da figura administrativa que exercerá a atividade fiscalizatória, modificando de órgão público para autarquia em regime especial, por entender que a autonomia do ente e a independência de seus membros são características essenciais para a adequada prestação do serviço público em questão;
> 5. Tanto os órgãos públicos quanto as autarquias apresentam a mesma finalidade, que é a prestação de serviços públicos, sendo que o traço distintivo entre tais figuras administrativas é que as autarquias possuem personalidade jurídica própria, o que lhes confere maior autonomia;
> 6. A opção por criar uma política pública de proteção de dados, exercida por meio de um órgão fiscalizador, já foi deflagrada com o encaminhamento do Projeto de Lei nº 5.276, de 2016, por parte da Presidência da República. A mera modificação pelo Congresso Nacional da forma como o serviço será prestado (por meio de ente personalizado), sem que tenha havido aumento de despesas nem seu desvirtuamento, não tem o condão de macular o PLC nº 53/2018."

Independente das opiniões legais que recaem sobre a discussão travada acerca da criação da ANPD por intermédio da LPGD, como foi proposto, é fato incontroverso entre os estudiosos do tema de que a maneira como o texto foi aprovado e promulgado não deixa muito espaço para um debate sobre a necessidade de existência ou não de referida autoridade. Apesar do veto presidencial à sua criação, a ANPD é citada na LPGD cerca de quarenta vezes, de onde denota-se o caráter essencial da sua existência para eficácia das disposições legais lá previstas, como veremos a seguir.

4.2 A NECESSIDADE DE CRIAÇÃO DE UMA ANPD NO ÂMBITO DA LGPD

[44] Ibid.

A LGPD tutela não apenas os direitos básicos de acesso, retificação, cancelamento e oposição, mas inova ao possibilitar a portabilidade, explicação e revisão de decisões automatizadas, conforme depreende-se do art. 18, incisos I a IX da LPGD[45]. No parágrafo primeiro do mesmo artigo encontra-se a previsão de que "o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional".

Não obstante a abrangência da atuação que se espera atribuir a tal autoridade, nota-se que a tutela da privacidade (o cerne da legislação) depende diretamente da existência de tal autoridade, na medida em que assim está previsto na lei aprovada.

A criação e existência da ANPD é essencial para a afirmação dos princípios, direitos e obrigações previstos na LGPD, e nesse sentido, o Projeto de Lei nº 5.276/2016 trouxe em sua exposição de motivos:

> "Com o objetivo de dar efetividade à regulamentação sugerida, a proposta prevê um órgão competente para a proteção de dados pessoais no País. Será sua responsabilidade elaborar diretrizes de uma Política Nacional de Proteção de Dados Pessoais e Privacidade, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança, estimular a adoção de padrões para serviços e produtos que facilitem o exercício dos titulares sobre seus dados pessoais, entre outras medidas".

Resta claro, novamente, que a existência de uma instituição com expertise, independência e poder de fiscalizar e penalizar, é pressuposto do pleno exercício legal dos direitos atribuídos ao titular dos dados. Da mesma forma, é elemento indispensável para dar segurança jurídica às entidades que deverão estar *compliant* com os requisitos e obrigações da LGPD, ao passo que tem entre suas atribuições o dever de promover diretrizes e prestar orientação aos diversos setores da economia afetados.

4.2.1 A PARTICIPAÇÃO BRASILEIRA NA OCDE E A ADEQUAÇÃO INTERNACIONAL

---

[45] BRASIL. **LEI Nº 13.709 DE 14 DE AGOSTO DE 2018 (LEI GERAL DE PROTEÇÃO DE DADOS)**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 27 de novembro de 2018.
Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Não bastantes os argumentos de que a existência da ANPD é essencial à eficácia interna da LGPD para garantia da tutela à privacidade e segurança jurídica dos entes envolvidos, destacam-se aqui outros dois argumentos de suma importância para garantir que o Brasil esteja inserido no contexto internacional de proteção da privacidade. Sejam eles, como sugere este subtítulo, a participação brasileira na Organização para Cooperação e Desenvolvimento Econômico (OCDE) e adequação perante autoridades estrangeiras, especialmente a Autoridade Nacional de Proteção de Dados da União Europeia.

No âmbito da OECD a recomendação da existência de uma autoridade nacional supervisora vem de encontro com a confiabilidade e compromisso que se espera dos Estados-membro em relação à proteção de dados pessoais, como depreende-se das recomendações de medidas domésticas previstas no *OECD Privacy Framework*[46] que:

> "2. This Recommendation is intended to foster international co-operation among Privacy Enforcement Authorities to address the challenges of protecting the personal information of individuals wherever the information or individuals may be located. It reflects a commitment by Member countries to improve their enforcement systems and laws where needed to increase their effectiveness in protecting privacy. 3. The focus of this Recommendation is the authority and enforcement activity of Privacy Enforcement Authorities. However, it is recognized that other entities, such as criminal law enforcement authorities, privacy officers in public and private organizations and private sector oversight groups, also play an important role in the effective protection of privacy across borders, and appropriate co-operation with these entities is encouraged."

Em razão da natureza intangível dos dados pessoais, as leis nacionais de proteção de dados tendem a ter efeitos extraterritoriais, como é o caso da GDPR, no âmbito da União Europeia. A *compliance* com os requisitos da GDPR é uma das condições para o comércio com os Estados-membro da União Europeia, sendo que entre tais pressupostos está a existência de uma autoridade supervisora, a saber do artigo 45 da GDPR[47], sobre transferências com base numa decisão de adequação:

> 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.
>
> 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:
>
> a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência

---

[46] **OECD Privacy Framework.** França, 2013. Disponível em https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em 27 de novembro de 2018.

[47] GDPR, op. Cit.

> ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;
>
> b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e
>
> c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

Na medida em que todos os argumentos apontam para a necessidade do Brasil adotar o modelo institucional similar ao originalmente proposto, de autarquia especial com independência administrativa, ausência de subordinação hierárquica e autonomia financeira, também se demonstra relevante que o Poder Executivo observe as diretrizes estabelecidas pela OCDE quando da estruturação de uma ANPD, assim como aquelas indicadas na GDPR. As medidas de adequação inserem o Brasil em um contexto de cooperação internacional quanto a políticas concretas de proteção de dados para possibilitar e permitir a transferência internacional de dados e a continuidade do comércio internacional, de maneira geral.

4.2.2. A CRIAÇÃO DA ANPD PELA MEDIDA PROVISÓRIA Nº 869/2018

Finalmente (pouco antes da publicação do presente artigo), em 28 de dezembro de 2018 a Presidência da República editou a Medida Provisória (MP) nº 869/2018, que, enfim, estabeleceu a criação da ANPD, em vista da essencialidade da existência de uma ANPD, conforme acima exposto.

Apesar de o modelo seguido na referida MP não ser exatamente igual àquele adotado pela LGPD, a criação da ANPD serve certamente ao propósito inicial de adequação da legislação brasileira, em matéria de proteção de dados, aos mais evoluídos padrões internacionais e supre a falha gerada pelo referido veto presidencial de agosto de 2018.

Diverso do modelo institucional originalmente sugerido (autarquia especial vinculada ao Ministério da Justiça, com independência administrativa, autonomia financeira e ausência de subordinação hierárquica), a autoridade estabelecida pela referida MP, será um órgão da Administração Pública Federal, vinculado à Presidência da República. Garante-se a tal autoridade autonomia técnica, sendo-lhe designada a responsabilidade por zelar, implementar e fiscalizar o cumprimento da LGPD.

4.3 PILARES DAS FORMAS DE ATUAÇÃO DE UMA ANPD

Após tratar dos diversos tipos de autoridades de proteção de dados no direito comparado, é importante falar a respeito dos tipos de atuação da ANPD em âmbito nacional.

Desta forma, espera-se da autoridade nacional regulação que respeite o caráter transversal da LGPD e possibilite uma discussão multisetorial, na medida em que o tratamento de dados é tema afeto à diversos – em número e natureza – setores da economia.

4.3.1 PILAR REPRESSIVO

Conforme pode ser verificado nas autoridades instituídas pelo globo, é comum a aplicação de sanções administrativas àqueles que de alguma forma violarem ou não cumprirem as diretrizes traçadas pela legislação de proteção de dados. No Brasil, a LGPD dedica os artigos 52 ao 54 para elencar as penalidades aplicáveis para cada tipo de infração.

Nesse ponto, merece destaque a transcrição do texto legislativo:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> § 1o As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2o do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
> § 2oO disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.
> § 3o O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº

> 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).
> § 4o No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.
> § 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.
> § 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.
> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.
> Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.[48]

A intenção do legislador nesse caso é garantir que a ANPD tenha poder sancionatório e possa, a seu critério e por intermédio da instauração de um processo administrativo, punir condutas contrárias à lei. Nesse sentido, a LGPD assemelha-se muito com as disposições de caráter punitivo da *General Data Protection Regulation* promulgada pela União Europeia, estipulando, entre outras sanções, multa pecuniária de até R$ 50 milhões.

4.3.2 PILAR ORIENTATIVO

Apesar de a LGPD possuir multas na casa dos milhões de reais, é possível verificar que a legislação possui um caráter orientativo, que tem por objetivo oferecer orientações e diretivas para que os setores interessados possam atuar em consonância com a Lei Geral de Proteção de Dados.

Tal modelo de orientação resta evidenciado tanto no artigo 32, quanto no 51, da Lei Geral de Proteção de Dados:

> Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

[48] LGPD, op. Cit.

> Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais[49].

Portanto, a atuação de cunho orientativo deve incluir a promoção de boas práticas e instruções acerca do tratamento de dados pessoais. Assim, a ANPD poderá fornecer diretivas para que tanto o setor público, quanto o privado possam atuar de acordo com os objetivos da legislação de tratamento de dados, em especial sem concentrar a atenção em condutas específicas ou adotar ferramentas punitivas.

4.3.3 PILAR PREVENTIVO

O pilar preventivo da Lei Geral de Proteção de Dados é vislumbrado principalmente nos artigos 10, §3 e 35, da LGPD.

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
> Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.
> § 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
> § 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.
> § 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.
> § 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
> § 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei[50].

---

[49] **LEI GERAL DE PROTEÇÃO DE DADOS.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm > . Acesso em: 28 de novembro de 2018.
[50] LGPD, op. Cit.

Assim, em virtude da transferência internacional de dados é de suma importância que sejam criados regras e padrões para a avaliação de quando seria permitida a transferência desses dados.

Ou seja, a atuação da Autoridade Nacional de Proteção de Dados deverá ser *ex ante*, para evitar o dado, principalmente com o intuito de observar os direitos, garantias e os princípios da legislação. Portanto, a atuação da ANPD estaria focada em determinadas práticas comerciais, que teria como objetivo analisa-las de maneira a prevenir eventuais desvios da lei.

4.3.4 PILAR ENGAJADOR ("*Advocacy*")

Nesse ponto o Projeto de Lei nº 53/2018 previa que a ANPD deveria ter como objetivo explicar a relevância no tratamento de dados pessoais. Ou seja, a disseminação da cultura e da importância desse tratamento, tanto dentro da Administração, quanto nas sociedades, sejam elas de caráter civil ou as empresas, entidades do terceiro setor. No entanto, a LGPD não trouxe diretamente a questão.

De qualquer maneira, uma vez que a LGPD segue as diretrizes da GDPR, promulgada na União Europeia, é possível que a ANPD venha a desempenhar esse papel.

5. CONCLUSÃO

É importante destacar que a criação da ANPD está diretamente vinculada ao impacto econômico para o país, haja vista que uma vez criada tende a aumentar o "custo Brasil".

Entretanto, a ANPD deve existir e estar de acordo com as disposições trazidas pela GDPR, considerando que as autoridades estrangeiras, assim como a OCDE analisará se a autoridade nacional está organizada de modo a não sofrer influência externa do Poder Executivo e se lhe são fornecidos recursos humanos, técnicos, financeiros e infraestrutura adequada para que seu desempenho possa ocorrer de forma completa. A medida de tal adequação passará também, em alguns casos, pela verificação da independência financeira da, portanto, se de fato possui dotação orçamentária própria, bem como se seus membros estão ou não sujeitos à influência de terceiros, seja ela direta ou indiretamente, devendo eles serem livres para exercer suas funções sem qualquer tipo de pressão externa.

De 120 países que atualmente possuem uma legislação para proteção de dados pessoais apenas 12 não possuem uma autoridade regulatória. Na era informacional, o acesso das empresas nacionais aos mercados estrangeiros, assim como a própria relação entre Estados Soberanos, depende diretamente da existência de uma legislação de proteção de dados pertinente e adequada aos padrões de proteção internacionalmente adotados.

Assim, a experiência internacional nos ensina que – na medida em que os dispositivos legais centralizados numa lei geral e principiológica são dependentes entre si -, a criação de uma autoridade supervisora independente é instrumento para a eficácia da tutela da privacidade, no âmbito da proteção de dados pessoais. A LGPD foi cuidadosamente elaborada não apenas com o propósito de estabelecer princípios à tutela da privacidade e consolidar as regras que até então estavam dispersas em nosso ordenamento jurídico, mas também com o objetivo de assegurar que o Brasil estivesse em adequação com os mecanismos internacionais de proteção de dados. Ora, a necessidade da criação e manutenção de uma ANPD no modelo batizado internacionalmente torna-se, no cenário apresentado, incontroversa.

Finalmente, e considerando que apesar do veto presidencial à criação da ANPD por intermédio da LGPD, ainda se debate a criação da ANPD, vale utilizar-se de tal oportunidade para a realização de eventuais melhorias e aperfeiçoamentos no modelo sugerido, a fim de garantir que o as atividades da ANPD serão exercidas não apenas com autonomia, mas também com a técnica e expertise indispensáveis ao tema.

REFERÊNCIAS

WHAT ARE DATA PROTECTION AUTHORITIES (DPAs)? Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en >. Acesso em: 27 de novembro de 2018.

THE GDPR AND THE DPA 2018. Disponível em: < https://www.itgovernance.co.uk/data-protection >. Acesso em: 27 de novembro de 2018.

ABOUT FTC. Disponível em: < https://www.ftc.gov/about-ftc >. Acesso em: 27 de novembro de 2018.

LEUAN JOLLY, LOEB & LOEB. **DATA PROTECTION IN THE UNITED STATES: OVERVIEW.** Disponível em: < https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1 >. Acesso em: 27 de novembro de 2018.

CADE. Disponível em: < http://www.cade.gov.br/acesso-a-informacao/institucional >. Acesso em: 28 de novembro de 2018.

BRASIL. **PROJETO DE LEI Nº 5.276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural**. Disponível em <https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=62B6CCB8D15F03BD169F7421D3CDB6EE.proposicoesWeb1?codteor=1457971&filenamççlvce=Avulso+-PL+5276/2016>. Acesso em 25 de novembro de 2018.

GALVÃO, Ilmar Nascimento; GALVÃO, Jorge Octávio Lavocat. **Parecer sobre a criação de órgão público e/ou de autarquia.** Brasília, 21 de julho de 2018. Disponível em: <https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018>. Acesso em 25 de novembro de 2018.

BRASIL. **LEI Nº 13.709 DE 14 DE AGOSTO DE 2018 (LEI GERAL DE PROTEÇÃO DE DADOS). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 27 de novembro de 2018.

OECD Privacy Framework. França, 2013. Disponível em https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em 27 de novembro de 2018.

LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 28 de novembro de 2018.

FINTECHS E MEIOS DE PREVENÇÃO AO CRIME DE LAVAGEM DE DINHEIRO

ANA PAULA DE OLIVEIRA
Advogada, pós-graduanda em Direito Civil e Direito Processual Civil pela Unicuritiba, pós-graduanda em Direito do Trabalho e Direito Previdenciário pela UNISC; Membro da Comissão de Compliance da OAB/PR, Membro do Comitê Brasileiro de Compliance e Membro da Comissão de Processo Disciplinar da Federação Paranaense de Futebol.

AMANDA CRISTINA RIBEIRO
Advogada, pós-graduada em direito e processo tributário pela Universidade Positivo, Acadêmica de Ciências Contábeis pelo Instituto Federal do Paraná, Membro do Comitê Brasileiro de Compliance e Membro da câmara técnica de inovação do Instituto de Engenharia do Paraná.

GIOVANY MACIEL
Advogado, pós-graduando em Direito Civil e Empresarial pela PUCPR; Membro Fundador e Primeiro-Secretário do Comitê Brasileiro de Compliance; Membro da Comissão de Direito Empresarial da OAB/PR e Membro da Comissão de Compliance da OAB/PR.

LUCAS TEIDER
Advogado; aprovado no Mestrado em Direito Econômico e Desenvolvimento do Programa de Pós Graduação em Direito da PUCPR (2019); Pesquisador de Direito Constitucional (2014-2016) e de Compliance (2017-2018) da PUCPR. Sócio do IBCCRIM.

THEMIS ORTEGA SAMPAIO
Advogada, pós-graduada em Direito Contemporâneo pela FEMPAR, pós-graduada em Direito Civil e Direito Processual Civil pela Unicuritiba, Membro da Comissão de Inovação e

Gestão da OAB/PR e Membro do Comitê Brasileiro de Compliance.

RESUMO:

As *Fintechs* surgiram para solucionar, facilitar e diminuir custos de atividades financeiras. Contudo, exercem atividades sensíveis ao crime de lavagem de dinheiro. Por isso, é necessário estudar meios e instrumentos capazes de prevenir tais ilícitos no âmbito corporativo. Diante disso, esse estudo irá abordar os temas de *Compliance, Criminal Compliance,* Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT) e as Recomendações de Basiléia.

Palavras-chave: *Fintechs*, *Lavagem de Dinheiro, Compliance, Recomendações de Basiléia.*

Sumário: 1. Introdução; 2. *Compliance e Fintechs*; 3. *Criminal Compliance,* Combate à Lavagem de Dinheiro e *Fintechs*; 4. Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT) e *Fintechs*; 5.Recomendações de Basiléia*;* 6. Conclusão; 7. Referências Bibliográficas.

1. INTRODUÇÃO

As *Fintechs*, instituições financeiras inovadoras, exercem atividades sensíveis aos esquemas de lavagem de dinheiro, conforme art. 9º, I da Lei de Lavagem de Dinheiro (Lei 9.613/98), eis que possuem como atividade a captação, intermediação e aplicação de recursos financeiros de terceiros.

O crime de lavagem de dinheiro traz consequências graves para a sociedade, como a presença de capital ilícito no sistema financeiro e na economia nacional e a sonegação fiscal.

Diante disso, se faz necessário estudar meios a serem adotados pelas *Fintechs* no combate à Lavagem de Dinheiro.

Considerando-se os riscos do negócio e os preceitos basilares dos programas de integridade, como prevenção, processamento de informações sensíveis, e treinamento de colaboradores, pode-se enquadrar as necessidades de proteção das *Fintechs* como um tema de conformidade.

Importante mencionar que a Lei 9.613/98 iniciou um sistema de *compliance* no Brasil[51], tendo em vista que especificou obrigações para as instituições de identificar seus clientes e manter registros dos mesmos, bem como comunicar certas operações financeiras ao órgão competente. Tudo isso, com a finalidade de prevenir a lavagem de capitais.

No presente trabalho, realizado a partir de pesquisa doutrinária e legal, será abordado o tema *criminal compliance*, tendo em vista as implicações de ordem penal no ambiente corporativo, por ausência de boa governança. Busca-se mostrar que este seria um instrumento capaz de lidar com as complexidades do âmbito empresarial de uma instituição financeira e produzir efeitos de interesse coletivo, como a prevenção à lavagem de dinheiro.

Quando cuidando-se, especificamente, de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT), duas abordagens (complementares entre si e necessárias para a adequada compreensão e implantação do tema, em ambientes teóricos e operacionais) demonstram-se como possíveis: uma principiológica e calcada na própria e essencial racionalidade da temática de PLD-FT; e outra de cunho mais prático e operacional.

A racionalidade (*ratio*) de PLD-FT é aquilo que, *v. g.*, permite a compreensão, *ab initio*, da própria (alegada) necessidade de criminalização das condutas de lavagem de dinheiro e de financiamento do terrorismo, bem como desnuda as (macro)políticas (criminais e penais) e estratégias de combate e prevenção institucional à ocorrência destes delitos.

De outra mão, mas, repisa-se, em caráter complementar e não de oposição, o caráter operacional de PLD-FT, notadamente os programas, as políticas e os procedimentos de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, constitui-se como aqueles instrumentos por meio dos quais é possível que determinada instituição cumpra, de maneira adequada e efetiva, os objetivos impostos pela racionalidade de PLD-FT. De maneira muitíssimo breve e concisa, mas não simplista, o caráter operacional de PLD-FT é o que permitirá a empresa prevenir a lavagem de dinheiro e o financiamento do terrorismo, seja em estrito caráter de *prevenção*, ou ainda, de *monitoramento* ou de *resposta*.

PLD-FT é um assunto altamente dinâmico e que, como tudo aquilo que circunda as ciências jurídicas, devem manterem-se atualizados com o surgimento de novas tecnologias, necessidades e

---

[51] SAAD-DINIZ, Eduardo; SILVEIRA, Renato de Mello Jorge. ***Compliance*, Direito Penal e Lei Anticorrupção.** 1 ed. São Paulo: Saraiva, 2015. p. 180.

soluções. Deste modo, imperioso é um estudo, ainda que preliminar, sobre como PLD-FT pode (e deve) auxiliar o inovador ambiente das *Fintechs*.

Além disso, o estudo das *Fintechs* deve passar pelas regulamentações já existentes para que se projetem formas de adequação do tema as diretrizes já existentes ou a necessidade de reformulações.

A principal regulamentação que se deve atenção é o Acordo da Basiléia que surgiu com o intuito de estabilização da política monetária e financeira internacional, que deve ser adequada a nova realidade.

2. COMPLIANCE E FINTECHS

As *Fintechs* são compreendidas instituições financeiras novas no mercado, que ganharam destaque por unir tecnologia e serviços financeiros[52]. Assim, realizam todos os serviços dos bancos tradicionais, porém apresentam uma estrutura mais enxuta com tecnologia avançada.

Tratando-se de instituições financeiras autorizadas pelo Banco Central, as *Fintechs* devem atender a Resolução de nº 2.554[53], que dispõe sobre a implantação e implementação de sistemas de controles internos voltados para as atividades por ela desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a ela aplicáveis.

Assim, além da previsão legal apontando para a necessidade da conformidade, insta considerar também que o *compliance* tem objetivos tanto preventivos, quanto reativos[54], mostrando-se como importante ferramenta tanto no levantamento e avaliação de riscos, quanto na prevenção e redução de danos.

Neste ínterim, tratando-se da dinâmica de um programa de integridade, é possível defini-lo basicamente sob três etapas: num primeiro momento, correspondente a formulação, ou seja, análise e valoração de riscos, definição de medidas de prevenção e a criação de uma estrutura de *compliance*. No segundo, implementação, ou seja, comunicação e detalhamento do programa, consistente em medidas organizacionais para criação de processos de *compliance*. E no terceiro, por fim, correspondente a consolidação, buscando estabelecer um processo para apuração de violações, critério de sanções e avaliação continuada, e aperfeiçoamento do programa[55].

No que diz respeito à gestão dos riscos, consiste num processo estruturado[56], onde são levantados os ímpetos possíveis do negócio para, em seguida, dar sequência às demais etapas, buscando formas de reduzir ou eliminar seus efeitos.

Risco é definido por BARROS como sendo um "composto de dois grandes componentes: a probabilidade de ocorrência e a magnitude de perda", sendo que esta última consiste em "impacto"[57]. Nesse contexto, a probabilidade de ocorrência pode ser representada pela frequência do evento danoso – ou ameaça – em determinado período de tempo. Quanto ao impacto, se revela no "comprometimento de uma das propriedades básicas da segurança de informação: confidencialidade, integridade e disponibilidade".[58]

Assim, considerando, além da exigência legal, também os riscos das atividades das *Fintechs* e os princípios básicos que compõe os programas de integridade, pode-se entender a aplicação do

---

[52] NAJJARIAN, Irene Patrícia de Noronha. **Fintech: novo desafio regulatório. Revista de Direito Bancário e do Mercado de Capitais**. v.74. São Paulo, 2016. p. 33.
[53] <https://www.cbc.gov.br/pre/normativos/res1998/pdf/res_2554_v3_P.pdf>. Último acesso em 27/11/2018.
[54] VERÍSSIMO, Carla. **Compliance: incentivo à adoção de medidas anticorrupção**. São Paulo: Saraiva, 2017. p.91.
[55] Ibidem, p.277.
[56] BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p. 38.
[57]BARROS, Augusto Paes de. **Gestão de Risco.**In CABRAL, Carlos; CAPRINO, Willian (org.). Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados. Rio de Janeiro: Brasport, 2015. p. 39.
[58] Ibidem, p. 40.

compliance às novas instituições financeiras, não só como um meio importante na prevenção de ilícitos, mas necessário.

3. *CRIMINAL COMPLIANCE,* COMBATE À LAVAGEM DE DINHEIRO E *FINTECHS*

As *Fintechs* exercem atividades sensíveis aos esquemas de lavagem de dinheiro, conforme art. 9º, I da Lei de Lavagem de Dinheiro (Lei 9.613/98), eis que possuem como atividade a captação, intermediação e aplicação de recursos financeiros de terceiros.

A exposição de motivos da Lei de Lavagem de Dinheiro explica que "entre a prática da atividade ilícita e o usufruto dos recursos dela originados, há a necessidade de que seja realizada uma série de operações financeiras e comercias com o fito de dar a esses recursos uma aparência de valores obtidos licitamente"[59]. Ou seja, na Lavagem de Dinheiro é inevitável que os valores transitem por setores regulares da atividade econômica[60].

Ademais, a exposição de motivos mencionada alude dois pilares de sustentação do combate à Lavagem de Dinheiro a serem observados pelas instituições financeiras, sendo eles:

> a) "Fixação de procedimentos que dificultem o encobrimento da origem dos recursos e facilitem o trabalho da investigação;
> b) Criação de um órgão especializado para investigar a prática de operações de lavagem."[61]

Assim, percebe-se a necessidade de compartilhar a responsabilidade de combate à essas operações entre o Estado e os setores da atividade econômica sujeitos a essa prática. O fundamento teórico para esta divisão de tarefas surge da ideia de que a responsabilidade ao enfrentamento à lavagem de capitais se estende à sociedade[62].

Outrossim, percebe-se que determinados setores da economia servem como via para a consolidação desse crime, sendo que isto contamina as suas atividades lícitas, destruindo a imagem da instituição envolvida perante a comunidade[63]. Além do mais, na prática estas instituições possuem maiores recursos para combater a lavagem de dinheiro, eis que estão diretamente em contato com seus clientes, tendo maiores condições para averiguar a licitude ou ilicitude das operações[64].

Diante disso, tendo em vista o novo panorama que instituições econômico-financeiras intituladas *Fintechs* trouxeram, cumulado com o aumento do perigo da ocorrência do crime de lavagem de dinheiro, surge a necessidade de se falar em *criminal compliance*.

No combate à prevenção à lavagem de dinheiro, o *compliance* surge como um instrumento, capaz de evidenciar se uma Instituição está em observância com normas e regulamentos vigentes, de forma a assegurar a aplicação e efetividade dos mesmos[65].

---

[59] BRASIL. Exposição de Motivos da Lei n.º 9.613/98. Disponível em <http://fazenda.gov.br/orgaos/coaf/legislacao-e-normas/legislacao/exposicao-de-motivos-lei-9613.pdf/view>. Último acesso em 24/11/2018. Parágrafo 77.

[60] Ibidem, parágrafo 78.

[61] Ibidem, parágrafo 81.

[62] Ibidem, parágrafo 83.

[63] Ibidem, parágrafo 83.

[64] Ibidem, parágrafo 86.

[65] APARECIDA CARDOSO, Maria; CHAVES DE AMORIM, Evelyse; RODRIGUES VICENTE, Ernesto Fernando. **Os Impactos da Implementação de Controles Internos, Auditoria e Compliance no Combate e Prevenção à Lavagem de Dinheiro no brasil.** Enfoque: Reflexão Contábil, vol.31, num. 3, set.-dez., 2012, p. 26. Disponível em: <http://www.redalyc.org/articulo.oa?id=307125339003>. Último acesso em 23/11/2018.

Em relação ao Direito Penal, o *compliance* vem invertendo a noção de atuação em *ultima ratio*, e passa a ser mecanismo de prevenção de crimes praticados no seio corporativo, como a lavagem de dinheiro. Diante desse cenário, BUSATO afirma que "*compliance* é instrumento de controle social"[66]. Ou seja, além de funcionar no âmbito empresarial, também é uma forma de controle que produz efeitos de interesse coletivo[67], desde que equivalente com as suas aspirações sociais[68].

Outrossim, o *criminal compliance* apresenta o aspecto de autorregulação. Isto parte da privatização da função de prevenção de irregularidades, tendo em vista a responsabilidade penal das empresas e o desenvolvimento do Direito Penal econômico[69]. Ademais, o Estado não tem capacidade para exercer isoladamente a função preventiva, tendo em vista a sofisticação e a complexidade dos crimes que ocorrem no seio empresarial e com caráter transnacional[70], como é o caso da lavagem de dinheiro, especialmente no âmbito das *Fintechs*.

Como solução, a autorregulação possibilita que o Estado recorra às empresas para colaborarem no cumprimento de leis, estabelecendo regras e determinando a adoção de comportamentos adequados aos sujeitos do meio empresarial. Assim, instituições privadas e o poder público atuam conjuntamente no combate à atividade criminosa[71].

Além do mais, a redução da criminalidade, especialmente no que tange aos crimes de lavagem de dinheiro diretamente ligados a atividade financeira, depende de uma cooperação entre o Estado e a sociedade. Nessa seara, o *compliance* orienta-se pelo fim preventivo, por meio de ajustamento de uma série de condutas que incitam a redução dos riscos da atividade[72].

Aliando o *criminal compliace* à boa governança, a ideia de relação estruturada entre o setor público e o privado surge com a finalidade de que fique definido e padronizado o papel de cada um. Nesta seara, a organização forma uma rede, na qual a interação não pode ser submetida a instrumentos de mercado ou por uma atribuição hierárquica de comando[73]. Segundo SAAD-DINIZ e SILVEIRA, "a disposição das redes e as modalidades de gestão também operam para orientar as boas práticas de forma prescritiva, com a finalidade de melhoria dos critérios de direção/gestão empresarial"[74].

---

[66] BUSATO, Paulo César. **O que não se diz sobre *Compliance* em Direito Penal.** In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017. p. 54.

[67] Idem.

[68] SCANDELARI, Gustavo Britta. ***Compliance* como Prevenção Idônea de Crimes e sua Compatibilização com a Intervenção Mínima.** In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017.p. 108.

[69]BUSATO, Paulo César. **O que não se diz sobre *Compliance* em Direito Penal.** In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017. p. 55.

[70] FORIGO, Camila Rodrigues. **A Figura do *Compliance Officer* no Direito Brasileiro: funções e responsabilização penal.** 1 ed. Editora Multifoco: Rio de Janeiro, 2017. p. 202.

[71]Idem.

[72]SCANDELARI, Gustavo Britta. ***Compliance* como Prevenção Idônea de Crimes e sua Compatibilização com a Intervenção Mínima.** In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017. p.110.

[73]SAAD-DINIZ, Eduardo; SILVEIRA, Renato de Mello Jorge. ***Compliance*, Direito Penal e Lei Anticorrupção.** 1 ed. São Paulo: Saraiva, 2015. p. 258.

[74]Ibidem, p. 259.

Dessa forma, pode-se dizer que o *compliance* é um instrumento de controle penal, que leva em consideração a expectativa negocial[75], especialmente em relação a crimes econômicos, que demanda ingerência regulatória no âmbito corporativo ou institucional[76].

Nesse contexto, SAAD-DINIZ e SILVEIRA afirmam:

> "Assim é que as estruturas normativas peculiares ao *compliance* e à boa governança apontam para uma reorganização da intervenção jurídico-penal no sentido de estabelecer estruturas de atuação no âmbito regulatório, principalmente quando observada a criminalidade econômica. Esse, sem dúvida, um lado positivo do *compliance* ao ambiente penal."[77]

Então, a propagação de regras de *compliance* passaram a ser vistas como marcos regulatórios, em contextos situacionais próprios, focalizados em uma boa governança[78]. Um Bom Governo Corporativo está ligado à fidelidade e lealdade ao Direito, controles internos e externos, limitação e equilíbrio de poder, oportunidades de negócios etc.[79]. Assim, pode-se afirmar que para se garantir o *compliance*, é indispensável que haja uma boa condução da empresa[80].

Por fim, vale ressaltar que o programa de *compliance* deve ser efetivo para mitigar a ocorrência da lavagem de dinheiro. Caso contrário, sendo meramente formal ou absolutamente ineficaz, feito apenas com a finalidade de aparentar preocupações com crimes, deve ser desconsiderado como tal. Isso porque, parece que nesse caso, o *compliance* de "fachada" serviria apenas para proteger a intenção delituosa e possibilitar a prática de ilícitos de forma "blindada"[81].

Observando o crimes que ocorrem no ambiente corporativo, inclusive à lavagem de dinheiro nas *Fintechs*, é importante refletir acerca da capacidade organizacional das empresas para conduzir situações de crise, considerando, além do fluxo de capital, "o alcance das medidas sancionatórias para impor limites ao capital regulatório ou tipificar um parâmetro mínimo de capitalização e controle dos fluxos de pagamentos, responsável pelo excesso de liquidez"[82].

Nesse contexto, ressalta-se a necessidade de delinear uma abordagem econômica do conceito de crime, que se percebe numa aproximação da regulação privada como reforço à Lei Penal[83].

Ainda, para se manter em *compliance,* é importante que as instituições intituladas *Fintechs* se atenham aos conceitos de PLD/FT – PROGRAMA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO e às Recomendações de Basiléia.

---

[75]Ibidem, p. 260.

[76]SAAD-DINIZ, Eduardo; SILVEIRA, Renato de Mello Jorge. ***Compliance*, Direito Penal e Lei Anticorrupção.** 1 ed. São Paulo: Saraiva, 2015. p. 260.

[77]Ibidem, p. 262.

[78] Ibidem, p. 249

[79]Ibidem, p. 252.

[80]Ibidem, p. 256.

[81] SCANDELARI, Gustavo Britta. ***Compliance* como Prevenção Idônea de Crimes e sua Compatibilização com a Intervenção Mínima.** In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017. p.99

[82]SAAD-DINIZ, Eduardo; SILVEIRA, Renato de Mello Jorge. ***Compliance*, Direito Penal e Lei Anticorrupção.** 1 ed. São Paulo: Saraiva, 2015. p. 307.

[83]Ibidem, p. 308.

4. PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO (PLD-FT) E FINTECHS

Lavagem de dinheiro, de maneira central ou ainda que lateral, é o tema do momento no *locus* brasileiro. Combate à corrupção é, ao menos supostamente, a agenda e a pauta principal (ou, no mínimo, uma das) das instituições e seus agentes. O (conjecturado) corrupto tornou-se o *inimigo* público número um, contra o qual se monta uma estrutura punitiva em utilização da verdadeira matriz política do Estado[84].

Consequentemente, a Prevenção à Lavagem de Dinheiro tornou-se assunto e matéria de destaque. E, embalado por iniciativas, sobretudo de organizações e organismo internacionais, as temáticas sobre o combate e a prevenção ao terrorismo e o seu financiamento também se impuseram como relevantes.

Salienta-se, de início, que, em que pese *lavagem de dinheiro* ser, como acima indicado, o tema do momento, "a lavagem de dinheiro seria uma prática tão antiga que poderia ser inclusive ser classificada como 'o terceiro crime mais antigo do mundo'"[85] (após o roubo e o homicídio). Contudo, com o fenômeno da globalização a *lavagem de dinheiro*, suas formas e, sobretudo, o seu impacto, iniciaram a ser relevantemente notadas. A primeira estrutura moderna de criminalização da *lavagem de dinheiro*, como conhecemos atualmente, deu-se na Itália, em 1978, no período conhecido como "Anos de Chumbo", por meio da Lei 59, de 21 de março de 1978, que logo foi adicionada ao Código Penal Italiano. O principal objetivo desta lei era o de assegurar penas mais rigorosas aos envolvidos nestes crimes. O termo *lavagem de dinheiro* ("*moneylaundering*") foi utilizado pela primeira vez em um Tribunal da Flórida, no ano de 1982, em um caso de alegada ocultação de bens provenientes de organizações criminosas envolvidas com o tráfico de drogas local. Junto ao cenário brasileiro, o país, em 26 de junho de 1991 (por meio do Decreto nº. 154), aderiu à Convenção de Viena, realizada em dezembro de 1988, promulgando a sua Lei específica sobre *lavagem de dinheiro* em 03 de março de 1998 (Lei nº. 9.613).

De início: porque é importante estudar-se e debater-se a Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT)? A resposta, independentemente do fato de a pergunta ser direcionada para um *garantista*ou um *punitivista*, será: em razão dos impactos destes crimes (de lavagem de dinheiro e do terrorismo e o seu financiamento) e dos delitos necessariamente (ou eventualmente) correlacionados.

De acordo com o Fundo Monetário Internacional (FMI), cerca de US$ 3 trilhões são "lavados" anualmente no mundo inteiro. Este montante equivale a 5% do PIB global. A Organização das Nações Unidas (ONU) estima que é de US$ 1,6 trilhão (o equivalente a 2,7% do PIB global) o faturamento anual do tráfico internacional de drogas. A Organização Internacional do Trabalho (OIT), por sua vez, concluiu que o trabalho forçado gera lucros anuais de cerca de US$ 150 bilhões. Ainda, segundo a companhia Havocsope, apenas na Tailândia, o "turismo sexual" (conceito que abrange desde a prostituição até o tráfico e a exploração humana) rende US$ 6,4 bilhões por ano.

No Brasil, o Sindicato Nacional dos Procuradores da Fazenda (SINPROFAZ) registrou que R$ 339 bilhões foram sonegados em 2016, sendo que, deste total, R$ 271 bilhões (80%) teriam sido

---

[84]TEIDER, Lucas H. **A presunção de culpabilidade nos delitos econômicos como Direito Processual Penal do inimigo e os reflexos no instituto da prisão preventiva**. *In*: Revista Iberoamericana de Derecho Penal y Criminología: Instituto Peruano Argentino de Derecho Penal - Universidad Nacional de Lomas de Zamora (Instituto enCienciasPenales - Facultad de Derecho) (Argentina), Número 1, Novembro de 2018.

[85]DE CARLI, Carla Veríssimo. **Lavagem de Dinheiro: Ideologia da Criminalização e Análise do Discurso**. 2ª ed. Verbo Jurídico, 2012.

sonegados por meio de mecanismos de lavagem de dinheiro. De acordo com a *Global Financial Integrity* (*GFI*), cerca de R$ 67,3 bilhões em dinheiro "sujo" (proveniente de atividades ilícitas), ligados aos crimes de corrupção e sonegação tributária, sairiam todos os anos do Brasil.

Em se tratando do financiamento do terrorismo, de acordo com o *World Atlas ofIllictFlows*, um estudo realizado em parceria pela INTERPOL, a RHIPTO e a *The Global IniciativeAgainst Transnacional Organized Crime*, o orçamento do terrorismo, apenas por financiamentos e doações, ultrapassou US$ 36 milhões (cerca de 3% do orçamento integral do terrorismo)[86].

Sequencialmente, uma segunda pergunta pode ser apresentada: qual é a importância de as instituições (públicas ou privadas e de qualquer setor do mercado) atentarem-se para PLD-FT? Em primeiro lugar, qualquer corporação deve estar atenta para os riscos de sua atividade e, sobretudo no mercado financeiro, mas não unicamente, o risco de lavagem de dinheiro e de financiamento do terrorismo, não apenas na empresa, mas por meio da empresa, cuida-se de algo muitíssimo real. Desde 2014, o Banco Central do Brasil já liquidou ao menos 8 instituições em virtude de graves irregularidades de PLD-FT, instaurou 23 processos administrativos punitivos e aplicou R$ 695 milhões em multas. E, sem dúvida alguma, o risco reputacional apresenta-se como o mais severo (vide Samarco, Zara, BTG Pactual, Odebrecth, Friboi, Opportunity e Enron), em diversas oportunidades, diferentemente de um revés financeiro, pode ser irrecuperável. Além dos riscos, sanções também podem se fazer presentes, como aquelas administrativas (de multa até de R$ 20 milhões por evento, inabilitação dos administradores por até 10 anos ou cassação da autorização para operação ou funcionamento, por exemplo) e legais (de até mais de 16 anos de prisão).

Junto ao cenário emergente das *Fintechs*, para estas surgem necessidades, mas também oportunidades. Como precursoras (ao menos de um discurso) de acessibilidade, inclusão, transparência e modelo de negócio mais ético e oxigenado (congruente, propositalmente ou consequencialmente, com as demandas atuais), apresenta-se uma oportunidade de diferenciação por excelentes fatores, como a elevação do patamar ético das relações negociais. Contudo, como operantes no mercado financeiro, diversas obrigações lhes são impostas. Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT) constitui-se, ao mesmo tempo, como necessidade (da qual das *Fintechs* não podem se dissociar) e oportunidade.

E, ultimamente, como se previne a lavagem de dinheiro e o financiamento do terrorismo? A resposta para esta pergunta não é de forma alguma simples, bem como não é, também de nenhuma maneira, impossível. PLD-FT é formada, essencialmente, por 4 pilares: cadastro atualizado de clientes; programa "Conheça Seu Cliente" (*KnowYourCostumer- KYC*); ações de monitoramento de operações; e comunicações de operações ao COAF.

As principais exigências de cadastro de clientes (considerado o "coração" de PLD-FT) estão dispostas à Resolução 2.025/93 e Circulares 3.461/09, 3.583/12 e 3.654/13, todas do Banco Central do Brasil, de onde se podem extrair importantes e indispensáveis obrigações, como a exigência de coleta e manutenção (inclusive de cópias) de dados pessoais (qualificação e localização) e informações sobre a atividade, renda, faturamento e patrimônio; a identificação dos beneficiários finais dos clientes pessoa jurídica PJ) (abertura da cadeia societária ou acionária); a identificação obrigatória das Pessoas Expostas Politicamente (PEPs); a implantação e execução de procedimentos de confirmação e atualização das informações cadastrais; a definição de critérios de classificação de clientes como permanentes ou eventuais (sobretudo com o uso da metodologia de Abordagem Baseada em Risco [ABR]); a aplicação de testes de verificação cadastral, independentemente das ações de auditoria interna; entre diversos outros fatores.

---

[86]INTERPOL, PHIPTO e THE GLOBAL INICIATIVE AGAINST TRANSNACIONAL ORGANIZED CRIME. **World Atlas ofIllictFlows**, 2018. Disponível em: <http://globalinitiative.net/world-atlas-of-illicit-flows/>. Acesso em 24 out. 2018.

O Programa “Conheça Seu Cliente” é uma ação continuada que objetiva a coleta, o registro e a manutenção das informações sempre seguras e atualizadas sobre os negócios do cliente, as quais devem ser utilizadas para verificar a compatibilidade das suas operações em relação à atividade e capacidade financeira declarada e demonstrada. Visa, também, a realização de uma análise reputacional do cliente, possibilitando a descontinuidade (ou o desinteresse já no processo de *onboarding*) da relação de negócios com aqueles que possam representar riscos à instituição. As melhores práticas de mercado, como ações de *duediligence*, constituem-se como: visitas periódicas ao cliente com o preenchimento de um “Relatório de Visita”; pesquisa de mídias negativas e em listas públicas nacionais (de trabalho escravo, infrações socioambientais, empresas inidôneas, e outras) e de terroristas e traficantes internacionais (OFAC, ONU, UE, e outras); bem como pesquisas em listas de PEPs e acerca de processos (administrativos e judiciais) e restrições financeiras.

As ações de monitoramento, detecção e análise de operações, por sua vez, compreendem todo um fluxograma (*workflow*) especificamente moldado e adequado à instituição, contendo, por exemplo, ferramentas informatizadas para o acionamento de suspeitas de lavagem de dinheiro ou de financiamento do terrorismo; comunicações internas prévias e com o cliente, apoiadas no Programa “Conheça Seu Cliente”; elaboração de dossiê analítico e deliberação por parte do Comitê de PLD-FT da instituição acerca da comunicação ao COAF.

Consequentemente, as comunicações ao Conselho de Controle de Atividades Financeiras (COAF), Unidade de Inteligência Financeira (UIF) do Brasil, serão o que permitirão que as atitudes da instituição ultrapassem a *prevenção* e permitam, por parte das instituições persecutórias de Estado, o *combate* à lavagem de dinheiro e ao financiamento do terrorismo. Em simples termos, são 3 as comunicações ao COAF: Comunicação de Operação em Espécie (COE), onde devem ser comunicados todos os depósitos e retiradas em espécie e pedidos de provisionamento para saque em espécie de valor igual ou superior a R$ 50 mil (em até 1 dia útil após o depósito ou a retirada, ou em até 3 dias úteis de antecedência, para provisionamentos, pela área responsável por PLD-FT na instituição, por meio do SISCOAF); Comunicação de Operações Suspeitas (COS), em havendo indícios de ilícitos (como, por exemplo, fragmentação de valores; uso de “laranjas”; empresas fictícias ou de “fachada”; uso de empresas para mesclas de valores, comercialização ou aquisição de bens de alto valor, constituição de procuradores, entre outras situações), em até 24 horas após a decisão do colegiado executivo; e Comunicação de Não Ocorrência, nas hipóteses em que a instituição não apresentou, durante toda a extensão do ano, quaisquer operações suspeitas. As comunicações devem ser analíticas, detalhadas e substanciais, calcadas nos procedimentos de conhecimento do cliente da própria instituição (que, igualmente, devem ser robustos e efetivos), para permitir o deslinde (absolutório ou condenatório) das suspeitas.

Ainda, as melhores práticas de mercado de PLD-FT (muito apoiadas na Autorregulação FEBRABAN SARB nº. 011/2013) também salientam a importância de Programas outros, como “Conheça Seu Funcionário”, “Parceiro” e “Fornecedor”; a avaliação de novos produtos e serviços também sobre a ótica de PLD-FT; e o treinamento dos membros da instituição e demais envolvidos operacionalmente.

Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT), como se pode perceber, é realizada na prática, em que pese os importantíssimos debates e teorizações que proporcionam corpo ao tema e permitem o aperfeiçoamento técnico e operacional dos procedimentos. E o comprometimento de todos que integram a instituição é essencial: apenas com a integralidade é possível alcançar a integridade.

5. RECOMENDAÇÕES DE BASILÉIA

5.1 ORIGENS E CONTEXTO

Em meados dos anos 70, diversos acontecimentos mudaram a forma de se pensar a política monetária internacional. Neste contexto, o abandono de um sistema baseado em taxas de câmbio fixas que causava grande instabilidade, em conjunto com demais fatores econômicos, resultaram em uma menor regulamentação estatal.

Como consequência de menores intervenções governamentais, houve a facilitação de realização de empréstimos internacionais entre as instituições financeiras. Tal fato gerou insegurança por parte das instituições que passaram a conviver com o temor de prejuízos decorrentes a quebra dos bancos internacionais, já que não havia qualquer controle internacional. Ainda, outro ponto de vulnerabilidade era a possibilidade de instituições se deslocarem para outros países, buscando regulamentações menos rigorosas.

Conforme dispõe Carvalho "iniciou-se um período de revisão profunda dos princípios que regiam até então a ação reguladora do estado nos mercados financeiros. Desregulação e liberalização da atividade financeira passaram a ser objetivos perseguidos com afinco em todos os países, ainda que com graus variados de entusiasmo"[87]

Com base nas mencionadas motivações, visando maior estabilidade monetária e financeira, o BIS (Bank for InternationalSettlements) ou Banco de Compensações Internacionais, instituição que estimula a colaboração entre os bancos centrais de cada país com demais agências interessadas, passou a patrocinar o comitê de supervisão bancária da Basiléia, que fora criado para este fim.

O comitê passou a desempenhar ações visando reunir as mais diversas regulamentações de diferentes países, para realizar fiscalizações em tais localidades pautas na legislação específica, partindo de princípios gerais estabelecidos.

5.2 DISPOSIÇÕES ESPECÍFICAS

Com o desenvolvimento dos trabalhos voltados para a estabilidade monetária e financeira, o comitê editou o Acordo da Basiléia, assinado em 1988. O acordo que foi denominado como "Basiléia I", delimitou diretivas que almejavam o fortalecimento da estabilidade sistema monetário, recomendando a adoção de um capital mínimo para a diminuição de falência dos bancos.[88]

Inicialmente, imaginava-se que as recomendações trazidas pelo comitê fossem adotadas unicamente por países desenvolvidos e para bancos com abrangência internacional. Porém, com a medida do Fundo Monetário Internacional (FMI) de condicionar a adesão ao acordo da Basiléia na avaliação de solidez dos bancos nos países membros, as regulamentações passaram a ser ponto de partida para muitos países com tamanhos e economias distintas.

O ponto primordial do Basiléia I foi a recomendação de um capital regulatório que atingia as operações de crédito. Além disso, o acordo editou regras relacionadas ao patrimônio das instituições, calculados com base no risco de cada uma delas.

---

[87]CARVALHO. F.C. et al. Economia Monetária e Financeira. Teoria e Política, Rio de Janeiro: Editora Campus, 2000, p. 341.

[88]https://www.bcb.gov.br/fis/supervisao/basileia.asp. Ultimo acesso em 27/11/2018

Outro ponto a se considerar foi que o Basiléia I estabeleceu o padrão de solvência das instituições financeiras, passando a considerar que o capital para cobrir os riscos deveria ser superior a 8% da avaliação de risco.

No ano de 2004, o Comitê de Supervisão Bancária de Basileia editou o segundo acordo, conhecido como "Basiléia II", que buscou abarcar pontos faltantes na primeira minuta, bem como suprir as questões trazidas com as inovações que surgiram no espaço de tempo desde o primeiro acordo.

Um documento editado pela Convergência Internacional de Mensuração de Capital e Padrões de Capital 18 de Junho 2004, o Acordo de 1988 foi revisado para desenvolver uma: "estrutura que fortaleça ainda mais a solidez e a estabilidade do sistema bancário internacional e, ao mesmo tempo, mantenha consistência suficiente para que o regulamento de adequação do capital não seja uma fonte significativa de desigualdade competitiva entre os bancos internacionalmente ativos."

Ainda, conforme crítica apontada por Ana Rosa Mendonça:

> "as ponderações de risco exigidas pelo Acordo de 1988 não estimulam ou mesmo reconhecem o uso e o amplo desenvolvimento de métodos internos de avaliação de riscos e uma vez que são fixas por classe de ativos acabam por incentivas a realização de operações de arbitragem de capital; e, por fim, o Acordo de 1988 não admite a utilização das várias técnicas utilizadas para a mitigação do risco de crédito, tais como as garantias para o cálculo do capital.[89]

O Basiléia II abordou amplamente a questão do risco operacional, buscando encontrar mecanismos de gestão para a promoção da estabilidade internacional. Na minuta buscou-se abranger a administração dos riscos operacionais, de crédito e de mercado.

Nesse sentido, o acordo de 2004 abordou a questão de um capital mínimo, buscando bons níveis de capitalização para cobrir os riscos assumidos, as diretrizes também abarcaram a supervisão das instituições, elaborando procedimentos internos para avaliar os riscos e buscar capital necessário de acordo com cada perfil. Outro ponto importante foi o estabelecimento de formas de fomento da transparência e de condutas pautadas na ética para a atuações no mercado.

Em 2010 houve a publicação do acordo "Basiléia III", sendo um adendo ao Basiléia II, motivado pela crise econômica internacional iniciada em 2007. Tal acordo deixou claro que o Basiléia I e II não foram suficientes para frear a instabilidade financeira.

Por ter surgido em um ambiente de crise, o terceiro acordo editado teve por finalidade principal o fortalecimento do sistema monetário e eficácia das instituições em reagirem a ambientes e acontecimentos negativos advindos do próprio sistema financeiro.

O Basiléia III teve como principais alterações a descrição de um patrimônio de referência mais robusto, deixando de fora instrumentos incapazes de auxiliar na recuperação em momentos de perda. A divisão do capital também foi reformulada em relação ao acordo anterior, havendo novas definições quanto ao capital principal e o complementar.

Neste sentido o artigo "Basiléia III: Impactos para os Bancos no Brasil" brilhantemente explicitou o tema:

---

[89]MENDONÇA, Ana Rosa Ribeiro de. O Acordo da Basiléia de 2004: uma revisão em direção ás praticas de mercado. Revista Economia Politica Internacional: Análise Estratégica. Rio de Janeiro, UFRJ, nº 2, julho a setembro de 2004

> Basileia III introduziu importantes modificações, particularmente no tocante às definições de capital. Entre as mudanças, destacam-se uma nova estrutura de capital, priorizando o capital de melhor qualidade e estabelecendo restrições aos instrumentos de capital de menor qualidade; ajustes prudenciais ao capital da instituição; o conceito de capital conservation buffer, que é o capital adicional para fazer frente a possíveis perdas; e o conceito de countercyclical buffer, ou capital contracíclico. Diferente dos acordos anteriores, que resumiam a estrutura de capital da instituição a Tier 1 e Tier 2, o novo Acordo de Capital é consideravelmente mais rigoroso e passa a consistir na soma dos seguintes elementos: a) Tier 1, ou Capital Nível 1, cujo requerimento é de 6% de APR, composto por: i. Common Equity, ou Capital Principal, na denominação da Resolução do Conselho Monetário Nacional (CMN) n. 4.192/2013, que deverá ser maior ou igual a 4,5% de APR; e ii. AdditionalTier 1, ou Capital Complementar, segundo a mesma resolução. b) Tier 2, ou Capital Nível 2. A soma de Tier 2 e Tier 1 deve ser, no mínimo, 8% de APR. Além de Tier1 e Tier 2, o Acordo de Basileia III prevê que o capital regulatório da instituição deve incluir: c) Capital conservation buffer, ou capital de conservação, consiste em um "colchão" extra de capital para possíveis perdas, proporcionando à instituição que "adentrar" esse limite a continuidade de suas operações. Nessas condições, a instituição é obrigada a interromper o pagamento de dividendos, até a recomposição do capital. O capital de conservação requer 2,5% de APR adicionais de Capital Principal. d) Countercyclical buffer, ou capital contracíclico. Visa a garantir a estabilidade financeira da economia e seu uso confere graus de liberdade aos bancos centrais: fora dos tempos de crise, cria-se um colchão de capital para fazer frente às perdas em possíveis crises; e nos tempos de crise, a autoridade monetária pode abolí-lo para evitar uma recessão. O capital contracíclico requer 2,5% de APR adicionais de Capital Principal.[90]

Ainda, o acordo incluiu nas diretrizes ajustes conhecidos como prudenciais que consistiam em retirar os componentes que comprometiam a capacidade das instituições em lidar com as perdas de capital principal, dentre outros motivos pela força da liquidez reduzida.

Além de se preocupar com a qualidade do capital, o acordo estabeleceu critérios também quanto a quantidade, igualmente com a intenção de se reagir a perdas. Assim, o Basiléia III estipulou mais de dois critérios mínimos de capital, quais sejam o índice de capital principal e o índice de capital nível I.

Ainda na questão do capital, buscando um movimento "contra cíclico" em relação ao Basiléia II, o acordo inovou ao criar adicionais ao capital principal.

[90] PINHEIRO, Fernando Antonio de, SAVÓIA, José Roberto Ferreira e SECURATO, José Robeto. Basiléia III: Impactos para os Bancos no Brasil. Disponível em http://www.scielo.br/pdf/rcf/2015nahead/1808-057x-rcf-201500720.pdf. Último acesso 23/11/2018

6. CONCLUSÃO

O *Criminal Compliance* surge como um instrumento poderoso no combate à lavagem de dinheiro no âmbito corporativo das *Fintechs.* Funciona de forma preventiva, invertendo a noção de *ultimaratio* do Direito Penal. Além do mais, é eficaz para a instituição internamente, e traz benefícios para a sociedade, como um meio de controle social.

Nesse contexto, o *compliance* emerge como uma alternativa de gestão da atividade empresarial, voltada ao cumprimento do Direito, de valores e princípios éticos. Inclusive, que se demonstra mais efetivo na prevenção de crimes e outras condutas ilícitas. Ou seja, o *compliance* corresponde a uma adaptação da política criminal no cenário econômico-financeiro.

A Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, por sua vez, cuida-se de temática de suma importância, seja pelo momento político-criminal (ou político-penal) do Estado Brasileiro de combate institucional à alegada corrupção, ou, ainda, pelo alargamento da tutela de regulação do Banco Central do Brasil e o acirramento em suas fiscalizações e apontamentos.

E a importância de se estudar, debater e implementar Programas de PLD-FT justifica necessariamente pelos impactos que os crimes de lavagem de dinheiro e de financiamento do terrorismo (entre outros) podem causar na sociedade, em níveis micro e macro. O ambiente inovador das *Fintechs*, além de proporcionar novas soluções, pode propiciar problemáticas nunca enfrentadas. Contudo, neste diapasão, as *Fintechs* possuem, mais do que a necessidade de PLD-FT (da qual não há como se escusar), a oportunidade de revolucionar o mercado financeiro, não apenas no oferecimento de soluções inovadoras, como anteriormente mencionado, mas também no estabelecimento de um arejado e moderno padrão ético mais elevado, oferecendo *prevenção*, *monitoramento* e *resposta*, calcados em procedimentos adequados e efetivos.

Diante de tal cenário é necessário observar, no que cabe as *Fintechs*, a importância da adoção de critérios trazidos pelo Acordo da Basiléia desde a sua primeira edição. Ainda, tais regulamentações devem passar por revisões, buscando adequar o conteúdo às *Fintechs*.

7. REFERÊNCIAS BIBLIOGRÁFICAS

APARECIDA CARDOSO, Maria; CHAVES DE AMORIM, Evelyse; RODRIGUES VICENTE, Ernesto Fernando. Os Impactos da Implementação de Controles Internos, Auditoria e Compliance no Combate e Prevenção à Lavagem de Dinheiro no brasil. Enfoque: Reflexão Contábil, vol.31, num. 3, set.-dez., 2012, p. 23-35. Disponível em: <http://www.redalyc.org/articulo.oa?id=307125339003>. Último acesso em 23/11/2018.

BRASIL. Exposição de Motivos da Lei n.º 9.613/98. Disponível em <http://fazenda.gov.br/orgaos/coaf/legislacao-e-normas/legislacao/exposicao-de-motivos-lei-9613.pdf/view>. Último acesso em 24/11/2018.

BUSATO, Paulo César. O que não se diz sobre *Compliance* em Direito Penal. In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017.

CARVALHO. F.C. et al. Economia Monetária e Financeira. Teoria e Política, Rio de Janeiro: Editora Campus, 2000, p. 341.

DE CARLI, Carla Veríssimo. Lavagem de Dinheiro: Ideologia da Criminalização e Análise do Discurso. 2ª ed. Verbo Jurídico, 2012.

FORIGO, Camila Rodrigues. A Figura do *Compliance Officer* no Direito Brasileiro: funções e responsabilização penal. 1 ed. Editora Multifoco: Rio de Janeiro, 2017.

INTERPOL, PHIPTO e THE GLOBAL INICIATIVE AGAINST TRANSNACIONAL ORGANIZED CRIME. World Atlas ofIllictFlows, 2018. Disponível em: <http://globalinitiative.net/world-atlas-of-illicit-flows/>. Acesso em 24 out. 2018.

MENDONÇA, Ana Rosa Ribeiro de. O Acordo da Basiléia de 2004: uma revisão em direção ás praticas de mercado. Revista Economia Politica Internacional: Análise Estratégica. Rio de Janeiro, UFRJ, nº 2, julho a setembro de 2004

NAJJARIAN, Irene Patrícia de Noronha. Fintech: novo desafio regulatório. Revista de Direito Bancário e do Mercado de Capitais. v.74. São Paulo, 2016.

SCANDELARI, Gustavo Britta. *Compliance* como Prevenção Idônea de Crimes e sua Compatibilização com a Intervenção Mínima. In. BUSATO, Paulo César; COUTINHO, Aldacy Rachid (org.). Aspectos Jurídicos do *Compliance*. 1. Ed. Florianópolis: Empório do Direito, 2017.

SAAD-DINIZ, Eduardo; SILVEIRA, Renato de Mello Jorge. *Compliance*, Direito Penal e Lei Anticorrupção. 1 ed. São Paulo: Saraiva, 2015.

TEIDER, Lucas H. A presunção de culpabilidade nos delitos econômicos como Direito Processual Penal do inimigo e os reflexos no instituto da prisão preventiva. *In*: Revista Iberoamericana deDerecho Penal y Criminología: Instituto Peruano Argentino de Derecho Penal - Universidad Nacional de Lomas de Zamora (Instituto enCienciasPenales - Facultad de Derecho) (Argentina), Número 1, Novembro de 2018.

VERÍSSIMO, Carla. Compliance: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2017.

FUTUROS POSSÍVEIS NO SISTEMA FINANCEIRO BRASILEIRO:
Arranjos de Pagamento, *fintechs* e pagamentos instantâneos

Danton Zanetti

Advogado. Professor na Faculdade de Direito Santa Cruz. Pós-graduado em Direito Processual Civil, pós-graduado em Direito e Processo do Trabalho.

Marta Regina Savi

Advogada na BoletoBancario.com. Mestra em Direito, pós-graduada em Direito, Logística e Negócios Internacionais e Direito Aplicado, graduada em Direito e História.

Thiago Camilo Alberton

Advogado. Coordenador de Risco e Compliance na BoletoBancário.com. MBA Executivo em Gestão Empresarial, pós-graduado em Direito Processual Civil.

RESUMO:
O presente artigo apresenta uma visão panorâmica do Sistema de Pagamentos Brasileiro, a partir da promulgação da Lei 12.365/2013, que traçou as linhas gerais dos Arranjos de Pagamento, bem como das diversas circulares e resoluções emitidas pelo Banco Central do Brasil com o fito de regular o sistema financeiro. A regulação é vista a partir da questão das *fintechs*, novas empresas de tecnologia de pagamentos, que crescem em número e representatividade perante o setor. Com a convergência do sistema financeiro nacional com as propostas de modernização trazidas por empresas que têm como motor a inovação, há a possibilidade de adoção de pagamentos instantâneos, nos moldes de países que já adotam a solução, como Estados Unidos e Reino Unido.

Palavras-chave:

Banco Central do Brasil – Arranjos de Pagamento – Pagamento Instantâneo – Direito Regulatório

Sumário:

1. Introdução 2. Arranjos de Pagamento 3. Credenciadores e Subcredenciadores 4. Um futuro possível: Pagamentos Instantâneos 5. Referências Bibliográficas

INTRODUÇÃO

Embora existam no Brasil inúmeras opções de meios de pagamento, o Sistema de Pagamentos Brasileiro (SPB) ainda não dispõe de meios hábeis a atender toda a população e não está plenamente adequado às necessidades do mercado. Em localidades remotas, por exemplo, não há um volume suficiente de cédulas de moeda em circulação, em decorrência de dificuldades logísticas, agravadas pelo fechamento de agências ante aos ataques maciços de quadrilhas especializadas em explodir caixas eletrônicos.

Mesmo nas grandes cidades observa-se uma dificuldade dos estabelecimentos comerciais em obter moedas metálicas para troco, pois o custo para cunhar as moedas supera o seu valor monetário. Para agravar o problema há pessoas que têm o hábito de acumulá-las, ainda que cientes dos rendimentos que estão deixando de ter caso optassem por uma aplicação financeira.

Por questões de logística e segurança, dentre outros fatores, o pagamento via cartão de débito e crédito difundiu-se amplamente nas últimas décadas. Eles conferem maior segurança ao consumidor, que não necessita transportar um grande volume de dinheiro e ainda pode parcelar suas compras. Para o lojista, além da segurança e de afastar o risco de inadimplência, reduz o risco de perdas financeiras decorrentes de roubos.

Os pagamentos via cartão de crédito acarretaram uma redução significativa nas operações realizadas via cheque, uma vez que o risco de inadimplência decorrente da sua utilização é praticamente nulo. O único risco para o lojista, é ser vítima de um pagamento realizado mediante fraude ou ser objeto de uma tentativa de fraude por meio da solicitação indevida de um *chargeback* pelo cliente. Em contrapartida, os lojistas têm que arcar com taxas elevadas para poderem operar com essa modalidade de pagamento. Já os consumidores, são obrigados a pagar tarifas de anuidade para utilizarem o método e sua utilização como meio de pagamento é limitada a limites pré-estabelecidos pelas instituições emissoras.

Da mesma maneira, as transferências eletrônicas entre bancos permitiram uma redução no risco de roubos em decorrência da desnecessidade de transportar grandes volumes financeiros em espécie. Contudo o sistema é disponibilizado apenas em dias úteis e ainda é um serviço relativamente caro. Os valores elevados das tarifas bancárias decorrem em grande parte da concentração bancária. No Brasil 5 grandes bancos controlam 82% dos ativos financeiros[91]. Tal fenômeno se explica pelo alto nível de regulamentação imposta aos bancos e da dificuldade de consolidação de bancos menores, evitados pelos clientes, que primam pela presença física, para realização de saques e pagamentos com seus cartões de débito.

Nesse cenário as *fintechs* surgem como uma opção viável para redução da concentração bancária, por meio do livre mercado. O crescente aumento no volume de transações financeiras realizadas por essas empresas demonstra que a tendência é que essas empresas ocupem um espaço cada vez maior no sistema financeiro, o que demandará a observância de regras rígidas de *compliance*, governança corporativa, controles internos, prevenção à lavagem de dinheiro e o financiamento ao terrorismo.

Todavia, a ausência de caixas eletrônicos e da possibilidade da realização de algumas formas de pagamento inviabiliza a sua utilização como plataforma única para serviços financeiros. Atualmente, os clientes de *fintechs* que pretendam usufruir de todo o sistema financeiro precisam

---

[91] CASTRO, Fabrício de. **Concentração bancária cresceu no Brasil, diz Banco Central.** Cinco grandes bancos concentram 82% dos ativos brasileiros, maior índice para todos os países incluídos na pesquisa, à exceção da Holanda. Disponível em: https://economia.estadao.com.br/noticias/geral,concentracao-bancaria-cresceu-no-brasil-diz-banco-central,70002348108 Acessado em: 23/11/2018

manter contas em bancos. Algumas *fintechs* já consolidadas no mercado começam a listar clientes interessados em usufruir de seus sistemas de conta digital, mas as versões das plataformas ainda estão em fase de experimentação.

Nesse contexto os pagamentos instantâneos se apresentam como potencial meio de substituir em definitivo os pagamentos realizados em espécie e como funcionalidade que permitirá que as *fintechs* assumam por completo os serviços financeiros. Eles reúnem os benefícios já observados nos meios de pagamentos eletrônico existente, trazendo, também, benefícios adicionais.

1. ARRANJOS DE PAGAMENTO

A ementa da Lei 12.865, de 09 de outubro de 2013, deixa claro que o tema Arranjos de Pagamento foi incluído na ordem do dia "às pressas":

> Autoriza o pagamento de subvenção econômica aos produtores da safra 2011/2012 de cana-de-açúcar e de etanol que especifica e o financiamento da renovação e implantação de canaviais com equalização da taxa de juros; dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB); autoriza a União a emitir, sob a forma de colocação direta, em favor da Conta de Desenvolvimento Energético (CDE), títulos da dívida pública mobiliária federal; estabelece novas condições para as operações de crédito rural oriundas de, ou contratadas com, recursos do Fundo Constitucional de Financiamento do Nordeste (FNE); altera os prazos previstos nas Leis no 11.941, de 27 de maio de 2009, e no 12.249, de 11 de junho de 2010; autoriza a União a contratar o Banco do Brasil S.A. ou suas subsidiárias para atuar na gestão de recursos, obras e serviços de engenharia relacionados ao desenvolvimento de projetos, modernização, ampliação, construção ou reforma da rede integrada e especializada para atendimento da mulher em situação de violência; disciplina o documento digital no Sistema Financeiro Nacional; disciplina a transferência, no caso de falecimento, do direito de utilização privada de área pública por equipamentos urbanos do tipo quiosque, trailer, feira e banca de venda de jornais e de revistas; altera a incidência da Contribuição para o PIS/Pasep e da Cofins na cadeia de produção e comercialização da soja e de seus subprodutos; altera as Leis nos 12.666, de 14 de junho de 2012, 5.991, de 17 de dezembro de 1973, 11.508, de 20 de julho de 2007, 9.503, de 23 de setembro de 1997, 9.069, de 29 de junho de 1995, 10.865, de 30 de abril de 2004, 12.587, de 3 de janeiro de 2012, 10.826, de 22 de dezembro de 2003, 10.925, de 23 de julho de 2004, 12.350, de 20 de dezembro de 2010, 4.870, de 1o de dezembro de 1965 e 11.196, de 21 de novembro de 2005, e o Decreto no 70.235, de 6 de março de 1972; revoga dispositivos das Leis nos 10.865, de 30 de abril de 2004, 10.925, de 23 de julho de 2004, 12.546, de 14 de dezembro de 2011, e 4.870, de 1o de dezembro de 1965; e dá outras providências.[92]

A extensa redação, que dá conta de tópicos como financiamento da renovação e implantação de canaviais, por exemplo, reservou o espaço dos artigos 6º ao 15 para regulamentar e definir conceitos importantes para o Sistema de Pagamentos Brasileiro (SPB).

A lei define o arranjo de pagamento como o "conjunto de regras e procedimentos que disciplina a prestação de determinado serviço de pagamento ao público aceito por mais de um recebedor, mediante acesso direto pelos usuários finais, pagadores e recebedores"[93]. Em seguida, conceitua os instituidores do arranjo (art. 6º, II), a pessoa jurídica responsável pelo arranjo de pagamento, e os participantes desse arranjo (art. 6º, III).

Elenca como atividades principais dessas empresas: disponibilizar serviço de aporte ou saque de recursos mantidos em conta de pagamento; executar ou facilitar a instrução de pagamento relacionada a determinado serviço de pagamento, inclusive transferência originada de ou destinada

---

[92] BRASIL. **Lei 12.365, de 09 de outubro de 2013**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12865.htm Acesso: 29/11/2018

[93] BRASIL. **Lei 12.365, de 09 de outubro de 2013**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12865.htm Acesso: 29/11/2018

a conta de pagamento; gerir conta de pagamento; emitir instrumento de pagamento; credenciar a aceitação de instrumento de pagamento; executar remessa de fundos; converter moeda física ou escritural em moeda eletrônica, ou vice-versa, credenciar a aceitação ou gerir o uso de moeda eletrônica; e outras atividades relacionadas à prestação de serviço de pagamento.

A legislação ainda esclarece que a adesão de a adesão a arranjos de pagamento por parte das Instituições Financeiras deve seguir as normas previstas pelo Banco Central e diretrizes do Conselho Monetário Nacional e estabelece a diferenciação entre as Instituições Financeiras e demais instituições de pagamento, que não podem realizar atividades privativas das primeiras.

Há, ainda, a previsão de observância de princípios básicos para arranjos, instituidores e participantes. Solidez, eficiência, promoção da competição, acesso não discriminatório, atendimento às necessidades dos usuários finais, com liberdade de escolha, segurança, proteção de interesses econômicos, tratamento não discriminatório, privacidade, proteção de dados pessoais, transparência, acesso a informações claras e completas sobre as condições de prestação dos serviços. Criação e manutenção de mecanismos e processos para a garantia do sigilo das operações e serviços fornecidos ao mercado e formas de assegurar a integridade, confiabilidade e segurança das transações realizadas e legitimidade das operações contratadas.

Tais obrigações são basilares e de fundamental importância para o funcionamento do sistema financeiro nacional, considerando a sensibilidade da questão monetária, tanto nacional quanto internacionalmente. E, neste aspecto, vale frisar que a abertura de possibilidade para que outras empresas além de instituições financeiras – e, dentre elas, os bancos tradicionais – operem no país é recente e ainda é fato notório a alta concentração bancária verificada no Brasil[94].

Contudo, buscando possibilitar o surgimento de novos *players* no mercado financeiro nacional, nem todas as entidades presentes no mercado de meios de pagamento estão, de forma direta, sujeitas às regras do Banco Central. O BACEN excluiu de sua competência aqueles que não apresentam riscos sistêmicos significativos, tendo estipulado, mediante as circulares de regulamentação, que arranjos de pagamento que fiquem abaixo de seus parâmetros definidos, atualmente, na circular de 3.885, de 2018[95], devem observar as regras do setor, mas não dependem de autorização de funcionamento.

O artigo 9º da Lei ora debatida define que a competência do Banco Central está estabelecida na disciplina dos arranjos de pagamento, bem como da constituição, funcionamento, fiscalização e descontinuidade das instituições de pagamento; adoção de medidas de promoção de competição, inclusão financeira e transparência na prestação de serviços de pagamentos, dentre outras atribuições. Através dessa autorização legal concedida, o Banco Central regula o setor, expedindo circulares e resoluções que devem ser observadas pelas instituições que necessitam da autorização do BACEN e, considerando a competição no setor, acabam sendo incorporadas também por instituições que ainda não atingiram os parâmetros mínimos para o pedido de funcionamento.

Os Arranjos de Pagamento são instituídos por bandeiras, que devem, de acordo com as normas do Banco Central, ter constituição no Brasil, objeto social compatível e comprovada capacidade técnica-operacional, organizacional, administrativa e financeira. Devem, ainda, estabelecer em seu

---

[94] ASERC, Associação Nacional de Empresas de Recuperação de Crédito. **Cinco bancos detêm R$ 4 de cada R$ 5 movimentados no país**. 17 de outubro de 2017. http://www.aserc.org.br/2017/10/17/cinco-bancos-detem-r-4-de-cada-r-5-movimentados-no-pais/ Acesso: 29/11/2018.

[95] BRASIL, Banco Central do. **Circular nº 3885, de 26 de março de 2018**. https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=3885&tipo=Circular&data=26/3/2018 Acesso: 29/11/2018.

regulamento procedimentos de gerenciamento de riscos, requisitos operacionais mínimos a serem cumpridos pelos participantes[96].

Por seu turno, as instituições de pagamento podem ser divididas em três grandes categorias: credenciador, que faz habilitação de estabelecimentos sem gerenciar conta de pagamento, e que será abordado com maiores detalhes no próximo tópico; emissor de instrumento de pagamento pós-pago e, finalmente, emissor de moeda eletrônica, entidade que faz gestão de uma conta de pagamento, disponibiliza transação e converte em moeda física o numerário eletrônico disponível a cada cliente final. Para fins de regulação, o Banco Central define que as moedas eletrônicas são caracterizadas como recursos em reais mantidos em meio eletrônico, permitindo que o usuário realize pagamentos com estes valores.

Aqui vale pontuar que o emissor de moeda eletrônica não tem relação com entidades que trabalham com moedas virtuais, chamadas também de criptomoedas. O Banco Central do Brasil não emite, regula ou garante de qualquer forma as criptomoedas. Não existe, atualmente, qualquer legislação ou regulação vigente que trate especificamente deste tema. O BACEN, em sua página na internet, aponta, ainda, que "o cidadão que decidir utilizar os serviços prestados por essas empresas deve estar ciente dos riscos de eventuais fraudes ou outras condutas de negócio inadequadas, que podem resultar em perdas patrimoniais"[97].

A Lei 12.365 prevê que descumprimentos às normas legais e também à regulamentação específica estão sujeitas às penalidades previstas pela legislação, e que a responsabilidade é tanto das instituições como de seus administradores e membros de diretoria. O parágrafo único do artigo 11 do mesmo diploma legal é, ainda, incisivo quanto à possibilidade de aplicação pontual dos dispositivos do Código de Defesa do Consumidor, em especial.

Por fim, a legislação é clara ao exigir que os recursos mantidos em contas de pagamento administradas por instituições de pagamento – quer sejam autorizadas pelo BACEN, quer não – constituem patrimônio separado e não se confundem, em qualquer hipótese, com patrimônio da entidade. Tal salvaguarda é um importante mecanismo na construção da confiança no sistema financeiro nacional e deve ser observado por qualquer empresa que pretenda atuar no setor.

Vale, ainda, estabelecer que uma das intenções do legislador é a de fazer com que o cidadão possa ter a seu serviço uma maior gama de serviços de pagamento, em especial pensando na parcela da população que não possui contas em banco, chamados desbancarizados. A lei observada pretende a construção de um ambiente mais seguro para a prestação dos serviços, além de incentivar a competição e facilitar o processo de inclusão financeira.

Todavia, o que se observa é que, na prática, a bandeira regulamenta seu arranjo de pagamento, instituindo normas que devem ser cumpridas por todas as instituições que desejem integrar aquela rede de credenciamento. Há que se notar que a abertura de mercado apresentada e anunciada tanto pela legislação quanto pelo próprio Banco Central acaba perdendo a amplitude quando concentra na instituidora do arranjo o regramento de seus arranjos de forma hierárquica.

---

[96] BRASIL, Banco Central do. **FAQ – Arranjos e Instituições de Pagamentos.** Disponível em https://www.bcb.gov.br/pre/bc_atende/port/arranjo.asp Acesso: 29/11/2018.

[97] BRASIL, Banco Central do. **FAQ – Moedas Virtuais.** Disponível em https://www.bcb.gov.br/pre/bc_atende/port/moedasvirtuais.asp?idpai=FAQCIDADAO Acesso: 29/11/2018.

O resultado é que a bandeira que detém maior alcance nacional e, por consequência, maior poder financeiro, acaba detendo, também, o controle efetivo de participantes e não participantes de seu arranjo.

A) CREDENCIADORES E SUBCREDENCIADORES

No contínuo processo de evolução das relações financeiras, que tem como principais objetivos proporcionar a melhora na qualidade e velocidade da prestação de serviços, redução de custos, mitigação de riscos e promover a inclusão financeira[98], em especial da população desbancarizada[99], ganham relevo as atuações dos "credenciadores" e dos "subcredenciadores", que, na terminologia comumente adotada pelo mercado, também são conhecidos como "adquirentes" e "subadquirentes", respectivamente.

Partindo do conceito previamente apresentado de Arranjo de Pagamento, conclui-se pela possibilidade da inclusão de intermediários na cadeia de arranjo de pagamento através de instituições de pagamento responsáveis por, dentre outras atividades, *"credenciar a aceitação de instrumento de pagamento"* (art. 6º, III, "e") – os credenciadores – o que vai ao encontro do princípio da interoperabilidade, previsto no artigo 7º, I, da Lei 12.865/2013, dispositivo legal do qual se extrai ser possível que transações sejam realizadas por sistemas que não fazem parte do mesmo arranjo de pagamento.[100]

Poucos dias após a publicação da Lei 12.865/2013, foram expedidas pelo Banco Central as Circulares nº 3.682 e 3.683, ambas de 4 de novembro de 2013 (atualmente revogada), sendo que esta última trouxe em seu artigo 2º, III, o conceito de credenciador como toda *"instituição de pagamento que, sem gerenciar conta de pagamento, habilita recebedores, pessoas naturais ou jurídicas, para a aceitação de instrumento de pagamento emitido por instituição de pagamento ou por instituição financeira participante de um mesmo arranjo de pagamento".*

Quanto à figura do subcredenciador, não contemplada na Lei 12.865/2013 e nas Circulares do BACEN acima mencionadas, cabe historiar que esta teve sua gênese no mercado de vendas *online*, surgindo como um meio para conferir maior segurança e credibilidade às plataformas de vendas pela internet e às transações realizadas em meio digital, uma vez que podem inclusive atuar como instrumentos antifraude e de conciliação bancária.[101]

Há quem veja os benefícios proporcionados pelo subcredenciador, mas o considere uma solução imperfeita, pois, embora os custos de implantação sejam sensivelmente mais baixos que os de outros meios de pagamento[102], sua receita provém essencialmente da divisão – ou *"split"* – de taxas pagas a credenciadores.[103]

Muito embora houvesse um esforço em regular o arranjo de pagamento, até então persistia um cenário de grande insegurança jurídica para alguns dos *players* que, direta ou indiretamente

---

[98] PEREIRA, Cesar; CARDOSO, André Guskow; BENZECRY, Rubens; QUINTÃO, Luísa. **Regulação do Pagamento Eletrônico (E-payment) e da Moeda Eletrônica (E-Money).** Disponível em: <https://www.migalhas.com.br/arquivos/2016/5/art20160505-03.pdf>; Acesso em 20.11.2018.

[99] Com relação à democratização do acesso ao sistema bancário, o Banco Central do Brasil – BACEN emitiu documento intitulado "Relatório de inclusão financeira", no qual definiu o termo inclusão financeira como o *"processo de efetivo acesso e uso pela população de serviços financeiros adequados às suas necessidades, contribuindo com sua qualidade de vida".*

[100] COTS, Márcio. **Regulação do Pagamento Eletrônico no Brasil.** *In: E-Commerce News,* 12 de maio de 2014. Disponível em: <https://ecommercenews.com.br/artigos/cases/regulamentacao-do-pagamento-eletronico-no-brasil/>; Acesso em 23/11/2018.

[101] PEREIRA, Cesar, et. al. Op. Cit.

[102] Idem.

[103] *"Ainda assim, é bom lembrar que apesar de diminuir o custo de um lado, a subadquirente ainda não é a solução perfeita, já que esse tipo de sistema tem um contrato que é cobrado com porcentagens das vendas, algo que varia de 3 a 7% nos maiores players. Isso significa que os lucros são menores, e diminuem ainda mais caso o cliente compre parcelado, com taxas próximas de 2 a 3% por cada parcela".* Disponível em: <https://pagar.me/blog/subadquirente-e-adquirente-o-que-voce-precisa-saber>; Acesso em: 28.11.2018.

influíam na cadeia de pagamento, uma vez que, na ausência de norma específica acerca do tema, os subcredenciadores em operação há época não detinham qualquer certeza sobre sua legitimidade e licitude de sua atividade, tampouco dos requisitos para sua atuação, considerando que se considerava desnecessária sua sujeição à autorização de funcionamento e demais condições voltadas a regulação das demais instituições de pagamento.[104]

Consequentemente, para se resguardarem de eventuais riscos e interferências dos órgãos regulatórios, muitos subcredenciadores já adotavam postura conservadora, visando se adequar às regras dos arranjos de pagamento, inclusive no que tange à participação na liquidação centralizada em grade única.[105]

Feitas estas considerações, novo marco regulatório se deu a partir das Circulares do BACEN nº 3.885 e 3.886, ambas de 26 de março de 2018, que aprofundou diversos pontos da Lei 12.865/2013 e da Circular nº 3.682/2013.

A Circular nº 3.885/2018 ampliou o conceito de credenciador, que não mais se limitava apenas às instituições de pagamento que habilitam recebedores, mas passou a alcançar também aquelas que participam do processo de liquidação das transações de pagamento como credor perante o emissor (art. 4º, III, "b").

A seu turno, a Circular nº 3.886/2018, enfim, trouxe definição objetiva da figura do subcredenciador, tratando expressamente do modo de interação deste com os responsáveis pela instituição do arranjo de pagamento, estabelecendo, ainda, os critérios para exigir a participação dos subcredenciadores na liquidação centralizada em grade única.

No que tange ao conceito, definiu-se subcredenciador como o *"participante do arranjo de pagamento que habilita usuário final recebedor para a aceitação de instrumento de pagamento emitido por instituição de pagamento ou por instituição financeira participante de um mesmo arranjo de pagamento, mas que não participa do processo de liquidação das transações de pagamento como credor perante o emissor"*, conceito que foi introduzido no inciso VIII, do artigo 2º, do texto vigente da Circular nº 3.682/2013.

Em outras palavras, o subcredenciador nada mais é que uma empresa que oferta serviços de pagamento por meio eletrônico, intermediando arranjos de pagamento principalmente junto a negócios de pequeno porte ou com operação *online,* ao possuir relação com um ou mais credenciadores, ao mesmo tempo em que habilita estabelecimentos fornecedores de bens e prestadores de serviços para aceitarem instrumentos de pagamento, como, por exemplo, cartões de crédito.[106]

Desde a edição da Circular nº 3.885/2013 do BACEN, que estabeleceu limites regulatórios para a atuação de instituições de pagamento e dispôs os critérios de sujeição destas à autorização do BACEN, a figura do subcredenciador, não dependia de autorização para operar[107], situação que, em regra, permanece inalterada, ressalvadas as instituições subcredenciadoras que tiveram

---

[104] PEREIRA, Cesar, et. al. Op. Cit.

[105] BALDUCCINI, Bruno; GOMES, Fernando Mirandez Del Nero; CARA, Maria de; SALOMÃO, Raphael Palmieri; MELLO, Marcelo Junqueira de. **Banco Central disciplina a figura do subcredenciador.** Disponível em: <https://www.migalhas.com.br/dePeso/16,MI277839,31047-Banco+Central+disciplina+a+figura+do+subcredenciador>; Acesso em: 26.11.2018;

[106] FIALDINI, Vanêssa; RIBEIRO, Tatiana Facchim. **Os "Subadquirentes" no mercado de Meios de Pagamento.** Disponível em: <https://www.migalhas.com.br/dePeso/16,MI223673,11049-Os+Subadquirentes+no+mercado+de+Meios+de+Pagamento>; Acesso em 22/11/2018.

[107] BRASIL, Banco Central do. **FAQ – Liquidação Centralizada.** Disponível em <https://www.bcb.gov.br/htms/novaPaginaSPB/liqcentralizada.asp?idpai=SPBARRPAG#12>; Acesso em 27.11.2018;

participação na liquidação centralizada de transações em valor total igual ou superior a R$ 500.000,00 (quinhentos milhões de reais), considerados os últimos doze meses de operação, conforme disposto no artigo 26, § 5º, I, da Circular nº 3.682/2013, com a redação dada pela Circular nº 3.886/2018.

Tanto em virtude da recente regulação da figura do subcredenciador, quanto por conta dos multifacetados debates jurídicos travados acerca de temas ligados à responsabilidade de tais instituições, há muito campo para estudo, sobretudo com relação a eventual dever de indenizar perante consumidores. Num hipotético cenário de invasão da conta de determinado cliente por terceiro durante uma transação efetuada pelo subadquirente, por mais que este atue apenas como um intermediário e não detenha uma relação direta com o consumidor em si, há quem defenda[108] – a nosso ver com razão – ser *também* de responsabilidade do subadquirente a reparação pelos danos causados, eis que, ao prestar tais serviços, ocupa a posição jurídica de fornecedor (art. 3º, CDC) na relação de consumo, respondendo solidariamente ao fornecedor principal, que detém a relação direta com o consumidor.

Conclui-se, pois, que as medidas legislativas e principalmente regulatórias foram levadas a cabo em razão da necessidade de alavancagem de acesso do empresariado aos instrumentos de pagamento, sendo que, quanto à atuação específica dos subcredenciadores, vislumbrou-se baixo risco de impacto das operações sobre o sistema financeiro. As medidas foram bem vistas pela comunidade empresária justamente por estabelecer procedimento diferenciado a instituições de pagamento perante o Banco Central do Brasil – BACEN e, assim, dar efetividade ao princípio da interoperabilidade, barateando custos operacionais e, assim, ampliando o acesso a serviços de arranjos de pagamento, sobretudo considerados os pequenos e médios empreendedores, cujas atividades, como visto, comumente demandam transações de menor porte.[109]

[108] FIALDINI, V.; RIBEIRO, T. F., Op. cit.
[109] Idem.

B) UM FUTURO POSSÍVEL: OS PAGAMENTOS INSTANTÂNEOS

O pagamento instantâneo pode ser definido como pagamento em tempo real, em que não apenas a mensagem de confirmação de pagamento é realizada segundos após o processamento da transação, mas também a disponibilização dos fundos ao recebedor. O tempo de processamento do pagamento chegar a ser mais rápido que o da maioria das criptomoedas, que dependem de uma mineração de blocos para a confirmação do pagamento.

Dentre as características dos Pagamentos Instantâneos, as que mais se destacam são a velocidade de processamento e disponibilidade contínua do serviço. Os pagamentos instantâneos serão disponibilizados 24 horas por dia, todos os dias do ano, inclusive fins de semana e feriados. O tempo máximo total da transação (pagador - liquidação - recebedor) será de 12 segundos. Assim sendo, tais pagamentos permitirão a transferência imediata de recursos por meios simplificados, incluindo a leitura de *QR Code*.

Respeitando mecanismos de segurança, a facilidade para a realização de um pagamento será próxima a existe hoje para o envio de mensagens instantâneas pelo celular.

A descentralização dos serviços financeiros por meio de *fintechs* propiciará uma redução significativa no custo das transações, cujo volume tende a aumentar significativamente. Ao mesmo tempo, a redução progressiva da circulação de valores em espécie favorecerá os mecanismos de prevenção a fraudes, lavagem de dinheiro, sonegação fiscal e financiamento ao terrorismo, uma vez que permitirá um maior controle do fluxo financeiro.

Os pagamentos instantâneos abrangerão não apenas a relação entre particulares e as transações comerciais, podendo ser classificados da seguinte forma:

Person to Person (P2P)	Pagamentos entre indivíduos; pagamentos para relacionamentos de troca entre pessoas físicas, incluindo vendas e prestação de serviços
Person to Business (P2B)	Comércio e serviços em geral no ponto de venda ou no comércio eletrônico; pagamento de contas
Business to Business (B2B)	Pagamentos entre pessoas jurídicas, em geral
Business to Person (B2P)	Pagamento de salários; seguros
Person to Government (P2G)	Pagamento de impostos e taxas, em geral
Government to Person (G2P)	Pagamento de salários; benefícios sociais
Business to Government (B2G)	Recolhimento de impostos pelas empresas
Government to Business (G2B)	Pagamento de convênios e serviços dos entes governamentais para empresas

Atento às possibilidades e dificuldades do tema, o Banco Central do Brasil instituiu um Grupo de Trabalho para definir os parâmetros a serem observados na implementação do Ecossistema de Pagamentos Instantâneos Brasileiro, cuja conclusão dos trabalhos está prevista para o fim do ano de 2018. Esse grupo foi estabelecido por meio da Portaria 97.909/2018, do Chefe do Departamento de Operações Bancárias e de Sistema de Pagamentos (DEBAN) e do Chefe do Departamento de Regulação do Sistema Financeiro (DENOR), ambos do BACEN. Esse grupo de trabalho foi constituído no âmbito do Fórum de Arranjos e Instituições de Pagamento (AIP), o qual foi Instituído pela Portaria 85.478/2015.

Participam desse grupo de trabalho associações, *players* do mercado e também consultorias. Dentre seus objetivos, está a avaliação se haverá a necessidade de ser estabelecida uma camada de compensação, que consistiria na existência de agentes que provejam serviços de receber e transmitir as instruções de pagamento entre os participantes do ecossistema. Em relação a esse ponto, a ABIPAG sinalizou que caso isso ocorra, deverá ser propiciada a ampla concorrência, para evitar a criação de barreiras para novos entrantes no mercado.

As definições mais relevantes do grupo de trabalho são as de que: o ecossistema funcionará em um modelo de liquidação bruta em tempo real; o Banco Central irá prover serviço de transmissão de instrução de pagamento entre os diversos prestadores de serviços de pagamento participantes do ecossistema, além da infraestrutura de liquidação; será constituído um comitê central consultivo para ajudar o Banco Central a definir as regras gerais do ecossistema e um comitê de governança para definir regras específicas do ecossistema, com o objetivo de formar convenções sobre temas diversos; e serão previstas pelo menos três modalidades de participação no ecossistema: participante direto, participante indireto e provedor de serviço de iniciação de pagamentos.

Esse grupo de trabalho é apenas uma das frentes do BACEN, que também está realizando um *benchmarking* como modelos já existentes em outros países, como Estados Unidos, Canadá, Austrália, União Europeia, México, Suécia, Dinamarca, Reino Unido, Itália, Singapura e Índia. Essas duas frentes são necessárias, pois o BACEN já concluiu que nenhum modelo pode ser replicado exatamente da forma pela qual foi concebida em outros países para o Brasil, sendo necessário identificar o que faz sentido em cada um deles para o nosso sistema.

Da experiência internacional, opta-se por apresentar, nesta oportunidade, três modelos para análise. O primeiro, dos Estados Unidos. O país adota o *Real-Time Payments* (RTP System). O primeiro pagamento ocorreu em 13 de novembro de 2017, entre o BNY Mellon e o U.S. Bank. Críticos ao sistema apontam como deficiência a ausência de uma autoridade reguladora para liderar os esforços de desenvolvimento do sistema. O diferencial americano é o envio de mensagens de confirmação na realização do pagamento, o que permite maior transparência e segurança na transação entre as partes, ao notifica-las da conclusão da transação.

Já no Reino Unido houve a adoção do denominado *UK Faster Payments* (Pay.UK). O sistema foi implementado em 2008 pela Faster Payments Scheme Limited (FPSL), possibilitando a realização de transações por celulares, por laptops e desktops e telefone, com disponibilidade 24 horas, durante todos os dias da semana. Desde sua criação, já permitiu a circulação de nove bilhões de pagamentos, envolvendo um montante de seis trilhões de libras esterlinas em volume financeiro. Atualmente, vinte e uma organizações são participantes do Sistema e mais de quatrocentas instituições financeiras são aptas a operá-lo e o Sistema está disponível para mais de cinquenta e dois milhões de usuários.

Na União Europeia, o Banco Central Europeu está implementando o TARGET Instant Payment Settlement (TIPS), previsto para ser lançado no final de 2018. Ele também estará disponível de forma ininterrupta, durante todos os dias da semana. Em um primeiro momento o Sistema apenas aceitará transações em Euro, mas há previsão de que o Sistema aceite novas moedas no futuro. Nesse modelo, o tempo total de transação será de até dez segundos. A adesão ao sistema dependerá da observância de regras contratuais e regulatórias, sendo que o custo de transação foi fixado em 0.20 centavos de euro (€0.002) por transação, valor este que será mantido pelo menos nos 2 primeiros anos de operação. Está previsto que não haverá custo de depósito ou manutenção de saldo na plataforma. O projeto teve início em outubro de 2016. Os requerimentos técnicos foram frutos de um trabalho de consulta aos bancos centrais dos países envolvidos e participantes do mercado, realizado em 2017.

Neste caso, tal qual o grupo de trabalho criado pelo Banco Central no Brasil, também houve a composição de uma mesa de profissionais oriundos de bancos de varejo, câmaras interbancárias de pagamento e bancos centrais dos países participantes. Esse grupo tinha por objetivo prover informações necessárias para o planejamento, teste e cobrança. Para viabilizar a sua implementação, os testes do sistema foram iniciados no segundo trimestre de 2018.

Da análise do sistema financeiro nacional, bem como através de um breve panorama de soluções encontradas em outros países, tem-se que a implementação dos pagamentos instantâneos no Brasil permitirá uma redução na concentração bancária, ao permitir que as *fintechs* ofereçam todo tipo de soluções financeiras relacionadas a pagamentos. Consequentemente o custo transacional tende a ser reduzido, ao mesmo que uma parcela maior da população passará a ter acesso ao Sistema de Pagamentos Brasileiro, reduzindo o fluxo de moeda em espécie e favorecendo os mecanismos de prevenção a fraudes, lavagem de dinheiro, financiamento ao terrorismo e sonegação fiscal.

C) REFERÊNCIAS

ASERC, Associação Nacional de Empresas de Recuperação de Crédito. Cinco bancos detêm R$ 4 de cada R$ 5 movimentados no país. 17 de outubro de 2017. http://www.aserc.org.br/2017/10/17/cinco-bancos-detem-r-4-de-cada-r-5-movimentados-no-pais/ Acesso: 29/11/2018.

BALDUCCINI, Bruno; GOMES, Fernando Mirandez Del Nero; CARA, Maria de; SALOMÃO, Raphael Palmieri; MELLO, Marcelo Junqueira de. Banco Central disciplina a figura do subcredenciador. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI277839,31047-Banco+Central+disciplina+a+figura+do+subcredenciador>; Acesso em: 26.11.2018;

BIS, Bank for International Settlements. Committee on Payments and Market Infrastructures. Fast payments: enhancing the speed and availability of retail payments. Disponível em: https://www.bis.org/cpmi/publ/d154.pdf Acessado em 25/11/2018

BRASIL, Banco Central do. Circular nº 3885, de 26 de março de 2018. https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=3885&tipo=Circular&data=26/3/2018 Acesso: 29/11/2018.

BRASIL, Banco Central do. FAQ – Arranjos e Instituições de Pagamentos. Disponível em https://www.bcb.gov.br/pre/bc_atende/port/arranjo.asp Acesso: 29/11/2018.

BRASIL, Banco Central do. FAQ – Liquidação Centralizada. Disponível em <https://www.bcb.gov.br/htms/novaPaginaSPB/liqcentralizada.asp?idpai=SPBARRPAG#12>; Acesso em 27.11.2018;

BRASIL, Banco Central do. FAQ – Moedas Virtuais. Disponível em https://www.bcb.gov.br/pre/bc_atende/port/moedasvirtuais.asp?idpai=FAQCIDADAO Acesso: 29/11/2018.

BRASIL, Banco Central do. GT – Pagamentos Instantâneos. Disponível em: https://www.bcb.gov.br/htms/novaPaginaSPB/GTPagInst.asp?IDPAI=PAGINSTA Acessado em 25/11/2018

BRASIL, Banco Central do. Relatório de inclusão financeira. N. 3. Brasília: Banco Central do Brasil, 2015.

BRASIL. Lei 12.365, de 09 de outubro de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12865.htm Acesso: 29/11/2018

CASTRO, Fabrício de. Concentração bancária cresceu no Brasil, diz Banco Central. Cinco grandes bancos concentram 82% dos ativos brasileiros, maior índice para todos os países incluídos na pesquisa, à exceção da Holanda. Disponível em: https://economia.estadao.com.br/noticias/geral,concentracao-bancaria-cresceu-no-brasil-diz-banco-central,70002348108 Acessado em: 23/11/2018

COTS, Márcio. Regulação do Pagamento Eletrônico no Brasil. In: E-Commerce News, 12 de maio de 2014. Disponível em: <https://ecommercenews.com.br/artigos/cases/regulamentacao-do-pagamento-eletronico-no-brasil/>; Acesso em 23/11/2018.

European Central Bank. TARGET Instant Payment Settlement (TIPS). Disponível em: https://www.ecb.europa.eu/paym/target/tips/html/index.en.html Acessado em: 25/11/2018

FIALDINI, Vanêssa; RIBEIRO, Tatiana Facchim. Os "Subadquirentes" no mercado de Meios de Pagamento. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI223673,11049-Os+Subadquirentes+no+mercado+de+Meios+de+Pagamento>; Acesso em 22/11/2018.

PEREIRA, Cesar; CARDOSO, André Guskow; BENZECRY, Rubens; QUINTÃO, Luísa. Regulação do Pagamento Eletrônico (E-payment) e da Moeda Eletrônica (E-Money). Disponível em: <https://www.migalhas.com.br/arquivos/2016/5/art20160505-03.pdf>; Acesso em 20.11.2018.

The Clearing House. RTP. Disponível em: https://www.theclearinghouse.org/payment-systems/rtp/ Acessado em: 25/11/2018
UK Faster Payments. Disponível em: http://www.fasterpayments.org.uk/ Acessado em: 25/11/2018

EXCHANGES DE CRIPTOMOEDAS X BANCOS:

UMA QUESTÃO DE DIREITO CONCORRENCIAL?

Renata Caroline Kroska

Procuradora do Município de Quatro Barras,

Mestranda em Políticas Públicas pela UFPR em tecnologia, regulação e sociedade,

Membra da Comissão de Inovação e Gestão da OAB/PR

RESUMO:
O artigo propõe uma análise à luz do direito concorrencial sobre o encerramento das contas das exchanges de criptomoedas pelos bancos. A questão foi judicializada, argumentando-se, principalmente, aspectos relativos ao direito do consumidor, culminando em decisão em sede de recurso especial na qual se decidiu pela legalidade do encerramento das contas. Antes mesmo da decisão judicial, a matéria foi submetida ao CADE (Conselho Administrativo de Defesa Econômica) alegando-se duas violações ao direito concorrencial, quais sejam: recusa de contratar e negativa de acesso a infraestrutura essencial. Entretanto, para que sejam aplicadas medidas do antitruste deverá ficar caracterizado, através do teste do monopolista hipotético, que a atitude dos bancos eleva seu poder de monopólio e que os envolvidos, bancos e exchanges, disputam o mesmo mercado relevante.

1. INTRODUÇÃO

O setor bancário é altamente regulado no Brasil e bastante oligopolizado[110], contudo, isso não impediu o surgimento de empresas inovadoras no setor. Primeiro foram as fintechs[111] e depois as exchanges de criptomoedas. Enquanto as primeiras atuam no mercado regulado, as últimas estão completamente à margem da regulação, isso porque intermediam negociações com criptomoedas, as quais apenas são reconhecidas como ativos pela Receita Federal do Brasil para fins de tributação[112].

O objetivo deste trabalho consiste em analisar os aspectos do direito concorrencial aplicáveis ao processo administrativo em trâmite no CADE resultante da representação proposta pela Associação Brasileira de Criptomoedas e Blockchain contra o Banco do Brasil S.A pelo fechamento das contas correntes das exchanges.

---

110 A questão do oligopólio dos bancos brasileiros é comumente noticiada na mídia. A título de exemplo: http://g1.globo.com/economia/noticia/2015/08/concentracao-aumenta-e-5-bancos-ja-detem-mais-de-80-dos-ativos-no-pais.html Aceso em 16 jan. 2018

111 O Brasil possui centenas de fintechs proporcionando desde arranjos de pagamento até seguros. Três entre as cem fintechs mais inovadoras do mundo são brasileiras: https://www1.folha.uol.com.br/mercado/2018/10/brasil-tem-tres-das-cem-fintechs-mais-inovadoras-do-mundo-diz-relatorio.shtml

112 Valor Econômico. Receita define regra para taxação de IR sobre bitcoins. Disponível em: https://www.valor.com.br/financas/3507132/receita-define-regra-para-taxacao-de-ir-sobre-bitcoins Acesso em 05. ago. 2018.

2. BITCOIN E BLOCKCHAIN: A CRIPTOMOEDA PIONEIRA E SUA INOVAÇÃO

A internet desconhecia o conceito econômico de escassez até a criação do Bitcoin, dado que antes dele toda informação transmitida podia ser replicada infinitas vezes. Isso não ocorre com o Bitcoin, cuja tecnologia permite o envio do próprio ativo de uma chave para outra.

A tecnologia por trás do Bitcoin denomina-se *Blockchain* ou corrente de blocos. A *Blockchain* enquanto rede distribuída torna dispensável um terceiro de confiança para autenticar transações possuindo potencial para substituir entidades certificadoras e centralizadas de negócios[113], por essa razão é vista como um protocolo de confiança.

As transações de Bitcoin são inscritas num livro razão como um registro contábil (*ledger*) de dupla entrada. Os Bitcoins ou suas frações denominadas Satoshis que saem de uma carteira (wallet) ingressam em outra carteira, sendo essas carteiras identificadas no livro pelas chaves públicas dos usuários[114].

Cada um dos nós da rede B*lockchain* possui o *ledger* armazenado e é responsável por garantir sua integridade, sendo a criptografia e o consenso elementos chaves para a manutenção da autenticidade, integridade, consistência e disponibilidade do livro-razão[115].

Note-se que a *Blockchain* é instituída pelo consenso em rede acerca de cada operação realizada. Seus registros são públicos podendo ser consultados por qualquer pessoa a qualquer momento[116]. Contudo, não será possível identificar as pessoas que transacionaram, a menos que você saiba a chave da pessoa.

A *Blockchain* pioneira foi a do *Bitcoin*, mas atualmente existem muitas outras criptomoedas com suas redes próprias, tais como *Ethereum Classic*, *Ethereum, Bitcoin Cash, Litecoin*, para mencionar somente as mais conhecidas. Também já existem propostas de superação da tecnologia em razão dos seus limites de escalabilidade, a mais conhecida é a *Tangle* da moeda IOTA, criada para operacionalizar transações no universo da Internet das Coisas (*Internet of Things*).

---

113 GREVE, Fabíola; SAMPAIO, Leobino; ABIJAUDE, Jauberth; COUTINHO, Antonio; VALCY, Italo; QUEIROZ, Sílvio. **Blockchain e a Revolução do Consenso sob Demanda.** Disponível em: <http://portaldeconteudo.sbc.org.br/index.php/minicursossbrc> acesso em: 10.out. 2018.

114 ANTONOPOULOS, Andreas M. **Mastering Bitcoin.** Open Edition em Português do Brasil. FoxBit, p. 28.

115 GREVE, Fabíola; SAMPAIO, Leobino; ABIJAUDE, Jauberth; COUTINHO, Antonio; VALCY, Italo; QUEIROZ, Sílvio. **Blockchain e a Revolução do Consenso sob Demanda.** Disponível em: <http://portaldeconteudo.sbc.org.br/index.php/minicursossbrc> acesso em: 10.out. 2018.

116 As informações podem ser consultadas no site: <https://www.blockchain.com/pt/explorer>

3. CRIPTOMOEDAS COMO ATIVOS FINANCEIROS E AS EXCHANGES

O primeiro órgão brasileiro a se pronunciar sobre criptomoedas foi a Receita Federal, através de comunicado publicado em 2014, em que equiparou o Bitcoin e a Litecoin a ativos financeiros[117].

Assim, a renda obtida com a negociação de criptomoedas passou a ser de declaração obrigatória à Receita Federal, o que não surpreende, uma vez que nos termos do art. 118 do CTN a hipótese de incidência é interpretada abstraindo-se da validade jurídica dos atos efetivamente praticados e dos efeitos efetivamente verificados.

Como destacou a CVM, algumas *Initial Coin Offerings* (ICO's) destinam-se a captar recursos para investimento em empresas e projetos e assim assumem características de valores mobiliários. Nesse caso, a autarquia entende que estariam submetidas à regulação própria do mercado de capitais.

Entretanto, criptos como o *Bitcoin* cujo propósito é operar como meio de pagamento, sem destinação para financiamento de projetos ou empresas não estariam submetidas à CVM[118].. Essas seriam as criptomoedas ou *cryptocurrencies*, enquanto que os submetidos à CVM podem ser considerados como criptoativos ou *cryptoassets*.

A distinção é tecnicamente mais adequada aos conceitos econômicos uma vez que um ativo financeiro é definido como "um instrumento que canaliza a poupança até o investimento".[119]

A Receita Federal ao considerar as criptomoedas como ativos parece se aproximar do conceito contábil de ativo "compreendido como o somatório dos bens e direitos[120]" de uma pessoa jurídica ou física.

De uma perspectiva ampla, portanto, um ativo "é um título, uma reserva de valor que representa uma dívida ou uma propriedade[121]" entre os quais se enquadram imóveis, equipamentos, títulos, ações e quaisquer outros bens.

Na prática observa-se o surgimento e consolidação de um verdadeiro mercado em torno da negociação de criptomoedas com a participação de *exchanges* que nada mais são que agentes intermediários que se propõem a facilitar trocas entre diferentes criptos e por moeda *fiat*[122].

---

117 Valor Econômico. Receita define regra para taxação de IR sobre bitcoins. Disponível em: <https://www.valor.com.br/financas/3507132/receita-define-regra-para-taxacao-de-ir-sobre-bitcoins>. Acesso em 05. ago. 2018.

118 Sobre o Bitcoin, em específico, o STJ se posicionou afirmando que não se trata de moeda nem de valor mobiliário. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201802484304&dt_publicacao=05/12/2018> Acesso em: 18.dez.2018.

119 PINHEIRO, Juliano Lima. **Mercado de Capitais: fundamentos e técnicas**. São Paulo: Atlas, 2009, p. 102.

120 MONTOTO, Eugênio. **Contabilidade Esquematizado**. Organ. Pedro Lenza. São Paulo: Saraiva, 2011, p. 52.

121 MISHKIN, Frederic S. **Moedas, bancos e mercados financeiros**. 5ª ed. Trad. Chiristine Pinto Ferreira Studart. Rio de Janeiro: LTC Livros Técnicos, 2000, p.57.

122 Portal do Bitcoin. Brasil: **Muitas Exchanges de Criptomoedas e Pouco Volume de Bitcoin**. Disponível em <https://portaldobitcoin.com/brasil-vira-palco-de-enxurrada-de-novas-exchanges-de-criptomoedas-apesar-de-baixo-volume-de-bitcoin/> Acesso em 05. Ago. 2018.

As *exchanges* funcionam como bolsas de valores em que as pessoas negociam diretamente suas criptomoedas segundo um índice interno de preços estabelecido pelas negociações realizadas, mas também oferecem outros serviços, atuando em muitos casos como verdadeiros agentes de custódia.

Existe, portanto, cotação para criptomoedas com a diferença de que todo o ecossistema está funcionando na base da autorregulação, diante da ausência de normas específicas no Brasil.

Para se ter uma dimensão desse mercado, uma única exchange chega a movimentar num único dia mais de 400 mil reais. O volume transacionado pode ser verificado em tempo real através dos sites: Bitvalor[123] ou Icoinomia[124].

Em dezembro de 2018, o volume de transações das exchanges foi alvo de polêmica, sendo que várias delas são acusadas de manipularem seus valores. Um relatório elaborado pelo Blockchain Transparency Institute apontou que das 25 maiores exchanges do mundo apenas três não manipulavam os volumes de transação[125].

---

123 Bitvalor: https://bitvalor.com

124 Icoinomia: https://icoinomia.com.br

125 A íntegra do relatório pode ser conferida no endereço: https://www.blockchaintransparency.org Acesso em 10 jan.2019.

4. CONFLITO ENTRE AGENTES DO MERCADO REGULADO E DO NÃO REGULADO E APLICAÇÃO DA LEGISLAÇÃO ANTITRUSTE

É inegável que existe um mercado de negociação de criptoativos no qual as exchanges concentram parcela significativa das transações. Considerando o volume de movimentação financeira necessário a tanto, é inevitável que tais valores circulem pelo setor bancário, dando ensejo a conflitos entre um setor fortemente regulado e outro à margem da regulação.

É importante esclarecer que o Sistema Financeiro Nacional (SFN) é dividido em três grandes grupos: 1) seguros privados cujo órgão normativo é o Conselho Nacional de Seguros Privados e o órgão supervisor é a Superintendência de Seguros Privados (Susep); 2) previdência fechada cujo órgão normativo é o Conselho Nacional de Previdência Complementar e o Órgão Supervisor é a Superintendência Nacional de Previdência Complementar; e 3) moeda, crédito, capitais e câmbio cujo órgão normativo é o Conselho Monetário Nacional e os órgãos supervisores são o Banco Central do Brasil e a Comissão de Valores Mobiliários.

Este último grupo compõe o Sistema de Pagamentos Brasileiros (SPB) que compreende, nos termos do art. 2º da Lei 10.214/2001, "as entidades, os sistemas e os procedimentos relacionados com a transferência de fundos e de outros ativos financeiros, ou com o processamento, a compensação e a liquidação de pagamentos em qualquer de suas formas".

O parágrafo único do art. 2º enumera quais tipos de operações estariam albergadas pelo SPB: a) serviço de compensação de cheques e outros papéis; b) serviços de compensação e liquidação de ordens eletrônicas de débito e de crédito; c) serviços de transferência de fundos e de outros ativos financeiros; d) serviços de compensação e de liquidação de operações com títulos e valores mobiliários; e) serviços de compensação e de liquidação de operações realizadas em bolsas de mercadorias e de futuros; f) outros, incluindo as operações com derivativos financeiros, cujas câmaras ou prestadores de serviços tenham sido autorizados na forma da lei.

É importante frisar que para compor o SPB é exigida autorização pelo Banco Central do Brasil ou pela Comissão de Valores Mobiliários, em suas respectivas áreas de competência. Trata-se de mercado profundamente regulado no Brasil, sujeito à prestação de informações não apenas ao Bacen e CVM como também à Receita Federal do Brasil para combater os crimes de evasão de divisas e lavagem de dinheiro.

Ocorre que as exchanges de criptomoedas utilizam o Sistema de Pagamentos Brasileiro para movimentar quantidades expressivas de dinheiro, sem, contudo, estarem sujeitas à fiscalização dos órgãos supervisores e à regulação do setor do setor bancário.

É importante recordar que tanto a regulação quanto o antitruste surgem, à grosso modo, para responder às falhas de mercado. Contudo, conforme leciona o professor Alexandre Faraco, a regulação é aplicável a determinado setor da economia e consiste numa atuação estatal que restringe a liberdade dos agentes econômicos quanto a certas variáveis como preço, quantidade, diferenciação e investimento[126]. Já o direito concorrencial é aplicável a todos os setores da economia quando constatado o abuso ou a concentração de poder econômico[127].

---

126 FARACO, Alexandre Dietzel. **Aplicação das Normas Gerais de Concorrência nos Setores Regulados.** Disponível em: <https://www.levysalomao.com.br/files/publicacao/anexo/20120614160300_aplicacao-das-normas-gerais-de-concorrencia-nos-setores-regulados.pdf> Acesso em: 19. Nov. 2018.

127 Idem.

O caso em análise é especialmente interessante porque se tem agentes não regulados (exchanges de criptomoedas) em conflito com agentes regulados (bancos). E, são justamente os primeiros que invocam ao CADE seja aplicada, face aos últimos, a legislação antitruste.

5. A REPRESENTAÇÃO NO CADE

Os valores movimentados pelas exchanges são expressivos, conforme mencionado anteriormente, contudo, à exceção dos valores atinentes ao preço do serviço de intermediação, o dinheiro movimentado não pertence às exchanges mas sim aos clientes delas.

Alguns bancos começaram a encerrar as contas das exchanges alegando "falta de interesse comercial" em manter o serviço para esses clientes. É digno de nota que antes de a questão ser submetida ao CADE, foi levada ao Poder Judiciário chegando até o Superior Tribunal de Justiça em dezembro de 2017.

Em sede de recurso especial a Mercado Bitcoin Serviços Digitais LTDA invocou o Código de Defesa do Consumidor (CDC) para que o Banco Itaú Unibanco S/A fosse obrigado a manter ativa a conta corrente de titularidade da exchange. O STJ entendeu que a utilização de serviços bancários pela recorrente tinha o propósito de incrementar sua atividade produtiva de intermediação e afastou a aplicação do CDC.

Na decisão datada de 09/10/2018 o STJ considerou legítimo o encerramento da conta, tanto por iniciativa do banco quanto por iniciativa do correntista, desde que previamente notificada a outra parte contratante[128].

Antes mesmo que o STJ julgasse a matéria, mais precisamente em 01/06/2018, a Associação Brasileira De Criptomoedas e Blockchain (ABCB) ingressou com representação junto ao CADE contra o Banco do Brasil do S/A por recusa de contratar e negativa de acesso a infraestrutura essencial[129].

Nos termos da representação, o Banco do Brasil comunicou a Atlas, sócia mantenedora da ABCB do encerramento de sua conta corrente. A reclamante afirma não se tratar de caso isolado e que a prática vem sendo adotada por outros bancos.

A ABCB argumenta que as empresas inovadoras da economia digital são, por um lado, clientes dos bancos, dado que necessitam acesso ao sistema financeiro para negociar, por outro lado são concorrentes deles ao oferecerem produtos e serviços financeiros e meios de pagamento alternativos.

Ainda segundo a representação, essas empresas competem com os bancos tanto pelo lado da oferta (bancos e demais instituições financeiras), quanto pelo lado da demanda (investidores, credores/pagadores etc.).

Além do pedido de condenação do Banco do Brasil por prática de conduta anticompetitiva, a ABCB solicitou que seja determinado pelo CADE que os bancos e demais instituições financeiras se abstenham de encerrar as contas bancárias das operadoras de criptomoedas (corretoras, exchanges, fintechs etc.).

Embasando-se nas informações prestadas na representação e documentos juntados, o Coordenador(a)-Geral do CADE, Sr. Marcelo Nunes de Oliveira, determinou a instauração de

---

128 BRASIL. STJ. Resp. nº 1.696.214/ SP. Rel. Min. Marco Aurélio Bellizze. Julg. 09/10/2018. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1735391&num_registro=201702244334&data=20181016&formato=PDF> Acesso em: 16 dez.2018.

129 BRASIL. CADE. Processo Administrativo nº 08700.003599/2018-95. Disponível em: <https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?0c62g277GvPsZDAxAO1tMiVcL9FcFMR5UuJ6rLqPEJuTUu08mg6wxLt0JzWxCor9mNcMYP8UAjTVP9dxRfPBcSmM4M2ETTN1Mv7wWLGnEUiWmCLsr9jExmU5t47oOILQ> Acesso em: 08.nov.2018.

procedimento preparatório de inquérito administrativo em desfavor de: Banco do Brasil S.A., Banco Bradesco S.A., Banco Itaú S.A., Banco Santander S.A., Banco Inter S.A. E Banco Sicredi.

O Banco Itaú Unibanco S/A em sua manifestação alegou que os bancos são responsáveis por monitorar seus clientes de modo a identificar operações incompatíveis com sua atividade econômica. Isto é, ao notarem atividades suspeitas, que possam configurar lavagem de dinheiro e/ou financiamento ao terrorismo, as instituições devem comunicá-las ao Conselho de Controle de Atividades Financeiras (COAF). Trata-se de obrigação imposta nos termos da Lei 9.613/98, alterada pela Lei 12.683/12, e da Circular 3.461/09, alterada pela Circular 3.839/17, e Carta-Circular 3.542/12, as últimas do Banco Central do Brasil.

Segundo o Itaú Unibanco, os clientes que atuam com corretagem de criptomoedas e atividades equivalentes geralmente têm movimentações financeiras em alto volume, incompatíveis com as informações apresentadas ao banco. O banco ressalva que a atividade de corretagem de criptomoedas não é regulada, mas tampouco é ilícita. Contudo, as instituições financeiras, em decorrência do setor sensível em que atuam, não estão autorizadas a dispensar as medidas e procedimentos de *due diligence* com relação aos seus clientes.

Todos os demais bancos que já se pronunciaram no processo alegaram a mesma preocupação com implicações atinentes às normas de combate aos crimes de lavagem de dinheiro e terrorismo.

O Sicredi acrescentou ainda a dificuldade em identificar esses clientes uma vez que a atividade corretagem de criptomoedas não possui CNAE (Cadastro Nacional de Atividade Econômica) específico.

6. DIREITO CONCORRENCIAL APLICADO AO CASO

O direito concorrencial segundo o professor Calixto Salomão Filho tem por objetivo tutelar os interesses dos consumidores e dos participantes do mercado e o interesse institucional da ordem concorrencial[130].

O interesse institucional defendido por Salomão Filho tem titularidade difusa, isto é, pertence a uma coletividade indeterminada e é jurídica e economicamente diferente do interesse individual. Juridicamente porque existem instrumentos legais distintos daqueles destinados à tutela individual para sua proteção e economicamente porque encerra uma utilidade para a coletividade que não se limita a utilidade individual[131].

O Conselho Administrativo de Defesa Econômica (CADE) é o órgão responsável por proteger esse interesse institucional da ordem concorrencial, o que indiretamente pode resultar em um benefício aos consumidores e aos participantes do mercado.

Na representação da ABCB os bancos são acusados de violar a ordem concorrencial recusando-se a contratar com as exchanges e negando-lhes acesso à infraestrutura essencial. Tais condutas podem, em tese, caracterizar o uso abusivo da posição dominante do mercado prevista no art. 36, VI, da Lei 12.529/2011.

Embora as condutas não estejam elencadas com essas exatas palavras no art. 36, §3º, da Lei 12.529/2011 se assemelham às práticas dos incisos III, IV, V, XI e XII que, respectivamente, consistem em: limitar ou impedir o acesso de novas empresas ao mercado; criar dificuldades à constituição, ao funcionamento ou ao desenvolvimento de empresa concorrente ou de fornecedor, adquirente ou financiador de bens ou serviços; impedir o acesso de concorrente às fontes de insumo, matérias-primas, equipamentos ou tecnologia, bem como aos canais de distribuição; recusar a venda de bens ou a prestação de serviços, dentro das condições de pagamento normais aos usos e costumes comerciais; dificultar ou romper a continuidade ou desenvolvimento de relações comerciais de prazo indeterminado em razão de recusa da outra parte em submeter-se a cláusulas e condições comerciais injustificáveis ou anticoncorrenciais.

É importante que se diga que o rol do art. 36, §3º, da Lei 12.529/2011 não é taxativo, mas sim exemplificativo[132], contudo somente a prática da conduta não é suficiente para ensejar a aplicação das penalidades do direito concorrencial. Isso porque é necessário que a conduta tenha resultado

---

130 SALOMÃO FILHO, Calixto. **Direito Concorrencial: As condutas**. São Paulo: Malheiros Editores LTDA, 2003, p. 61.

131 Ibidem p. 70.

132 Há quem defenda a taxatividade da lista em razão das consequências penais, entre eles FRANCESCHINI, José Inácio. Introdução ao direito da concorrência. São Paulo: Malheiros, 1995, p.47; STEVENS, Dallal. Framing competition law within an emerging economy: the case of Brazil. Antitrust Bulletin, v. 40, 1995, p. 112; LEÃES, Luiz Gastão Paes de Barros. O dumping como forma de abuso do poder econômico. Revista de Direito Mercantil, v. 91, n. 5, 1993, p. 9, *apud* MACEDO, Alexandre Cordeiro.Restrições Verticais no Direito Antitruste Brasileiro à Luz da Análise Econômica do Direito. Disponível em: http://dspace.idp.edu.br:8080/xmlui/bitstream/handle/123456789/1674/Dissertação_Alexandre%20Cordeiro%20Macedo.pdf?sequence=1&isAllowed=y Acesso em 09. Jan. 2019.

em um dano a concorrência[133], que tenha tido um dos efeitos do art. 36, incisos I a IV, no caso em análise, esse último em especial.

A primeira questão que se apresenta, portanto, diz respeito aos efeitos na concorrência da conduta praticada pelos bancos: ao se recusarem a contratar com as exchanges, os bancos elevam seu poder de monopólio? E mais: bancos e exchanges disputam o mesmo mercado relevante, qual mercado seria esse?

Se as exchanges fossem fintechs como a Nubank seria evidente afirmar que bancos e fintechs disputam o mesmo mercado relevante. Mas em se tratando das exchanges de criptomoedas é interessante recordar que os bancos não trabalham com este produto ainda à margem de regulação.

A circulação das moedas virtuais independe dos bancos e desconhece fronteiras entre os países, ao contrário da moeda fiduciária que se submete ao regime de câmbio supervisionado pelos Bancos Centrais. Parte desses argumentos foram considerados pelo STJ no julgamento do Recurso Especial proposto pela Mercado Bitcoin contra o Itaú Unibanco, ponderando o Ministro relator Marco Aurélio Bellizze:

> O registro é relevante para evidenciar que o serviço bancário afigura-se importante no desenvolvimento da atividade de intermediação desempenhada pela recorrente, conforme ela própria consigna, mas sem repercussão alguma na circulação e na utilização dessas moedas virtuais, as quais, até o presente momento, não contam com nenhuma regulamentação pelo Conselho Monetário Nacional (em tese, porque não possuiriam vinculação com os valores mobiliários, cuja disciplina é dada pela Lei n. 6.385/1976).
>
> [...]
>
> A partir de tais considerações, ressai evidenciado, portanto, que o serviço bancário de conta-corrente oferecido pelas instituições financeiras em nada repercute na circulação ou na utilização das moedas virtuais, que, como visto, não dependem de intermediários, possibilitando a operação comercial e/ou financeira direta entre o transmissor e o receptor da moeda digital[134].

As exchanges necessitam do serviço bancário apenas quando o cliente delas solicita a conversão de suas criptomoedas em moeda fiduciária. Então parte da atividade desempenhada por elas não compõe o mercado de atuação dos bancos e instituições financeiras tradicionais.

Recorde-se que o mercado relevante é definido pela perspectiva do consumidor, de maneira que se ficar constatado que o consumidor pode substituir um produto ou serviço por outro igual ou semelhante, ambos os agentes pertencem ao mesmo mercado relevante material[135]. Dito de outro modo:

---

133 SILVA, Cleanto Fortunato. Restrições verticais no direito antitruste brasileiro. Disponível em: http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=17549 Acesso em 09 jan. 2019.

134 BRASIL. STJ. Resp. nº 1.696.214/ SP. Rel. Min. Marco Aurélio Bellizze. Julg. 09/10/2018. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1735391&num_registro=201702244334&data=20181016&formato=PDF> Acesso em: 16 dez.2018.

135 FURTADO, Rogério Dourado. Mercado Relevante no Direito da Concorrência. Disponível em: http://www.ambito-

> Na definição do mercado relevante antitruste, limita-se o conjunto de empresas que geram forças competitivas frente a aumentos de preços pelas empresas em foco, ou seja, aquelas que participaram de um ato de concentração ou processo administrativo. Este mercado relevante apresenta dimensões de produto e espaço[136].

Para definição do mercado relevante é o utilizado o teste do monopolista hipotético[137] explicado por Roberto Domingos Taufick da seguinte forma:

> Segundo esse teste, toma-se o produto, ou o serviço chave (cada produto do portfólio dos produtos, ou cada serviço do portfólio dos serviços do grupo adquirido) e faz-se uma análise dos comportamento dos consumidores ante um aumento de até 5% do seu preço (este teste é chamado teste SSNIP, que pode ser traduzido do inglês como um pequeno, mas significativo e não transitório aumento de preços). Caso o consumidor migre para outro produto, esse outro produto será incluído no mercado relevante e refaz-se o teste, desta vez com esse novo produto. O teste é repetido até que não haja mais migrações. O conjunto de alternativas identificado pela aplicação do teste SSNIP é o mercado relevante sob o viés do produto[138].

Considerando-se que no Brasil as criptomoedas não são reconhecidas como meio de pagamento o que impede que o consumidor permute o serviço bancário tradicional pelo serviço de uma exchange para atos do cotidiano. Nessa perspectiva, é possível que da aplicação do teste do monopolista hipotético se compreenda que os agentes não estão em disputa pelo mesmo mercado relevante.

De outro vértice, permitir que os bancos encerrem as contas das exchanges pode levar à extinção de várias dessas empresas, inviabilizando uma atividade econômica que diversifica o mercado de serviços financeiros que é bastante concentrado no Brasil.

---

juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10345&revista_caderno=8. Acesso em: 16.dez.2018.

136 Departamento de Estudos Econômicos. **Delimitação de mercado relevante.** Brasília, 2010. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/dee-publicacoes-anexos/delimitacao_de_mercado_relevante.pdf Acesso em: 14. jan.2019.

137 Departamento de Estudos Econômicos. **Delimitação de mercado relevante.** Brasilía, 2010. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/dee-publicacoes-anexos/delimitacao_de_mercado_relevante.pdf Acesso em: 14. jan.2019.

138 TAUFICK, Roberto Domingos. **Introdução ao Direito da Concorrência**. Brasília, 2014. Disponível em:http://www.fazenda.gov.br/centrais-de-conteudos/publicacoes/apostilas/advocacia-da-concorrencia/4-seae_introducao_direito_concorrencia.pdf. Acesso em 16 dez. 2018.

7. CONCLUSÃO

O caso em análise é especialmente interessante porque está na intersecção de agentes regulados (bancos) e não regulados (exchanges de criptomoedas), sendo que a circulação das criptomoedas não se submete ao controle dos Bancos Centrais, tampouco reconhece as fronteiras nacionais.

Contudo, há momentos em que os titulares desses criptoativos precisam convertê-los em moeda *fiat* e para isso podem utilizar o serviço de uma exchange de criptomoedas. Ocorre que o volume de movimentação bancária das exchanges de criptomoedas foi visto com desconfiança pelos bancos que começaram a encerrar as contas das exchanges.

Por um lado, a própria ausência de regulação para as atividades atinentes às criptomoedas impede que os serviços bancários comuns sejam completamente intercambiáveis por serviços em criptoativos pelos consumidores.

Dadas as peculiaridades do caso, é possível que aplicação do teste do monopolista hipotético resulte na ausência de disputa por mercado relevante entre os agentes, porém, se todos os bancos encerrarem as contas das exchanges a atividade será inviabilizada ou então reduzida a poucos players que possam ter participação em bancos tradicionais.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ANTONOPOULOS, Andreas M. Mastering Bitcoin. Open Edition em Português do Brasil. FoxBit, p. 28.

BRASIL. CADE. Processo Administrativo nº 08700.003599/2018-95. Disponível em: <https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?0c62g277GvPsZDAxAO1tMiVcL9FcFMR5UuJ6rLqPEJuTUu08mg6wxLt0JzWxCor9mNcMYP8UAjTVP9dxRfPBcSmM4M2ETTN1Mv7wWLGnEUiWmCLsr9jExmU5t47oOILQ> Acesso em: 08.nov.2018.

BRASIL. STJ. 161.123 - SP. Ministro Sebastião Reis Júnior. Julg. 28.nov. 2018. https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201802484304&dt_publicacao=05/12/2018> Acesso em: 12 jan. 2019

BRASIL. STJ. Resp. nº 1.696.214/ SP. Rel. Min. Marco Aurélio Bellizze. Julg. 09/10/2018. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1735391&num_registro=201702244334&data=20181016&formato=PDF> Acesso em 12.jan. 2019.

CORDEIRO, Margarida Robalo. A recusa de contratar no direito da concorrência. Lisboa, 2015. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/18076/1/A%20Recusa%20de%20Contratar%20no%20Direito%20da%20Concorrência%20-%20Dissertação%20de%20Mestrado%20_%20Margarida%20Robalo%20Cordeiro.pdf Acesso em 16 dez. 2018.

Departamento de Estudos Econômicos. Delimitação de mercado relevante. Brasilía, 2010. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/dee-publicacoes-anexos/delimitacao_de_mercado_relevante.pdf Acesso em: 14. jan.2019.

FURTADO, Rogério Dourado. Mercado Relevante no Direito da Concorrência. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10345&revista_caderno=8. Acesso em: 16.dez.2018.

GREVE, Fabíola; SAMPAIO, Leobino; ABIJAUDE, Jauberth; COUTINHO, Antonio; VALCY, Italo; QUEIROZ, Sílvio. Blockchain e a Revolução do Consenso sob Demanda. Disponível em: <http://portaldeconteudo.sbc.org.br/index.php/minicursossbrc> acesso em: 10.out. 2018.

FARACO, Alexandre Dietzel. Aplicação das Normas Gerais de Concorrência nos Setores Regulados. Disponível em: <https://www.levysalomao.com.br/files/publicacao/anexo/20120614160300_aplicacao-das-normas-gerais-de-concorrencia-nos-setores-regulados.pdf> Acesso em: 19. Nov. 2018.

MACEDO, Alexandre Cordeiro.Restrições Verticais no Direito Antitruste Brasileiro à Luz da Análise Econômica do Direito. Disponível em: http://dspace.idp.edu.br:8080/xmlui/bitstream/handle/123456789/1674/Dissertação_Alexandre%20Cordeiro%20Macedo.pdf?sequence=1&isAllowed=y Acesso em 09. Jan. 2019.

MARTINS, Catarina. A problemática do acesso à infraestrutura essencial no contexto do direito da concorrência. Porto, 2015. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/18916/1/A%20problemática%20do%20acesso%20à%20infra%20estrutura%20esssencial%20no%20contexto%20do%20direito%20da%20concorrencia%20.pdf Acesso em 16. Dez. 2018.

MISHKIN, Frederic S. Moedas, bancos e mercados financeiros. 5ª ed. Trad. Chiristine Pinto Ferreira Studart. Rio de Janeiro: LTC Livros Técnicos, 2000, p.57.

MONTOTO, Eugênio. Contabilidade Esquematizado. Organ. Pedro Lenza. São Paulo: Saraiva, 2011, p. 52.

PINHEIRO, Juliano Lima. Mercado de Capitais: fundamentos e técnicas. São Paulo: Atlas, 2009, p. 102.

PORTAL DO BITCOIN. Brasil: Muitas Exchanges de Criptomoedas e Pouco Volume de Bitcoin. Disponível em <https://portaldobitcoin.com/brasil-vira-palco-de-enxurrada-de-novas-exchanges-de-criptomoedas-apesar-de-baixo-volume-de-bitcoin/> Acesso em 05. Ago. 2018.

RIBEIRO, Eduardo Pontual; JACINTO, Paulo de Andrade. Delimitação de Mercado Relevantes para produtos Diferenciados Usando Elasticidades: O caso do chá pronto para beber. Disponível em: http://www.anpec.org.br/revista/vol11/vol11n4p267_284.pdf Acesso em 18. Dez. 2018.

SALOMÃO FILHO, Calixto. Direito Concorrencial: As condutas. São Paulo: Malheiros Editores LTDA, 2003.

TAUFICK, Roberto Domingos. Introdução ao Direito da Concorrência. Brasília, 2014. Disponível em:http://www.fazenda.gov.br/centrais-de-conteudos/publicacoes/apostilas/advocacia-da-concorrencia/4-seae_introducao_direito_concorrencia.pdf. Acesso em 16 dez. 2018.

SANTOS, Samuel Fernando Hübler. Análise do mercado relevante dos cartões de pagamento. Disponível em: http://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/download/48/11. Acesso em 19 jan. 2019.

SILVA, Cleanto Fortunato. Restrições verticais no direito antitruste brasileiro. Disponível em: http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=17549 Acesso em 09 jan. 2019.

VALOR ECONÔMICO. Receita define regra para taxação de IR sobre bitcoins. Disponível em: https://www.valor.com.br/financas/3507132/receita-define-regra-para-taxacao-de-ir-sobre-bitcoins Acesso em 05. ago. 2018.

SOBRE A CONSULTA PÚBLICA Nº 06/2018, DA RECEITA FEDERAL DO BRASIL E SEUS PONTOS POLÊMICOS.

Dayana de Carvalho Uhdre

Procuradora do Estado do Paraná. Graduada em Direito pela Universidade Federal do Paraná - UFPR. Pós-Graduada pelo Instituto Brasileiro de Estudos Tributários - IBET. Mestre em Direito do Estado pela Universidade Federal do Paraná - UFPR. Professora de Direito Tributário da FAPI - Faculdade de Direito de Pinhais. Professora convidada no curso de Pós-Graduação em Direito Tributário da Academia de Direito Constitucional - Abdconst. Professora seminarista no Instituto Brasileiro de Estudos Tributários - IBET. Membro da Comissão de Inovação e Gestão da OAB-PR. Coordenadora do Grupo de Discussão Permanente de Criptoativos da OAB-PR.

RESUMO:
Receita Federal do Brasil realizara consulta pública relativamente a proposta de Instrução Normativa em que se exigia a prestação de informações, por parte das exchanges nacionais e/ou pessoas envolvidas**,** de todas as operações realizadas com criptoativos. E, tal exigência é fulcrada em disposições normativas regentes das obrigações acessórias. No entanto, apesar de louvável a postura da Receita Federal do Brasil em capitanear as discussões relativas ao mercado de criptoativos, notadamente na parte importantíssima que lhe cabe (tributação), não pode, obviamente, fazê-lo para além do seu âmbito de competência. O objetivo do presente artigo é realizar uma análise mais cuidadosa da proposta apresentada, a fim de verificar se a Receita exorbitara, ou não, os limites de sua competência, ao implementar tal “obrigação acessória”.

ABSTRACT:
Federal Revenue Service of Brazil made public consultation regarding the proposal for a Normative Ruling requiring informations about all operations with cryptoactives. And this requirement is fulfilled in normative provisions governing ancillary obligations. despite the praiseworthy position assumed by the Federal Revenue Service of Brazil in leading discussions regarding the cryptoactive market, especially in the most important part of it (taxation), it can not obviously do so beyond its boundaries of competence. The purpose of this article is to do a more careful analysis of the proposal presented, in order to verify whether or not the Revenue exorbit the limits of its competence, when implementing such an "accessory obligation".

1. INTRODUÇÃO

Em final de outubro do corrente ano, a Receita Federal do Brasil Receita abriu consulta pública (de nº 06/2018) relativamente a proposta de Instrução Normativa envolvendo operações com criptoativos. Mais especificamente, objetiva-se sejam fornecidas informações, ao Fisco Federal, relativamente a toda e qualquer operação com criptoativos realizada por exchange domiciliada no Brasil, e/ou operações com criptoativos, que ultrapassem em um mês, R$ 10.000,00 (dez mil reais), realizadas diretamente entre os particulares (P2P), ou em exchange internacional[139].

Consta na exposição de motivos, que tal medida justifica-se, dentre outras razões, pelo expressivo aumento de valores negociados em referido mercado - de R$363.200.000,00, em 2016, para R$8.300.000.000,00, em 2017, com previsão de atingir 45 bilhões de reais em 2018 –, pelo aumento do número de pessoas nele envolvidas, e pela existência de ações semelhante por parte de outros países[140].

Por fim, fundamenta-se a instrução normativa em disposições normativas regentes das obrigações acessórias (art. 113 do CTN[141], art.16 da Lei 9.779/99, art. 57 da MP 2.158-35/2001, e art. 327, III do Regimento Interno da Secretaria da Receita Federal do Brasil).

No entanto, em que pese ser louvável a postura da Receita Federal do Brasil em buscar capitanear as discussões relativas ao mercado de criptoativos, notadamente na parte importantíssima que lhe cabe (tributação), não pode, obviamente, fazê-lo para além do seu âmbito de competência. E, uma análise mais cuidadosa da proposta apresentada demonstra que não só a Receita parece ter exorbitado os limites de sua competência, como intenta implementar "obrigação acessória" em todo custosa aos empreendedores desse mercado nascente. Esclareça-se, desde já, que o nosso foco principal será o impacto da proposta nas exchanges nacionais.

---

139 Art. 5º Está obrigada à entrega das informações:

I - a exchange de criptoativos domiciliada para fins tributários no Brasil;

II - a pessoa física ou jurídica residente ou domiciliada no Brasil quando :as operações forem realizadas em exchanges domiciliadas no exterior; ou as operações não forem realizadas em exchange.

Parágrafo único. Na hipótese prevista no inciso II do caput, as informações deverão ser prestadas sempreque o valor mensal das operações, isolado ou conjuntamente, ultrapassar R$ 10.000,00 (dez mil reais).

140 Citam-se os casos da Austrália, Coreia do Sul, da União Européia, e dos Estados Unidos.

141 Decreto-Lei 5.172, de 25 de outubro de 1966.

2. E, PODERIA A RECEITA FAZER O QUE FEZ?

2.1 UM RETORNO AO CONCEITO DE "OBRIGAÇÕES ACESSÓRIAS" E SEUS LIMITES

Destaque-se que o fundamento jurídico da proposta de instrução normativa, feita pela Receita Federal, seria a instauração de "obrigações acessórias" relativas ao pagamento do imposto de renda[142]. No entanto, análise mais cuidadosa do referido instrumento normativo (ou proposta de), nos demonstra que não é bem assim.

Obrigações acessórias seriam, consoante o art. 113 §2º do CTN, "prestações, positivas ou negativas, decorrentes da legislação tributária, e previstas no interesse da arrecadação ou fiscalização". PAULO DE BARROS CARVALHO esclarece tratar-se de "relações que prescrevem comportamentos outros, positivos ou negativos, consistentes num fazer ou não-fazer, os quais estão pré-ordenados a tornar possível a apuração, o conhecimento, o controle e a arrecadação dos valores devidos à título de tributo"[143]. Destaque-se que referido autor prefere utilizar a locução "deveres instrumentais[144]", haja vista inexistir verdadeira relação de acessoriedade entre a obrigação principal (de pagamento do tributo) e a instrumental: a existência dessa independe daquela. Destarte, lembremos que mesmo as entidades imunes (em relação as quais inexiste obrigações tributárias), devem observar os deveres instrumentais.

Pois bem, obrigações acessórias ou deveres instrumentais consistem em obrigações de fazer, ou de tolerar, que objetivam a verificação e comprovação da ocorrência dos eventos previstos nas hipóteses de incidência tributárias. Daí porque, consoante bem lembrado por ROQUE ANTONIO CARRAZZA, deve existir um liame, conexão entre a obrigação acessória, exigida do contribuinte (ou responsável) e a obrigação principal que se pretende ver verificada. Salienta o autor que uma racional interpretação do art. 113, § 2º do CTN "facilmente nos revela que a pessoa política só pode criar obrigações acessórias pertinentes, isto é, que se ajustem aos tributos compreendidos em seu campo tributável"[145].

Trata-se do que identificamos como "dever de cooperação" para com a Administração Pública. É dizer, o dever de fiscalizar e formalizar o débito tributário é do ente fazendário, precipuamente, porém, em razão do princípio da solidariedade conexo ao dever fundamental de pagar tributos, ambos ínsitos a um Estado Democrático de Direito, compete aos administrados cooperarem[146] a

142 Recordemos a manifestação da Receita Federal, na parte de dúvidas e respostas de sua página eletrônica, em que se esclarece a necessidade de se declarar a propriedade de criptomoedas, bem como a sujeição das operações com ela realizada estarem sujeitas a sujeição do imposto de renda (pelo ganho de capital). Disponível na URL: <http://idg.receita.fazenda.gov.br/interface/cidadao/irpf/2017/perguntao/pir-pf-2017-perguntas-e-respostas-versao-1-1-03032017.pdf>

143 CARVALHO, Paulo de Barros. Direito Tributário, Linguagem e Método. 4ª ed. rev e ampl. São Paulo: Noeses, 2011, p. 502.

144 Utilizar-se-á as expressões "deveres instrumentais" e "obrigações acessórias" como sinônimas.

145 CARRAZZA, Roque Antonio. Reflexões sobre a obrigação tributária. São Paulo: Noeses, 2010, p. 212.

146 Sobre o assunto, LEANDRO PAULSEN salienta que "as obrigações tributárias não se limitam à contribuição de cada um conforme a sua capacidade contributiva. Envolvem, também, a colaboração das pessoas em um sentido mais amplo de cooperação, ajuda, auxílio, requerendo que concorram para a efetividade da tributação. Faz-se necessário, enfim, que as pessoas coordenem esforços, participando conforme as suas possibilidades paa que a tributação ocorra e cumpra sua finalidade". E, prossegue esclarecendo que "Não apenas o dever de pagar tributos, mas também toda a ampla variedade de outras obrigações e deveres estabelecidos em favor da Administração

fim de que os valores tributários devidos sejam vertidos aos cofres públicos. Dito de outra forma, identificadas situações em que os administrados, em suas relações socioeconômicas, detém posições de poder tais aptas a auxiliarem o Estado no dever de recolher tributos (seja porque são as fontes pagadoras, ou os responsáveis por registrarem informações dos fluxos de propriedade, por exemplo), em razão do princípio da solidariedade, é legítimo que se lhes imponha o dever de cooperarem com a Administração Fazendária.

Ocorre que tais deveres de cooperação redundam em custos de conformidade, despesas em que incorrem os administrados a fim de cumprir para com a obrigação acessória. Daí a necessidade de que a imposição de tais deveres observe os princípios da proporcionalidade e razoabilidade, bem como o limite imposto pela vedação de se tributar com efeitos confiscatórios[147]. É dizer, a atribuição de obrigações acessórias aos administrados não pode ser tão onerosa a ponto de dificultar, além do razoável, as atividades empresariais. Afinal, a Carta Política prevê sejam garantidas a liberdade de iniciativa econômica, a livre concorrência, o tratamento favorecido das micro e pequenas empresas, e assim por diante.

Em suma, pertinência, razoabilidade e proporcionalidade: eis os limites[148] a que sujeita a Administração Fiscal na imposição dos deveres instrumentais. Assim, para além de razoáveis, eventuais obrigações acessórias a serem exigidas das exchanges e/ou usuários das redes de criptoativos devem estar relacionadas a comprovação de que operações com referidos criptoativos subsomem-se a hipótese de incidência do imposto de renda, sob o ganho de capital. É dizer, os deveres impostos pela autoridade fiscal só serão legítimos se conexos à obrigação principal, isto é, se ao entorno dela gravitarem, e não demandarem custos de conformidade tais a prejudicarem, de forma significativa, a própria atividade econômica das "exchanges".

No entanto, a proposta de instrução normativa, objeto da consulta pública nº 06/2018, não parece observar tais limitações. Afinal, todas as operações realizadas[149], seja nas exchanges nacionais ou internacionais, seja na modalidade P2P, bem como as pessoas que as fizeram, deverão ser relatadas à Receita Federal.

Ademais, não há como se desconsiderar os próprios custo de conformidade impostos às exchanges. Faz-se necessária, dentre outras providências, a contratação de mão-de-obra especializada (ou de mais horas de seus profissionais) a fim de se adaptar suas plataformas tecnológicas ao layout exigido pela RFB. Estima, o Grupo Bitcoin Banco[150], que terá um custo de ao menos R$ 50.000,00

Tributária para viabilizar e otimizar o exercício da tributação, encontram base e legitimação constitucional. O chamamento de todos, mesmo não contribuintes, ao c**umprimento de obrigações com vistas a viabilizar, a facilitar, a simplificar a tributação, dotando-lhe da praticabilidade necessária, encontra suporte no dever fundamental de colaboração com a Administração Tributária**" (Grifou-se). PAULSEN, Leandro. Capacidade Colaborativa. Princípio de Direito Tributário para obrigações acessórias e de terceiros. Porto Alegre: Livraria do Advogado Editora, 2014, p. 28-31.

147 CARRAZZA, Roque Antônio. Op. Cit., p. 215-216.

148 Discute-se, ainda, a imprescindibilidade de que tais obrigações acessórias venham veiculadas por meio de lei em sentido estrito. É que de um lado, o artigo 113 do CTN refere-se ao erigimento de deveres instrumentais por "legislação tributária", termo que engloba os atos infralegais (decretos, portarias, instruções normativas, etc). Por outro, há quem entenda ser necessária que tais deveres sejam veiculados em lei, por força do princípio da legalidade. É que tal princípio rege todos os aspectos da relação jurídico-tributária, firmada entre Fisco e contribuinte (e ou responsável), inclusive as relações que conformam os deveres de "colaborar com o fisco". CARRAZZA, Roque Antonio. Op. cit, p. 214. Dado o diminuto escopo desse artigo, tal discussão não será desenvolvida, de maneira a já se partir da premissa de que poderia a Receita Federal, em tese, erigir obrigações acessórias afetas a seu âmbito de competência tributária.

149 E, não apenas aquelas cujo valor (ou valores somados) possa configurar hipótese de incidência do imposto de renda sobre ganho de capital.

150 Informações dadas pelo gerente de controladoria do Grupo.

para fazer tal adaptação. Tais encargos podem tornar impraticável a exploração dessa atividade em solo brasileiro, mormente se somado ao custo indireto (burocrático) relacionado a manutenção do *compliance* exigido. Tal iniciativa, aliás, vai de encontro à desburocratização fiscal proposta pelo atual governo.

Verificado não se tratar de verdadeira obrigação acessória, afinal, desconexa da obrigação principal, o ponto que merece reflexão, agora, é o que de fato está em vias de ser instituído por tal instrução normativa.

2.2 DESVELANDO O QUE DE FATO ESTÁ SENDO FEITO…

De proêmio, chama a atenção a abrangência do conceito de "criptoativo" dado pela Receita Federal. Consoante art. 4º da proposta de instrução normativa, considera-se criptoativo, "a representação de valor digital, não emitida pelo Banco Central do Brasil, distinta de moeda soberana local ou estrangeira, cujo preço pode ser expresso em moeda soberana local ou estrangeira". Trata-se de redação sob cujo limite semântico remanescem inúmeras realidades distintas.

Destarte, tanto moedas virtuais (tais como as necessárias para adquirir funcionalidades aos games), quanto *utility* ou *security tokens*[151], ou ainda programas de milhagens (dotz etc.), estariam abrangidas pela definição normativa. Todos são representações de valor digital não emitidas pelo Banco Central, que não constituem moeda soberana, bem como possuem preço que pode ser expresso em moeda local ou estrangeira. No entanto, não parece se amoldar à competência da Receita Federal a notícia de toda e qualquer operação realizada com todo tipo de representação virtual de valores (tokens), que possam ser expressos em moeda (que tenham valor monetário).

É dizer, *tokens* representativos de participação acionária, ou que representem propriedades imobiliárias, ou mercadorias, bem como moedas virtuais necessárias a aquisição de funcionalidades nos games, ou que possibilitem troca por produtos (nos programas de milhagens), não parecem ser o foco de atenção da Receita Federal do Brasil, em que pese estarem dentro do conceito dado. Logo, parece necessário readequar tal redação a fim de que o dever de informar a Receita restrinja-se apenas ao universo das criptomoedas. Sugestões sobre o assunto serão dadas na parte final do presente artigo. No entanto, por ora, merece menção o conceito, negativo, que pode nos servir de inspiração, dado pela legislação de Malta[152], que fala em "ativos financeiros virtuais" e define-os como qualquer forma de registro digital que é usado como meio digital de troca, unidade de conta

---

151 Apertada síntese, os tokens de utilidade seriam unidades de serviço, que fornecem ao usuário/proprietário acesso futuro a um produto ou serviço. Já os security tokens seriam representações de valores mobiliários (ações e debêntures). Porém, existem outras classificações, mais abrangentes, que se referem a outras funcionalidades dos tokens. Sobre o assunto, vide Nugnes, Luiz Gustavo. Digitalização de ativos utilizando Crypto Tokens (Blockchain). Disponível na URL: < https://cryptowatch.com.br/digitalizacao-de-ativos-utilizando-crypto-tokens-blockchain/>, acesso em 25/11/2018.

152 Virtual Financial Assets Act (Lei de Ativos Financeiros Virtuais, em tradução livre). Disponível na URL: <http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12872&l=1>, acesso em 25.11.2018.

ou reserva de valor e que não é (a) dinheiro eletrônico[153]; (b) um token virtual[154]; ou (c) um instrumento financeiro[155]. Impende destacar justamente o afastamento de figuras próximas, mas que não configurem verdadeiras criptomoedas (espécie de criptoativos).

Pois bem, e já se adentrando no item relativo à prestação de informações pelas exchanges nacionais, nosso mote principal, leitura superficial do documento denuncia que não andou bem a Receita Federal. É que sob a pecha de "obrigação acessória", fixou-se verdadeiro dever ilegal para que as exchanges de criptoativos noticiem as movimentações de seus usuários, fornecendo, ao Fisco federal, dados sigilosos, sem uma justa causa a tanto. Esclareço.

O art. 7º da proposta de instrução normativa determina seja entregue à Receita Federal todas as informações inerentes à operação com criptoativos (tipo de operação[156], data, valores - inclusive em reais-, pessoas envolvidas, taxas cobradas pela exchange):

> Art. 7º Deverão ser informados para cada operação:
>
> I - nos casos previstos no inciso I e na alínea "b" do inciso II do caput do art. 5º:
>
> a) a data da operação;
>
> b) o tipo de operação, conforme Anexo Único;
>
> c) os titulares da operação;
>
> d) os criptoativos usados na operação;
>
> e) a quantidade de criptoativos negociados, em unidades;
>
> f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação;
>
> g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver;
>
> II - no caso previsto na alínea "a" do inciso II do art. 5º:

153 Dinheiro eletrônico seria o armazenamento digital de valores representativo de fundos, existente perante instituições financeiras, usado para fazer transações de pagamentos, e aceitas por pessoas físcas e jurídicas distintas das instituições financeiras emissoras (representação de "fiat" currencies).

154 "Token virtual" significa uma forma de registro em meio digital cuja utilidade, valor ou aplicação é restrita somente à aquisição de bens ou serviços, seja exclusivamente dentro da plataforma DLT (distributed ledger technology) na qual ou em relação à qual foi emitida ou dentro de uma rede limitada de plataformas DLT.

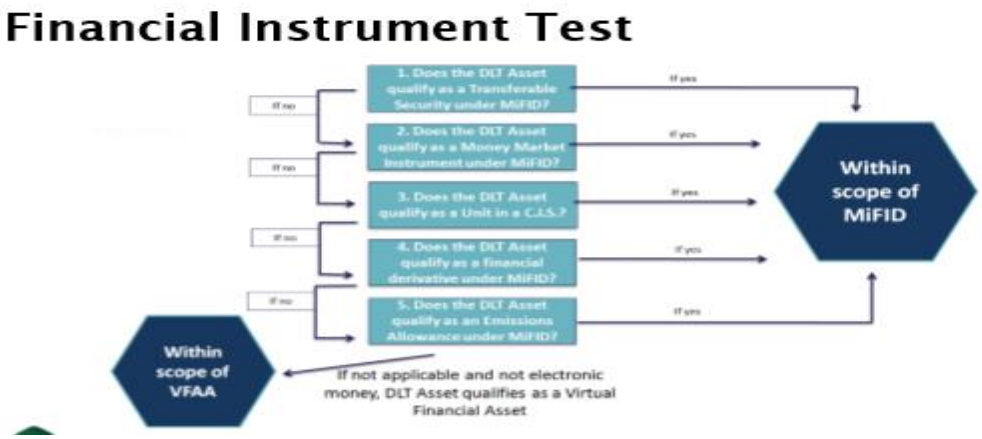
155 Fora criado um teste, em julho do presente ano a fim de se verificar a natureza de instrumento financeiro, ou não:

156 Compra e venda; permuta; doação; transferência de criptoativo para a exchange; retirada de criptoativo da exchange; cessão temporária (aluguel); dação em pagamento; dentre outras operações.

a) a identificação da exchange;

b) a data da operação;

c) o tipo de operação, conforme Anexo Único;



d) os criptoativos usados na operação;

e) a quantidade de criptoativos negociados, em unidades;

f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação;

g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver.

Parágrafo único. As informações a que se refere o caput devem conter a identificação dos titulares das operações e incluir nome, nacionalidade, residência fiscal, endereço, número de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ) ou Número de Identificação Fiscal (NIF) no exterior, quando houver, nome empresarial e demais informações cadastrais.

Tal previsão contraria o direito ao sigilo de dados, constitucionalmente assegurado pela Constituição Federal em seu art. 5º, XII[157]. Afinal, fixa-se, sem qualquer critério, ou justa causa, a obrigatoriedade das exchanges de criptomoedas fornecerem dados de seus clientes. É dizer, exige-se o fornecimento de dados sigilosos de milhares de usuários sem uma condicionante mínima,

157 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

XII - **é inviolável o sigilo** da correspondência e das comunicações telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

como, por exemplo, suspeita de sonegação fiscal, ou de outro delito financeiro, que eventualmente esteja sendo apurado em procedimento administrativo.

Sobre o assunto, merece relembrarmos o caso relativo à quebra de sigilo de dados bancários, sem prévia determinação judicial, consoante estabelecido nos arts. 5º e 6º da Lei Complementar 105/2001. A questão central dizia respeito à constitucionalidade dos artigos 5º e 6º da Lei Complementar 105/2001, que conferiam aos órgãos da administração tributária meios para obter dados bancários dos contribuintes sem necessidade de prévia autorização judicial.

O artigo 5º estabelece uma forma de fornecimento de dados periódicos à União relativamente às operações financeiras efetuadas pelos contribuintes. Nesse caso, devem ser encaminhados, pelas instituições financeiras, informes em que conste apenas a indicação dos titulares das operações e os montantes globais mensalmente movimentados, sem nada que permita identificar a sua origem ou a natureza dos gastos a partir deles efetuados (artigo 5º, parágrafo 2º).

Já o artigo 6º é mais amplo. Prevê mecanismo de acesso pontual que permite a todos os entes federados examinar "documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras". Porém, condiciona-se a obtenção desses dados a existência de "processo administrativo instaurado ou procedimento fiscal em curso". Ainda, exige-se que o exame desses dados seja considerado indispensável pela autoridade administrativa competente (artigo 6º, *caput*).

Ambos dispositivos foram objeto de controle de constitucionalidade[158]. Sob a ótica do Fisco, trata-se de reconhecer os meios necessários para que se possa identificar "o patrimônio, os rendimentos e as atividades econômicas do contribuinte", na forma do que prevê o artigo 145, § 1º, da Constituição Federal. Na interpretação do contribuinte, seria uma afronta ao direito à intimidade e privacidade do assegurado pelos incisos X e XII do artigo 5º da Constituição.

A decisão da Colenda Corte Constitucional foi no sentido de julgar pela constitucionalidade das previsões da Lei Complementar 105/2001, reconhecendo a prerrogativa da administração tributária em requisitar diretamente às instituições financeiras os dados bancários de seus correntistas para o fim de instruir processo administrativo ou procedimento fiscal já instaurados. A decisão do STF, evidentemente, não declarou o fim do sigilo bancário. Porém, reconheceu o fim desse direito contra o Fisco. É que, no entendimento dos ministros, o dever de guarda e sigilo em relação aos dados obtidos, na forma do previsto no parágrafo único do artigo 6º da LC 105/2001, permanece, posto que apenas se o "transfere" ao Fisco.

No entanto, em que pese a decisão exarada pelo E. STF, o que há de ser destacado é até mesmo nesse caso, é diploma legal que estabelece as condições e limites à quebra do sigilo bancário por parte das autoridades administrativas. É dizer, a quebra de sigilo das operações de instituições financeiras, para fins de informação das autoridades administrativas, pressupõe a essencialidade da informação a ser fornecida ao deslinde do processo administrativo instaurado, ou procedimento fiscal em curso. Assim, em juízo de ponderação entre o direito à privacidade e intimidade versus direito a obtenção de informações pelos Fiscos, optou o legislador por condicionar o acesso aos dados bancários à existência de uma justa causa a tanto (existência de processo administrativo instaurado ou procedimento fiscal em curso)[159].

É certo que as exchanges que operam com criptomoedas não se enquadram na definição legal de "instituições financeiras". No entanto, tais empresas também estão sujeitas à guarda do sigilo

158 O Supremo Tribunal Federal examinou a questão em quatro ADI's, de relatoria do ministro Dias Toffoli (ADIs 2.310, 2.397, 2.386 e 2.859) e em um recurso extraordinário, de relatoria do ministro Edson Fachin, com repercussão geral reconhecida (RE 601.314).

159 Além da garantia de que os dados devem ser protegidos no âmbito administrativo também.

daqueles que lhes confiam seus dados e, ainda, seus investimentos. Logo, não se afigura minimamente razoável, lançar contra tais organizações a obrigatoriedade de fornecer periodicamente às autoridades fiscais, as informações de seus clientes, de forma ampla e irrestrita. Sobretudo em razão de inexistir qualquer justa causa que fundamente o acesso a esses dados.

Não se defende inacesso a todo e qualquer dado, mas tão apenas que a prestação de informações seja prevista em lei e tenha uma justificativa plausível a tanto. Assim, parece ser necessário a existência de, ao menos, indícios de sonegação ou ainda de prática delituosa (como lavagem de dinheiro, evasão de divisas, entre outras), para que se admita a quebra de sigilo de dados em casos como os aqui descritos.

Não bastasse isso, há que se ter em mente que as operações com criptomoedas refletem transações que envolvem uma tecnologia de rede distribuída, que possibilita trocas por parte de cidadãos de todo o mundo em questões de segundos. Assim, as exchanges podem ter, em seus bancos de dados, informações de clientes de várias nacionalidades.

Adotada tal premissa, exigir das exchanges brasileiras o fornecimento de dados de seus clientes é atitude, no mínimo arriscada. Há o risco concreto de as exchanges nacionais serem demandas, juridicamente, por seus clientes. Por exemplo, caso uma exchange brasileira possua clientes europeus, estará sujeita às penas cominadas na GDPR (*General Data Protection Regulation*), a Lei Geral de Proteção de Dados, que se aplica a todas as organizações e estabelecimentos, sediadas tanto na União Europeia quanto em países estrangeiros, que oferecem bens e serviços a cidadãos europeus ou que tratam de dados pessoais de residentes na Europa.

Ainda, é de se lembrar da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais. Embora ainda esteja no período de *vacatio legis*, é cediço que entrará em vigor a partir de fevereiro de 2020, ocasionando verdadeira insegurança jurídica às operadoras de criptomoedas, frente ao teor protetivo da legislação em exame, relativamente ao tratamento de dados sensíveis, confrontar com a instrução normativa que ora se objurga.

3. CONCLUSÕES OU SUGESTÕES?

De todo o exposto, percebemos que a proposta de Instrução Normativa veiculada na Consulta Pública nº 06/2018, da Receita Federal do Brasil, não observou o âmbito de competência afeto ao erigimento dos deveres instrumentais, bem como parece ter ofendido o direito à privacidade e intimidade, inerente ao sigilo de dados. Assim, da forma como erigida, o diploma normativo não encontra guarida em nosso ordenamento jurídico. No entanto, a fim de iniciar, e/ou fomentar o debate, encerramos o presente artigo, propondo sugestões a referido projeto de instrução normativa, para que se a adéque aos ditames constitucionais e legais regentes do assunto.

Primeiramente, parece imprescindível que se delineie de forma mais adequado o campo de abrangência dos deveres impostos. Estamos nos referindo ao conceito bastante amplo dado, pela instrução normativa, ao termo "criptoativo". Como vimos, as criptomoedas são bens operados via *blockchain*, e que têm potencial de monetarização. Portanto, não basta ser representação digital de valor, e/ou tampouco basta ser operacionalizado via *blockchain*, para fins de caracterização da criptomoeda. Há que se reunir as duas características concomitantemente, e ser passível de monetização (vertida em moeda local ou estrangeira oficiais) para ser uma criptomoeda. Nesse sentido, a solução sugerida é que, ao invés de se utilizar "conceito" (delimitador do âmbito de competência), usemos "tipo"[160], elencando na categoria de "criptoativos" dignos de fiscalização, nesse primeiro momento, apenas as principais criptomoedas transacionadas, que apresentam potencial monetário para troca (fiat X criptomoeda). Afinal, muitas das criptomoedas lançadas sequer chegam a ter uma aceitabilidade mínima no mercado a justificar o monitoramento de dados (são as chamadas "*shitcoins"*).

Em segundo lugar, verificamos que os deveres instrumentais devem ser conexos à obrigação principal, cuja ocorrência pretende verificar por meio do exame de dados e documentos. Em sendo as operações com criptoativos sujeitos a incidência do imposto de renda, sob o ganho de capital, as obrigações acessórias eventualmente impostas às exchanges devem gravitar sob tal "fato jurídico". Consoante a legislação regente do imposto de renda sob o ganho de capital, apenas as operações em valor acima de R$ 35.000,00 (trinta e cinco mil reais) estão sujeitas a essa tributação. Assim, sugere-se que a instrução normativa em análise exija que sejam prestadas informações

160 A ideia de "tipo" foi sistematizada, em doutrina germânica, em oposição a de "conceito": enquanto um conceito jurídico" permite uma definição exata, com contornos precisos e específicos, no "tipo" não cabe falar em definição, mas em descrição. Esclarece Luis Eduardo Schoueri que "o conceito se define a partir de seus contornos, i.e., afirmando-se quais os pontos que ele não pode ultrapassar sob pena de fugir do conceito que se procura, enquanto o tipo se descreve a partir do seu cerne, i.e, daquilo que ele deve preferencialmente possuir" SCHOUERI, Luís Eduardo. Direito Tributário. 4ª ed. São Paulo: Saraiva, 2014, p. 269. Mizabel de Abreu Machado Derzi foi quem aprofundou a idéia de "tipo" na nossa doutrina especializada. Aliás, referida autora demonstrou a confusão terminológica ao entorno do termo "tipo". Salienta que "tipos" "(...) além de serem uma abstração generalizadora, são ordens fluidas, que, colhem, através da comparação, características comuns, nem rígidas, nem limitadas, onde a totalidade é critério decisivo para a ordenação dos fenômenos aos quais se estendem. São notas fundamentais ao tipo, a abertura, a graduabilidade, a aproximação da realidade e a plenitude de sentido na totalidade" - DERZI, Misabel de Abreu Machado. Direito Tributário, Direito Penal e tipo. São Paulo: Revista dos Tribunais, 1988, p. 48. No entanto, "a tipicidade é utilizada incorretamente no campo do Direito Penal e do Tributário, com mais frequência, em sentido oposto, como sinônimo de legalidade material rígida da hipótese de norma, do pressuposto ou fato gerador. (...) o estudo da tipicidade, como ordem fluida e transitiva do pensamento, ficou severamente prejudicado nos países de língua espanhola ou portuguesa" - DERZI, Misabel de Abreu Machado. Mutações, Complexidade, tipo e conceito, sob o signo da segurança e da proteção da confiança. In: TORRES, Heleno Taveira (coord). Tratado de Direito Constitucional Tributário. Estudos em homenagem a Paulo de Barros Carvalho. São Paulo: Saraiva, 2005, p. 262.

relativas a operações cujo valor seja superior a R$ 35.000,00 (trinta e cinco mil reais)[161] seja em uma única transação, ou sejam em várias cuja soma mensal ultrapasse esse valor.

Por fim, não se pode olvidar que, além do intuito arrecadatório da medida proposta pela Receita Federal do Brasil, objetiva-se evitar a ocorrência de operações de sonegação, de corrupção e de lavagem de dinheiro. Sob esse prisma, a exigência da Administração deveria estar limitada às operações que se mostrem suspeitas, ou indiciária de prática delituosa.

161 Art. 22 da Lei 9250/1995 estabelece a isenção do pagamento do imposto de renda relativo a ganho de capital auferido pela alienação de bens e direitos de pequeno valor, assim entendidos os valores de até R$ 35.000,00.

3. REFERÊNCIAS BIBLIOGRÁFICAS

CARRAZZA, Roque Antonio. Reflexões sobre a obrigação tributária. São Paulo: Noeses, 2010

CARVALHO, Paulo de Barros. Direito Tributário, Linguagem e Método. 4ª ed. rev e ampl. São Paulo: Noeses, 2011. Mutações, Complexidade, tipo e conceito, sob o signo da segurança e da proteção da confiança. In: TORRES, Heleno Taveira (coord). Tratado de Direito Constitucional Tributário. Estudos em homenagem a Paulo de Barros Carvalho. São Paulo: Saraiva, 2005.

DERZI, Misabel de Abreu Machado. Direito Tributário, Direito Penal e tipo. São Paulo: Revista dos Tribunais, 1988

PAULSEN, Leandro. Capacidade Colaborativa. Princípio de Direito Tributário para obrigações acessórias e de terceiros. Porto Alegre: Livraria do Advogado Editora, 2014

SCHOUERI, Luís Eduardo. Direito Tributário. 4ª ed. São Paulo: Saraiva, 2014.

TORRES, Heleno Taveira (coord). Tratado de Direito Constitucional Tributário. Estudos em homenagem a Paulo de Barros Carvalho. São Paulo: Saraiva, 2005.

A TUTELA DAS INSTITUIÇÕES FINANCEIRAS BRASILEIRAS EM FACE AOS RISCOS ENVOLVIDOS NO INVESTIMENTO EM CRIPTOMOEDAS E DAS *INITIAL COIN OFFERINGS* (ICO'S)

JOSÉLIO JORGE TEIDER

RESUMO:
A evolução da tecnologia da informação propiciou um aumento na capacidade computacional e também na conectividade de forma globalizada causando impacto notável no sistema financeiro possibilitando o surgimento de mudanças incisivas na forma como as pessoas lidam com as transações financeiras. Este contexto de impressionante inovação tecnologia foi o berço das criptomoedas que estão revolucionando as relações negociais em vários segmentos da sociedade, dispensando entes centralizadores ao fornecer um sistema que garante a autenticidade das transações por meio de avançadas técnicas de criptografia das transações. O presente artigo se propõe a realizar um estudo por meio de pesquisa bibliográfica pelo método dedutivo de como as instituições financeiras no Brasil estão tratando, direta ou indiretamente as os investimentos neste novo cenário por meio de aquisição de criptomoedas, criptoativos e ainda por meio das Ofertas Iniciais de Moedas, as ICO's (*Initial Coin Offering's*). São tratadas as principais manifestações a respeito do assunto emitidas pelas instituições brasileiras responsáveis pela regulamentação do setor financeiro: Receita Federal, Banco Central e Comissão de Valores Mobiliários (CVM). Deste estudo resta entendido que as instituições estão muito atentas na evolução do mercado, mas suas decisões estão em descompasso com a velocidade das inovações de mercado.

PALAVRAS-CHAVE: CVM, criptomoedas, criptoativos, investimento, ICO's.

ABSTRACT: The evolution of information technology has led to an increase in computational capacity and also in connectivity in a globalized way causing a remarkable impact on the financial system, allowing the emergence of a disruptive solution in the digital representation of how people deal with financial transactions. This context of impressive technology innovation was the cradle of cryptocurrencies that are revolutionizing business relationships in various segments of society, dispensing with centralizing entities by providing a system that ensures the authenticity of transactions by means of advanced transaction encryption techniques. This article proposes to study through a bibliographical research by the deductive method of how financial institutions in Brazil are directly or indirectly dealing with the investments in this new scenario through the acquisition of cryptocurrencies, cryptoassets and also through the Initial Coin Offering's ICO's. The main manifestations regarding the subject of the Brazilian institutions responsible for the regulation of the financial sector: Receita Federal, Banco Central e Comissão de Valores Mobiliários (CVM) are dealing with it. It is understood that institutions are very attentive in the evolution of the market, but their decisions are in discrepancy with the speed of market innovations.

KEYWORDS: CVM, cryptocurrencies, cryptoassets, investment, ICO's.

1. INTRODUÇÃO

A evolução da Tecnologia da Informação impulsionou a formação de uma aldeia global nos modelos previstos por Toffler (1980) onde as pessoas utilizam a tecnologia para praticamente todas as suas atividades. As transações financeiras não ficam incólumes a esta revolução. As instituições financeiras muito se beneficiam com a tecnologia, oferecendo novos serviços, mais eficiência e, por óbvio, maior lucratividade para si. O próprio dinheiro ganhou uma versão digital, por meio de transações eletrônicas que implementavam, de forma segura e prática, as transações com moeda e papel-moeda em suas versões físicas. Nesse caso, as próprias instituições financeiras, desenvolveram sistemas computacionais para que as transações monetárias pudessem ser realizadas por meio da Internet e dos dispositivos a ela conectados, com todos os benefícios que esta fornece. Os sistemas financeiros convencionais implementados na Internet apenas refletem a estrutura financeira do mundo físico e o uso da tecnologia propicia vantagens como a praticidade e a rapidez no uso dos serviços financeiros. Porém, o paradigma continua o mesmo: sistema financeiro centralizado e rigidamente controlado pelos governos de cada nação.

Este paradigma começa a ser descontruído com o surgimento das criptomoedas, uma forma de dinheiro puramente digital sem ente intermediador nem regulador, com informações distribuídas através de nós pela Internet, criando uma rede descentralizada e com confiabilidade garantida por meio de sofisticados algoritmos (ULRICH, 2014). Um dos primeiros casos práticos desta tecnologia foi a implementação da criptomoeda conhecida como Bitcoin, uma inovação monetária baseada em sofisticada estrutura tecnológica, essencialmente digital e descentralizada. Trata-se de um meio de pagamento eletrônico inovador, instantâneo e de alcance global que independe de uma instituição que garanta o seu lastro, auto regulamentada e com uma inovação tecnológica sem precedentes na história da humanidade (EVANS el al, 2017). A formalização desta inovação aconteceu em 2008 por meio do manifesto intitulado “Bitcoin: A Peer-to-Peer Electronic Cash System” de autoria de Satoshi Nakamoto, pseudônimo do programador (ou grupo de programadores) que desenvolveu e distribuiu livremente este sistema computacional (NAKAMOTO, 2008, p. 8).

Rapidamente houve um interesse pelo modelo proposto e uma disseminação bastante expressiva de outras criptomoedas e vários projetos utilizando a tecnologia por trás desta revolução. Trata-se da tecnologia Blockchain, um imenso livro digital formado por registros distribuídos em uma cadeia de blocos armazenados em arquivos eletrônicos interligados entre si, formando uma cadeia criptografada, em tese, inviolável. A cadeia de blocos é dinâmica e pode crescer indefinidamente a partir do bloco gênese (primeiro bloco na cadeia) por meio de sucessivos blocos de informação interligados com autenticidade confirmada por meio da aplicação de criptografia assimétrica[162] (DE FILIPPI; WRIGHT, 2015). A Blockchain é um sistema descentralizado e distribuído, onde não há necessidade de se confiar em um terceiro ou em um intermediário que valide das transações, como um banco central, cartório ou uma instituição governamental que autentique as transações entre os usuários. Toda confiança é garantida por sofisticados algoritmos computacionais implementados por softwares instalados nos computadores que fazem parte de uma rede conectada pela Internet. Estes algoritmos tem a capacidade de criar um consenso automático entre os usuários da rede para validar e confirmar a veracidade das transações na cadeia de blocos onde são registradas as informações que são armazenadas e distribuídas por computadores conectados em rede ponto-a-ponto pela Internet, sem obrigação da presença de um servidor central. Cada vez que uma informação realizada é inserida em um bloco nesta cadeia, ela é criptografada, marcada temporalmente e inserida em um bloco que está encadeado ao bloco anterior, dando sequência a esta cadeia de blocos. Esta transação é sincronizada e todos os nós da rede são atualizados. Os

[162] Criptografia assimétrica, também conhecida como de chave pública, é um tipo de protocolo de criptografia baseados em algoritmos que requerem duas chaves, uma delas sendo secreta (ou privada) e a outra delas sendo pública.

algoritmos em cada nó desta rede estão implementados de tal forma que a vinculação de um novo bloco depende do consenso da maioria dos outros participantes da rede, tornando a Blockchain muito segura, praticamente inviolável, pois para causar uma adulteração em um registro na cadeia de blocos seria necessário alterar todos os blocos anteriores até o bloco inicial (bloco gênese) para acomodar a nova informação falsificada, convencendo todos os outros nós da rede Blockchain a entrar em consenso com cada uma das interações de alteração (TAPSCOTT, 2016).

Apesar do primeiro e mais notável projeto baseado na tecnologia Blockchain ser a criptomoeda Bitcoin, é importante ressaltar que tecnologia Blockchain não se limita às transações financeiras, mas também serve como um sistema de registro e inventário para registrar, rastrear, monitorar e transacionar todos os ativos. Sua arquitetura, distribuída e descentralizada, pode ser aplicada para registrar ativos tangíveis como propriedades físicas, casas, carros ou ativos intangíveis como, por exemplo, votos, ideias, reputação, intenção, dados de saúde, informações etc. (SWAN, 2015, p. 24).

As possibilidades de soluções baseadas nesta tecnologia são muito promissoras e se houver implementações de soluções larga escala pode-se causar um impacto econômico significativo. Deste modo, os órgãos que têm a competência de organizar o sistema financeiro brasileiro estão se manifestando de forma prudente e paulatina. Neste contexto, o presente artigo se propõe a realizar um estudo sobre a questão da regulamentação das criptomoedas no Brasil e, em particular, sobre a regulação dos investimentos em "Initial Coin Offering" (ICO) que em português significa "Oferta Pública de Moedas".

A REGULAÇÃO DAS CRIPTOMOEDAS PELO BANCO CENTRAL

O Bitcoin foi a primeira de muitas criptomoedas que se encontram implementadas atualmente (INFOMONEY, 2017) e que tem como característica mais fascinante a sua natureza orgânica; não sendo emitida por nenhuma autoridade central, tornando-se teoricamente imune à interferência ou manipulação do governo ou de poderosos e influentes grupos econômicos (NARAYANAN et al., 2016).

A intensa proliferação de comunidades virtuais que estão criando e distribuindo o seu próprio dinheiro digital, fenômeno desencadeado pelos desenvolvimentos tecnológicos e pelo aumento do uso da Internet, chamou a atenção dos bancos centrais. Em 2012, o Banco Central Europeu definiu moeda virtual como "um tipo de moeda digital não regulamentada, que é emitida e geralmente controlada por seus desenvolvedores, usada e aceita entre os membros de uma comunidade virtual específica" (ECB, 2012, p. 13).

Também a academia científica apresentou importantes conceitos a respeito do tema. Segundo Lansky (2018), o sistema computacional que implementa uma criptomoeda atende a seis condições:

não requer uma autoridade central pois seu reconhecimento sucede do consenso distribuído;

mantém uma visão geral das unidades monetárias e de quem mantém sua propriedade;

define se novas criptomoedas podem ser criadas, em quais circunstâncias isso pode ocorrer e como será determinada a sua propriedade;

comprova a propriedade de uma criptomoeda exclusivamente por meio de criptografia;

realiza transações de transferência de propriedade das criptomoedas.

gerencia múltiplas instruções simultâneas reivindicando a propriedade da mesma criptomoeda e decide por somente uma delas.

O estabelecimento destas condições é importante para a fixação do conceito do que é uma criptomoeda por meio da observação do funcionamento do algoritmo que a implementa. Também é útil para a delimitação das peculiares condições que implementam as criptomoedas, de tal modo que se possa examinar os impactos que suas características provocam nos sistemas financeiros já instituídos e, também, como poderia ser possivelmente implementada uma tutela jurídica.

Seguindo o posicionamento de muitos países de tratar as criptomoedas como representação digital de valor, em uma perspectiva legal, as autoridades brasileiras também não consideram as criptomoedas como dinheiro em si, face ao monopólio estatal como emissor de moeda (EBA, 2015). No Brasil, a Constituição Federal em seu art. 21, inciso VII, atribui a competência exclusiva de emitir moeda soberana à União e expressa no art. 164 que é atribuído ao Banco Central do Brasil o monopólio na emissão de moeda (BRASIL, 1988).

O Banco Central do Brasil se manifestou oficialmente por intermédio do Comunicado n.º 31.379/2017 alertando enfaticamente que as criptomoedas não têm nenhuma entidade que as garanta, nem garantia de conversão para moeda fiduciária e, também, não tem lastro em nenhum ativo real, sendo que o seu valor é resultante da confiança que a comunidade tem na relação de compra e venda entre os seus usuários. Alerta também sobre os "riscos imponderáveis, incluindo, nesse caso, a possibilidade de perda de todo o capital investido, além da típica variação de seu preço" a que se expõem os detentores de criptomoedas uma vez que há muita especulação ao seu redor (BCB, 2017, p. 1). O comunicado também destaca que as empresas que negociam ou guardam criptomoedas (conhecidas como *exchanges*[163]) não são reguladas, autorizadas nem monitoradas pelo Banco Central do Brasil, do mesmo modo em que no cenário internacional também não há instituições financeiras oficiais que forneçam guarida legal ou regulatória em face às criptomoedas. Entende-se que o comunicado tem o objetivo de alertar a comunidade em geral e expressar que o Banco Central do Brasil "atento à evolução do uso das moedas virtuais (...) para fins de adoção de eventuais medidas, se for o caso, observadas as atribuições dos órgãos e das entidades competentes" (BCB, 2017, p. 1).

A REGULAMENTAÇÃO DAS CRIPTOMOEDAS PELA CVM

Seguindo o posicionamento de muitos países de tratar as criptomoedas como representação digital de valor, em uma perspectiva legal, as autoridades brasileiras também não consideram as criptomoedas como dinheiro em si, face ao monopólio estatal como emissor de moeda (EBA, 2015). No Brasil, a Constituição Federal em seu art. 21, inciso VII, atribui a competência exclusiva de emitir moeda soberana à União e expressa no art. 164 que é atribuído ao Banco Central do Brasil o monopólio na emissão de moeda (BRASIL, 1998).

A CVM (Comissão de Valores Mobiliários), autarquia do Ministério da Fazenda, posicionou-se a respeito do tema de criptomoedas em sua Relatório Anual de 2017. A instituição expressa que a CVM "não tem jurisdição sobre a regulação de criptoativos, como no caso do Bitcoin, restringindo a sua atuação à regulação de veículos de investimento que possam vir futuramente, a adquirir tais ativos" (CVM, 2017 p. 20).

Além de legislação específica, o Brasil também não conta com um índice de cotação oficial dos preços de criptomoedas. Por ora tem-se que conta com as avaliações dos índices internacionais. Estes índices demonstram uma queda dos preços do Bitcoin que recuou de US$ 19 mil em dezembro do ano passado para US$ 6,375 mil hoje é referenciada por meio do Ofício circular 11/2018 onde é dito que "até pela queda dos preços no mercado internacional, o interesse diminuiu bastante". Porém o pronunciamento oficial da CVM na referida circular demonstra que a instituição está se debruçando seriamente sobre o tema e acompanhando a evolução dos

[163] Tradução livre: o termo em inglês *exchanges* significa, em português, troca ou câmbio, no caso: câmbio de moedas.

criptoativos para estar preparada no caso de uma nova ascensão das criptomoedas no mercado financeiro global.

O ENTENDIMENTO DA CVM SOBRE AS INICIAL COIN OFFERINGS – ICO'S

A CVM define em seu site que uma *Initial Coin Offering*[164] (ICO) trata-se de uma captação pública de recursos junto ao público investidor que recebe em contrapartida ativos virtuais, exclusivamente digitais, conhecidos como *tokens* ou *coins*. Estes são assentamentos eletrônicos dos ativos adquiridos escritos em uma cadeia de registros criptografados e distribuída de forma descentralizada em muitos, ou até mesmo em todos, os computadores que fazer parte desta rede conhecida como Blockchain, o que garante, em tese a segurança e a inviolabilidade destes registros (CVM, 2017a; CVM, 2018; CVM, 2018).

As ICO's são estruturadas em modelos inteiramente digitais. Estes modelos proporcionam, por meio do uso alcance global da Internet, extraordinária capacidade de prospecção de investidores em qualquer localidade. A maneira de investir também é em muito facilitada através da transferência online em vários tipos de pagamentos, de moedas fiduciárias tradicionais até mesmo criptomoedas. Tamanha facilidade pode promover operações muito arriscadas para os investidores. A CVM ainda alerta que os gestores de fundos tenham especial atenção às caraterísticas muito flexíveis e até mesmo voláteis das criptomoedas como *airdrops* e *forks* que podem acontecer em um criptoativos influenciando o comportamento de tais ativos. Por isso a CVM alerta para que os investidores sejam muito cautelosos nos investimentos associados à negociação de ativos virtuais e à participação em ICO's e elenca uma série seguintes riscos inerentes a tais investimentos (em especial no que diz respeito a emissores ou ofertas não registradas na CVM):

1) Risco de fraudes e pirâmides financeiras;
2) Inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento (suitability);
3) Risco de operações de lavagem de dinheiro e evasão fiscal/divisas;
4) Prestadores de serviços atuando sem observar a legislação aplicável;
5) Material publicitário de oferta que não observa a regulamentação da CVM;
6) Riscos operacionais em ambientes de negociação não monitorados pela CVM;
7) Riscos cibernéticos (dentre os quais, ataques à infraestrutura, sistemas e comprometimento de credenciais de acesso dificultando o acesso aos ativos ou a perda parcial ou total dos mesmos) associados à gestão e custódia dos ativos virtuais;
8) Risco operacional associado a ativos virtuais e seus sistemas;
9) Volatilidade associada a ativos virtuais;
10) Risco de liquidez (ou seja, risco de não encontrar compradores/vendedores para certa quantidade de ativos ao preço cotado) associado a ativos virtuais; e
11) Desafios jurídicos e operacionais em casos de litígio com emissores, inerentes ao caráter multijurisdicional das operações com ativos virtuais.

Estes ativos virtuais podem vir a constituir valores mobiliários, ou seja, um título de propriedade ou de crédito, quando conferem ao investidor direitos de participação no capital ou remuneração pré-

[164] *Initial Coin Offering*, significa em português: "Oferta Inicial de Moeda". Trata-se de uma denominação inspirada em uma analogia na expressão consagrada para o lançamento de ações de uma nova empresa no mercado: *Initial Public Offering (IPO)*, em português "Oferta Pública Inicial".

fixada sobre o capital investido ou ainda voto em assembleias que decidem o futuro do negócio do emissor, assim estabelecido no art. 2º, IX, da Lei 6.385/76:

> 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.

Porém, em alguns casos não há clara definição se os *tokens* adquiridos estão conferindo participação no negócio do emissor ou se trata-se apenas de um modelo de acesso à plataforma de serviços oferecidos pelo projeto, como se fosse uma licença de uso ou créditos para consumir o serviço (CVM, 2017).

Para se determinar qual é a natureza de uma *Initial Coin Offerings* (ICO's) pode-se recorrer ao seu *white paper*[165] normalmente publicado pelo seu emissor em um site na Internet onde se publica informações técnicas e operacionais do modelo do negócio. No caso do ativo virtual oferecido se enquadrar na classificação de ativo financeiro, será necessário o devido registro da sua emissão na CVM.

REGISTRO DAS INITIAL COIN OFFERINGS (ICO'S) NA CVM

Uma emissão pública de valores mobiliários para ter guarida no ordenamento brasileiro precisa estar devidamente registrada na CVM conforme art. 19 da Lei 6.385/1976 que veda a emissão pública de valores mobiliários sem o prévio registro na CVM:

> Art. 19. Nenhuma emissão pública de valores mobiliários será distribuída no mercado sem prévio registro na Comissão (Brasil, 1976a).

Este registro obriga o emissor a revelar oficialmente ao mercado sua situação econômica e financeira, possibilitando aos investidores uma avaliação correta dos títulos oferecidos e também ambiciona evitar que aqueles que ocupam posições influentes na estrutura do emissor possam auferir desonesta vantagem na negociação dos títulos dos valores mobiliários emitidos a partir de utilização abusiva de informações privilegiadas.

Somente em casos excepcionais conforme estabelecido no Art. 19, § 5º I, pode a CVM dispensar este registro. Estas dispensas de registro estão regulamentadas nos artigos 4º e 5º da Instrução CVM 400 que dispõe sobre as ofertas públicas de distribuição de valores mobiliários, nos mercados primário (investimentos diretos nas empresas) ou secundário (investimento em bolsas de valores), e serão aplicadas pela CVM "a seu critério e sempre observados o interesse público, a adequada informação e a proteção ao investidor". Por seu turno, serão automaticamente dispensadas de registro as ofertas públicas de ações de propriedade da União, Estados, Distrito Federal e municípios e demais entidades da administração pública e que não envolvam o público em geral. De todo modo, a exceção confirma a regra de que quando a oferta de emissão de títulos de valores

[165] *White paper*, em livre tradução, significa "livro branco" e, no caso, trata-se de um documento publicado em um site que mostra todas as condições de criação, funcionamento e apoio de uma *token* ou criptomoeda.

mobiliários for direcionada ao público em geral, é necessária a solicitação de registro na CVM (CVM, 2003).

Mesmo as ofertas públicas de valores mobiliários que forem emitidas em outros países tornadas públicas pela Internet com "o propósito de atingir o público em geral residente no Brasil" ou as operações realizadas pela Internet que envolvam investidores residentes, domiciliados ou constituídos no Brasil, estão sujeitas à autorização pela CVM, conforme disposto nos pareceres de orientação CVM n.º 32 e CVM n.º 33 (CVM, 2005a) (CVM, 2005b).

Um dos documentos essenciais para pedido de registro de programa de distribuição de valores mobiliários na CVM é o prospecto para os investidores, conforme os moldes estabelecidos na Instrução CVM 400, onde são disponibilizadas informações como perspectivas e planos da companhia; situação do mercado em que ela atua; os riscos do negócio e da oferta; o quadro administrativo da empresa, bem como informações sobre a oferta em si.

Para que uma ICO se enquadre dentro desta normatização da CVM, é necessário que não se limite à publicação prospecto concentrado em aspectos tecnológicos e operacionais, por mais relevantes que sejam. É importante que seja desenvolvido um estudo que contemple os mecanismos de governança exigidos, tais como diligências, auditorias e demonstrações financeiras emitidas por peritos e submetidas à verificação de regularidade junto à CVM.

Todavia exsurgem alguns problemas face a esta orientação, pois quando se trata de ICO's, muitas dessas ofertas são feitas por empresas ainda não operacionais, o que acrescenta um risco para o investidor. Outro alerta é para a falta de regulamentação das *Exchanges* e da própria falta de regras para o mercado de moedas virtuais também pelo Banco Central (BC).

TRANSFORMANDO AS *EXCHANGES* EM CORRETORAS DE *TOKENS*

A CVM elenca em seu site um arcabouço para a regulação da operação de ativos mobiliários que é empregado, por analogia, também à regulação de ativos virtuais. Conforme o § 1º, Art. 4º da Lei 6.404/76 não apenas a oferta pública deve ser registrada na CVM, mas também os emissores dos ativos mobiliários também devem ser previamente registrados nesta instituição (Brasil, 1976b).

Na prática corrente, os ativos virtuais (*tokens)* emitidos pelos ICO's são negociados em empresas conhecidas como *Exchanges*. Estas empresas, a princípio, não são instituições financeiras, não sendo autorizadas pelo Banco Central ou pela CVM a operarem ativos financeiros. No caso de um ativo virtual negociado na *Exchange* se caracterizar como ativo mobiliário que possa ser qualificado como um investimento financeiro, considerando que a negociação destes ativos deve ser realizada tão somente por intermediários autorizados, será necessário que esta se registre na CVM.

Uma vez registrada na CVM, uma *Exchange* poderia ser classificada como uma corretora de valores mobiliários regulamentados na Instrução CVM 505 e deve observar as exigências de *compliance* dispostas na Instrução CVM 301 que trata da prevenção à lavagem de dinheiro e na resolução CVM 539 que trata da adequada identificação do investidor. A CVM também dispões sobre a estrutura de mercado para organizar o mercado secundário de valores mobiliários em várias outras Instruções, tais como CVM 541, 542 e 543. Um emissor de ICO's precisa estar em conformidade com todo este regramento para evitar sanções e penalidades aplicáveis. Não é se de espantar que até o momento nenhuma operação desta natureza tenha sido registrada ou dispensada de registro.

A CVM também regulamentou por meio da Instrução 588 uma possibilidade de dispensa automática de registro de oferta pública, com características próprias, por meio da modalidade de crowdfunding.

REGULAÇÃO DA CVM A RESPEITO DE INVESTIMENTO EM *TOKENS* E *INITIAL COIN OFFERINGS* (ICO'S)

A CVM publicou no início de 2018 por meio de sua Superintendência de Relações com Investidores Institucionais (SIN) um ofício circular onde declara expressamente que os fundos de investimento brasileiros, que são regulados pela Instrução CVM 555, não podem investir diretamente em criptomoedas, pois estas não estão qualificadas como ativos financeiro. O ofício ainda alerta que as criptomoedas apresentam riscos de segurança e sua custódia ainda apresentam particularidades indefinidas e não reguladas (CVM, 2018a).

Em 19 de setembro de 2018, a CVM emitiu um ofício circular (SIN nº 11/2018) complementando o anterior autorizando os fundos de investimentos possam realizar investimentos em criptomoedas. Ressalta-se no ofício que esta autorização é para os fundos de investimento devidamente autorizados, não se trata aqui de uma anuência da CVM a investimentos de particulares em criptoativos. O investimento em criptomoedas suscita riscos de operações ilegais, tais como manipulação de preços, fraudes financeiras, sistemas de pirâmide e lavagem de dinheiro. A CVM, por meio da sua Superintendência de Relações com Investidores Institucionais (SIN) orienta que os investimentos dos fundos em criptomoedas sejam feitos através de *Exchanges* que respeitem critérios dos órgãos reguladores e adotem sérios sistemas de controle de emissão, gestão e governança de seus criptoativos por meio de sérios mecanismos de diligências.

Os riscos das ICO's são relevantes e é necessária muita cautela para evitar investimentos em projeto fraudulentos, como é o caso de vários *scams* que ocorreram recentemente, como afirma o ofício circular 11/2018 da CVM. Vários cuidados devem ser tomados e a circular da CVM elenca seis deles:

> (i) se o software base é livre e de código fonte aberto ou fechado;
>
> (ii) se a tecnologia é pública, transparente, acessível e verificável por qualquer usuário;
>
> (iii) se há arranjos que suscitem conflitos de interesse ou a concentração de poderes excessivos no emissor ou promotor do criptoativo, ou o uso de técnicas agressivas de venda;
>
> (iv) a liquidez de negociação do criptoativo;
>
> (v) a natureza da rede, dos protocolos de consenso e validação, e do software utilizados;
>
> (vi) o perfil do time de desenvolvedores, bem como seu grau de envolvimento com o projeto.

"Ainda sobre o tema da normalidade de funcionamento dos mercados em que são negociados os criptoativos e seus derivativos, é importante que o gestor verifique se determinado criptoativo não representa uma fraude, como, aliás, tem sido visto com grande recorrência, por exemplo, nas operações recentes de ICO pelo mundo", diz o documento. Ressalta-se, em outras palavras, da necessidade de um programa de *compliance*.

CONCLUSÃO

No Brasil as criptomoedas não têm o caráter de moeda em si, sendo mais reconhecidas como ativos financeiros, tem-se que o termo mais apropriado seria, então criptoativos e, assim sendo, sua tutela se daria pela regulamentação da CVM. De todo modo, a questão dos investimentos em criptoativos está longe de ser uma questão pacificada no ecossistema normativo brasileiro. As instituições responsáveis por tutelar o sistema financeiro no Brasil estão atônitas em face ao significativo crescimento de investimentos em neste tipo de ativo. Também a proliferação de projetos baseados em tecnologia Blockchain, oferecendo oportunidades para se adquirir estas unidades de valor, muitas vezes com lastro não bem definido por gerar riscos sistêmicos que podem se alastrar e causar severas perdas aos investimentos mais desavisados. A tecnologia, apesar de muito interessante e inovadora, pode apresentar falhas e importantes riscos. Há riscos relevantes também nos modelos de negócios e na possibilidade de esquemas fraudulentos e estes riscos podem se espraiar em muitos contextos: (i) riscos para os usuários das criptomoedas; (ii) riscos para não usuários, mas que participam do mercado onde são realizadas operações com criptomoedas; (iii) riscos para o mercado financeiro, os quais incluem lavagem de dinheiro e outros crimes; (iv) riscos para os sistemas de pagamentos baseados nas tradicionais moedas fiduciárias e (v) riscos para as autoridades regulatórias (EBA, 2014, p. 05). Os riscos acentuam-se face à possibilidade de se construir sofisticados projetos de lançamento de novas criptomoedas, compostos por operações financeiras e tecnológicas muito complexas, denominados ICO's[166], são inspirados nos investimentos em bolsa de valores conhecidos como IPO's[167].

Deste modo, a CVM se mantém bastante cautelosa e, até o presente momento não está permitindo o investimento direto em criptoativos no Brasil. A possibilidade disponibilizada para se aproveitar oportunidades neste sentido seria o investimento de fundos nacionais em fundos constituídos em outros países, conforme a Instrução Normativa 555 da CVM, que implica que estes fundos estejam em *compliance* com as normas dos países de origem, admitidos e regulamentados naqueles mercados. Seria uma forma de se delegar a inspeção da qualidade e da solidez dos investimentos em criptoativos para as instituições dos países de origem enquanto, de forma tímida e acanhada, a CVM espreita o mercado para depois se posicionar e se comprometer. De certa forma, o investidor é protegido, mas há de se ter o cuidado para que o emaranhando de leis brasileiras não venha tolher as oportunidades propiciadas pela revolução tecnológica no setor financeiro.

---

[166] IPO significa, em inglês, "Initial Public Offering" que, em português, quer dizer, "Oferta Pública de Ações".

[167] ICO significa, em inglês, "Initial Coin Offering" que, em português, que dizer, "Oferta Pública de Moedas". No caso em estudo seriam as criptomoedas.

REFERÊNCIAS

BCB – BANCO CENTRAL DO BRASIL. **Comunicado nº 31.379. Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais**. Disponível em www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=31379&tipo=Comunicado&data=16/11/2017. Publicado em 16 nov. 2017. Acesso em 17 mar. 2019.

BRASIL. **Lei n.º 6.385 de 7 de dezembro de 1976. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6385.htm. Acesso em 17 mar. 2019.

BRASIL. **Lei n.º 6.404 de 15 de dezembro de 1976. Dispõe sobre as Sociedades por Ações**. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L6404consol.htm. Acesso em 17 mar. 2019.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Publicado em 05 de out de 1998. Acesso em 17 mar. 2019.

BRASIL. **Projeto de Lei 2303/15 - Banco Central Regular Moedas Virtuais.** Disponível em <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/banco-central-regular-moedas-virtuais>. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Instrução CVM 400. Dispõe sobre as ofertas públicas de distribuição de valores mobiliários, nos mercados primário ou secundário**. Disponível em http://www.cvm.gov.br/legislacao/instrucoes/inst400.html. Publicado em 29 dez. 2003. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Parecer de Orientação CVM n.º 32**. *Site da CVM.* Disponível em: http://www.cvm.gov.br/legislacao/pareceres-orientacao/pare032.html. Publicado em 30 set. 2005. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Parecer de Orientação CVM n.º 33**. *Site da CVM.* Disponível em: http://www.cvm.gov.br/legislacao/pareceres-orientacao/pare033.html. Publicado em 30 set. 2005. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Relatório Anual 2017**. Disponível em: http://www.cvm.gov.br/export/sites/cvm/publicacao/relatorio_anual/anexos/Relatorio_Anual_2017.pdf . Publicado em 25 mai. 2018. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Esclarecimentos sobre o investimento indireto em criptoativos pelos fundos de investimento**. Disponível em: http://www.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html. Publicado em 19 set. 2018. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Initial Coin Offerings (ICOs). FAQ da CVM a respeito do tema**. Disponível em http://www.cvm.gov.br/noticias/arquivos/2017/20171116-1.html. Publicado em 16 nov. 2017. Acesso em 17 mar. 2019.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Esclarecimentos sobre investimentos em criptomoedas**. Disponível em: http://www.cvm.gov.br/noticias/arquivos/2018/20180112-1.html. Publicado em 12 jan. 2018. Acesso em 17 mar. 2019.

DE FILIPPI, P; WRIGHT, A. **Decentralized blockchain technology and the rise of lex cryptographia.** Disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Publicado em 20 mar. 2015. Acesso em 17 mar. 2019.

ECB, EUROPEAN CENTRAL BANK. **Virtual Currency Schemes**. Disponível em: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Publicado em out. 2012. Acesso em 17 mar. 2019.

ECB, EUROPEAN CENTRAL BANK. **Virtual Virtual Currency Schemes – a further analysis**. Disponível em https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. Publicado em fev. 2015. Acesso em 17 mar. 2019.

EVANS, Philip; ARÉ, Lionel; FORTH, Patick; HARLÉ, Nicolas; PORTINCASO, Massimo. **O que fazer sobre o Blockchain**. HSM Management. São Paulo, n.121 , p.[20]-24, mar./abr. 2017.

INFOMONEY. **O que é Bitcoin?.InfoMoney Mercados**. http://www.infomoney.com.br/mercados/bitcoin/pagina/3. Acesso em 17 mar. 2019.

LANSKY, Jan. **Possible State Approaches to Cryptocurrencies**. Disponível em http://www.si-journal.org/index.php/JSI/article/viewFile/335/325. Publicado em jan. 2018 Acesso em 17 mar. 2019.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em https://bitcoin.org/bitcoin.pdf. Publicado em 31 ago. 2008. Acesso em 17 mar. 2019.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven (2016): **Bitcoin and Cryptocurrency Technologies**; Draft, Feb 9, 2016.
SWAN, Melanie. **Blockchain: Blueprint for a New Economy**. O'Reilly Media. Edição do Kindle, 2015.
TAPSCOTT, D., & TAPSCOTT, A. (2016). **Blockchain Revolution**. Cambridge, 2016.
ULRICH, Fernando. (2014). **Bitcoin: a moeda na era digital**. São Paulo: Instituto Mises Brasil.
TOFFLER, Alvin. **A terceira onda**. 22 ed. Rio de Janeiro: Record, 1997. 491 p.

ANÁLISE PREDITIVA DE DADOS E SUAS APLICAÇÕES NO DIREITO

Ellen Ferreira
É advogada, graduada em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR). Pós-Graduação em Processo Civil pela Uninter. Especialista em Coaching pelo Instituto Febracis. Atualmente integra a Comissão de Inovação e Gestão da OAB/PR.

Fulvio Leonardo Picoloto
É advogado, graduado em Direito pela Universidade Federal do Paraná (UFPR) e em Gestão Financeira pela Faculdade Opet. Especialista em controladoria pela FAE Business School. Atualmente integra a Comissão de Inovação e Gestão da OAB/PR.

Kael Moro
É advogado, graduado em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR). MBA em Gestão Estratégica de Empresas pela Fundação Getúlio Vargas (FGV). Especialista em Coaching pela Instituto Brasileiro de Coaching (IBC). Atualmente integra a Comissão de Inovação e Gestão da OAB/PR e cursa especialização em Direito para Startups na FGV.

Lígia Pedri
É advogada, graduada em Direito pelo Centro Universitário Curitiba (UNICURITIBA). Especialista em Direito Corporativo pela Universidade Positivo. Atualmente cursa especialização em Direito Público pela ESMAFE/PR.

Napoleão Lopes
É advogado, graduado em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR).

Máster em Direito Penal pela Universidade de Barcelona e Universidade Pompeu Fabra. Atualmente cursa especialização em Sociologia Política na UFPR.

RESUMO:
O estudo analisa a Análise Preditiva e algumas das possíveis aplicações no Direito, refletindo acerca do uso de Inteligência Artificial como meio para coleta e manipulação dos dados. Após uma digressão acerca dos conceitos e dos métodos empregados para análise de dados, alguns impactos do uso da Análise Preditiva são analisados de forma crítica, questionando-se a forma como a tomada de decisão pode ou poderá ser tomada a partir do resultado obtido com a análise de dados. O estudo considera ainda a recente Lei de Proteção de Dados Pessoais brasileira como mecanismo de efetiva tutela da privacidade individual. Quanto à metodologia, a abordagem da pesquisa foi teórica, exploratória e descritiva utilizando-se como procedimento a pesquisa bibliográfica nacional e internacional.

Palavras-chave: Análise Preditiva, Análise de Dados, Mineração de Dados, Proteção de Dados Pessoais, Privacidade.

ABSTRACT

The study analyzes the Predictive Analysis and some of the possible applications in Law, reflecting on the use of Artificial Intelligence as a means for collecting and manipulating the data. After a digression about the concepts and methods used for data analysis, some impacts of the use of Predictive Analysis are analyzed critically, questioning how decision-making can or can be taken from the result obtained with the data analysis. The study also considers the recent Brazilian Personal Data Protection Law as a mechanism for effective protection of individual privacy. As for the methodology, the research approach was theoretical, exploratory and descriptive using as a procedure the national and international bibliographic research.

Keywords: *Predictive Analysis, Data Analysis, Data Mining, Personal Data Protection, Privacy.*

LISTA DE ILUSTRAÇÕES

Figura 1 – Fluxograma da Análise Preditiva – MathWorks 3

Figura 2 – Modelo Preditivo – Erik Siegel 10

Figura 3 – Árvore de decisão – Stack Exchange 11

Figura 4 – Árvore de decisão – Erik Siegel 12

1. INTRODUÇÃO. O QUE É ANÁLISE PREDITIVA?

Atualmente, cada vez mais a inteligência artificial vem se expandindo e sendo utilizada como instrumento de auxílio na tomada de decisões públicas e privadas.

Os primeiros estudos sobre inteligência artificial foram realizados por Turing, em 1950. A inteligência artificial como é conhecida hoje, é resultado de um encontro de dez cientistas, interessados em computação simbólica, realizado em DartmouthCollege, New Hampshire, em 1956. Apesar de não possuir um conceito preciso, pode ser definida como "o estudo de como fazer os computadores realizarem tarefas para as quais, até o momento, o homem faz melhor"[168].

Em uma das suas diversas aplicações, busca-se resultado por meio da análise de dados, basicamente de duas formas, quais sejam, quantitativo e qualitativo[169]. O quantitativo estuda os dados procurando resultados em volume, enquanto o qualitativo busca qualificar os dados de forma objetiva ou subjetiva.

Neste artigo iremos analisar e estudar a qualitativa, que está voltada para análise de dados e predição. Esses dados podem tornar o mundo jurídico mais simples, facilitando tomadas de decisões e traçando objetivos que auxiliam empresas a se situar no atual cenário, definir metas e qual o caminho percorrer, prevendo o futuro com base no passado.

Para a análise dentro de uma empresa, existem níveis de maturidade, iniciam-se por planilha de excel, passando por *business intelligence*, chegando ao nível de predição, ou seja, análise descritiva, diagnóstica, preditiva e prescritiva[170]. Todavia, o objetivo será tratar sobre a análise preditiva.

A análise preditiva tem como objetivo prever os resultados futuros de uma empresa com base nos dados do passado, utilizando o computador, que os analisa e a partir disso realiza previsões.

Hoje, em regra, a maioria das empresas tomam decisões com base no "*feeling*", e a análise preditiva vem para ajudar nessas tomadas decisões de forma mais concisa, segura, assertiva, fazendo com que as empresas conquistem mais confiança no mercado. Segundo Eric Siegel, "prever é melhor do que adivinhar, e de fato, a máquina pode fazer isso".

A pergunta principal é: A análise preditiva está 100% correta?

Segundo Eric Siegel, como o comportamento humano na maior parte das vezes segue um padrão, a máquina consegue realizar muitas previsões assertivas, mas pode acontecer de errar, visto que tem uma minoria que não segue o padrão[171].

> "Agora, muitas coisas são simplesmente impossíveis de prever com alta precisão. Nós só podemos, na melhor das hipóteses, colocar probabilidades ásperas sobre se uma determinada pessoa irá... clicar, comprar, mentir, morrer ou qualquer outro resultado ou comportamento - mesmo se tivéssemos uma leitura de cada neurônio em seu cérebro. Os computadores, é claro, geralmente

[168] RICHE., **"Artificial Intelligence"**, McGraw-Hill, N.Y., 1983.
[169] SIEGEL, Eric – **AI, Machine Learning, and the Basics of Predictive Analytics for Process Management.** Agosto de 2018. Disponível em: <https://www.predictiveanalyticsworld.com/patimes/ai-machine-learning-and-the-basics-of-predictive-analytics-for-process-management/9632/> Acessado em 23/09/2018
[170] Retirado da aula sobre **"Análise Preditiva: Prevendo os resultados futuros da sua empresa"**. Abril de 2017. Disponível em: <https://www.youtube.com/watch?v=57DxJ0IaWoY>. Acessado em: 24/09/2018.
[171] SIEGEL, Eric – **Análise Preditiva**. Revisto e Atualizado. Alta Books.2017, página 12.

> sabem muito menos sobre uma pessoa do que isso - normalmente algumas dúzias ou talvez algumas centenas de detalhes sobre a pessoa e suas atividades anteriores. Mas mesmo previsões ruins são super valiosas. Apenas prever melhor do que adivinhar ajuda as organizações a melhorarem a tomada de decisões em grande escala. Por exemplo, se 5% de seus clientes cancelarem a cada mês, saber quais deles têm três vezes mais probabilidade de fazê-lo, ou seja, quem tem uma probabilidade de 15% de cancelar, faz uma grande diferença para o marketing, tornando mais eficiente e eficaz e, em alguns casos, literalmente multiplicando o lucro muitas vezes. E a mesma coisa se aplica para prever quais pacientes estão em maior risco de morrer - o que possibilita cuidados de saúde mais eficientes e eficazes"[172].

Pode-se aplicar a análise preditiva basicamente para clientes (marketing), operacional (aprender, planejar e gerir), parte de risco e fraude (monitorar, detectar e controlar).

Por fim, a análise preditiva responde basicamente três perguntas macros:

What Will Happen? O que vai acontecer?

Whatif? E se?

Howriskyis it? Como é o risco?

A análise preditiva não se trata de um simples exercício de vidência, mas sim de um trabalho de análise de um cenário específico, a fim de traçar possíveis tendências e prever determinados resultados futuros.

Trata-se, portanto, de uma *"tecnologia que aprende a partir da experiência (dados) para prever o comportamento futuro de indivíduos a fim de gerar melhores decisões"*[173].

Quanto mais eficiente for a mineração dos dados, mais segurança haverá para se tentar descobrir padrões e avaliar probabilidades de um determinado resultado futuro.

Cada aplicação de análise preditiva é definida da seguinte forma:

a) O que é predito: o tipo de comportamento (ou seja, ação, evento ou acontecimento) para prever para cada indivíduo, ação ou outro tipo de elemento.

[172] SIEGEL, Eric – **A Dr. Data Show Video: Why Machine Learning Is the Coolest Science.** Setembro de 2018. Disponível em: < https://www.predictiveanalyticsworld.com/patimes/dr-data-show-video-why-machine-learning-is-the-coolest-science/9703/> Acessado em 15/03/2019

[173] SIEGEL, Eric. 2017, página 13.

b) O que fazer com isso: decisões orientadas pela previsão; ação tomada pela organização em resposta ou informada por cada predição[174].

[174] Idem, página 22.

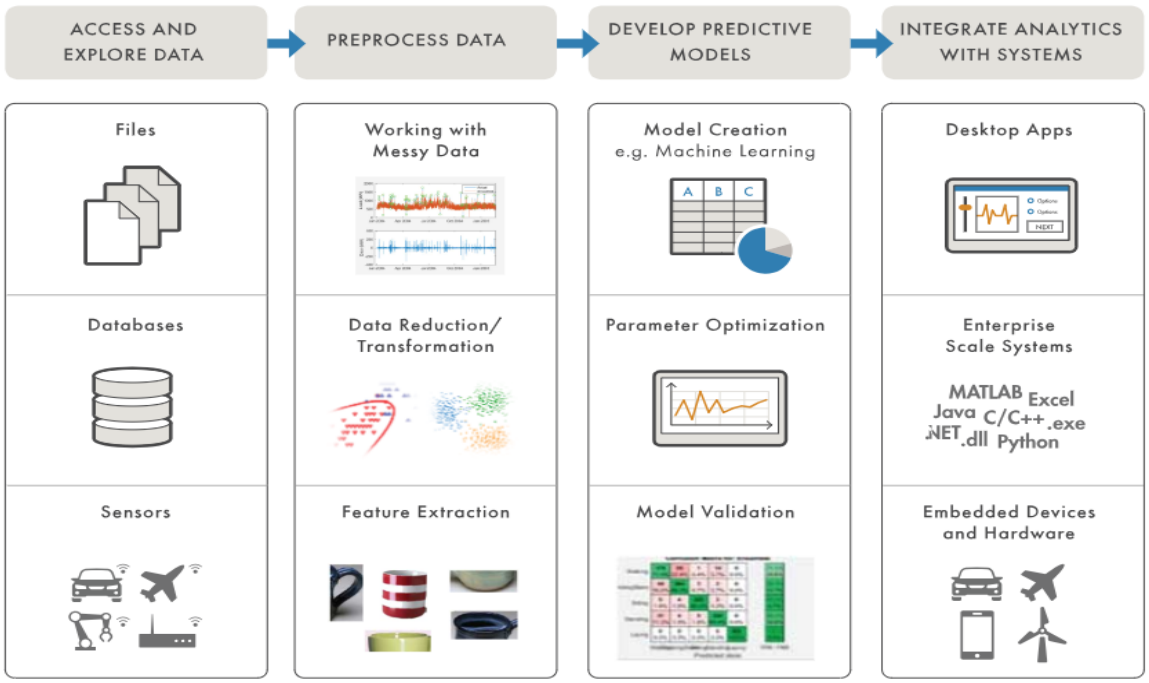
2. COMO A ANÁLISE PREDITIVA FUNCIONA?

Como já demonstrado, a Análise Preditiva é o resultado de um processo de aprendizado, que se inicia na mineração de dados, passa pelo processamento e limpeza da base, após, pelo aprendizado de máquina, modelagem preditiva e, por fim, a predição[175].

Cumpre destacar, entretanto, outra vertente que estabelece um processo prévio à própria mineração de dados, segundo a qual, os erros mais sérios nos projetos de análise preditiva resultam de uma compreensão deficiente do problema de negócio. Tal entendimento deve ser concebido em conjunto, entre desenvolvedores e especialistas do negócio, definindo objetivos do projeto e os requisitos sob a perspectiva final[176].

Desta forma, as etapas da Análise Preditiva, acima mencionadas, podem ser melhor delineadas a partir do fluxo de trabalho abaixo[177]:

Figura 1 – Fluxograma da Análise Preditiva – MathWorks



Fonte: https://www.mathworks.com/discovery/predictive-analytics.html

Dados

[175] Ibidem, páginas 5, 13, 31.
[176] SHMUELI, G. etall. **Data Mining for Business Analytics - Concepts, Techniques, and Applications in R**. 1 ed. Editora Wiley, 2017. p. 19.
[177] ANÁLISE PREDITIVA. MATHWORKS. Disponível em: <https://www.mathworks.com/discovery/predictive-analytics.html>. Acesso em: 26 set. 2018.

Produzidos rapidamente, em grande quantidade e por diversas fontes, os dados, tanto pessoais quanto profissionais, com ou sem formato padronizado, fazem parte da rotina atual da sociedade.

A título de exemplo, a cada minuto, 3.877.140 pesquisas são realizadas no Google, 4.333.560 vídeos são assistidos no YouTube e 12.986.111 mensagens de texto são encaminhadas[178].

Isoladamente, essa matéria prima representa apenas bytes e mais bytes. Por outro lado, ao ser agrupada e tratada, oferece insumo precioso para qualquer um que tenha seu domínio.

Data Mining

Esta etapa inicia com a coleta ou mineração de dados, de uma ou diversas fontes, sejam elas diferentes sistemas, áreas, setores, tabelas, dentre outros. Quanto mais variada a fonte, mais rica em conteúdo ela será, porém, de baixa qualidade, ou seja, sem padronização que viabilize a utilização imediata e precisa, exigida na criação do Modelo Preditivo[179].

Data Cleaning

Após a reunião dos dados, a informação deve ser explorada e tratada, conferindo integridade à base. Normalmente, tais dados se apresentam em diversos formatos, ou tipos de arquivos, que, embora possam ter uma estrutura interna, não são considerados estruturados, já que não se enquadram perfeitamente em um banco de dados.

Para tal, o processo de limpeza envolve uma inspeção criteriosa, que identifica inconsistências, podendo até mesmo atuar no enriquecimento da base. Alguns exemplos de tratamentos são amparados nas seguintes técnicas: i) manipulação de dados faltantes, seja ela com imputação a partir de análise técnica individual, seja utilizando a média dos outros objetos, ou até mesmo desconsiderando o valor; ii) alteração dos dados existentes, como a codificação de caracteres e conversão de datas; iii) a identificação e remoção dos pontos anômalos ou *outliers*, que prejudicam a interpretação dos resultados[180].

Negligenciar este passo pode comprometer total ou parcialmente as etapas subsequentes da análise de dados. Portanto, recomenda-se que o processo seja conduzido com muita atenção e de forma criteriosa, para que as técnicas de limpeza sejam aplicadas considerando o valor estratégico dos dados trabalhados e o cerne da questão que mobiliza o esforço analítico[181].

Machine Learning e Modelo Preditivo

---

[178] DATA NEVER SLEEPS 6.0. DOMO. Disponível em: <https://www.domo.com/blog/data-never-sleeps-6/>. Acesso em: 26 set. 2018.

[179] DASU, Tamraparni; JOHNSON, Theodore - **Exploratory data mining and data cleaning**. New Jersey: WileyInterscience, 2003. p. 5.

[180] CASTRO, Leandro Nunes de; FERRARI, Daniel Gomes. **Introdução à Mineração de Dados: conceitos básicos, algoritmos e aplicações.** São Paulo: Saraiva, 2016. P55.

[181] UMA VISÃO GERAL SOBRE A LIMPEZA DOS DADOS. INSTITUTO BRASILEIRO DE PESQUISA E ANÁLISE DE DADOS. Disponível em: <https://www.ibpad.com.br/blog/comunicacao-digital/uma-visao-geral-sobre-a-limpeza-dos-dados/>. Acesso em: 26 set. 2018.

Segundo a Nvidia, empresa detentora das GPUs (*GraphicalProcessingUnits*), hardware com melhor processamento voltado para Inteligência Artificial[182], "*Machine Learning*, em sua forma mais básica, é a prática de usar algoritmos para analisar dados, aprender com eles e depois fazer uma determinação ou previsão sobre algo no mundo"[183].

Existem diferentes abordagens capazes de fazer com que as máquinas aprendam e, portanto, criem os modelos preditivos. Vale destacar as três principais categorias[184]:

Supervisionada: Treinamento realizado por meio de exemplos, quando o programa detecta algo, acompanhado de sua definição. A título ilustrativo, a imagem de um cachorro, seguido da sua identificação (*label*).

Não Supervisionada: Neste caso, a aprendizagem ocorre com dados não rotulados, ou seja, o programa identifica padrões nas entradas fornecidas, apenas com base em atributos. Por exemplo, um grupo de clientes que compram produtos frescos, e outro com clientes que compram produtos industrializados.

Por Reforço: Método de programação que gera aprendizado por meio de interação com um ambiente dinâmico, mediante recompensas se executado corretamente ou, punições pelos erros. A título de exemplo, considere-se um carro autônomo "X", que deverá se deslocar do ponto "A" até o ponto "B", no menor tempo possível, sem causar acidentes. Ao analisar o ambiente à sua volta, o referido automóvel decide percorrer um caminho que, embora mais longo, não colidirá com nenhum objeto.

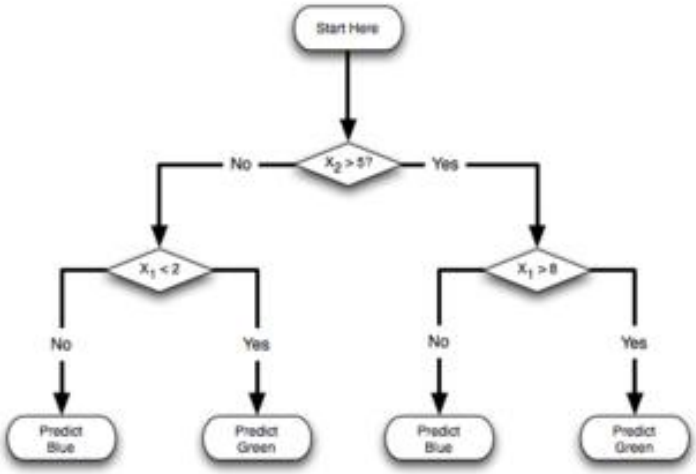
A partir das técnicas mencionadas, surge o produto da *machine learning*, o modelo preditivo. Existem diferentes modelos, desde os simples, tais como as árvores de decisão, até os mais complexos, assim como as redes neurais.

Figura 2 – Modelo Preditivo – Erik Siegel

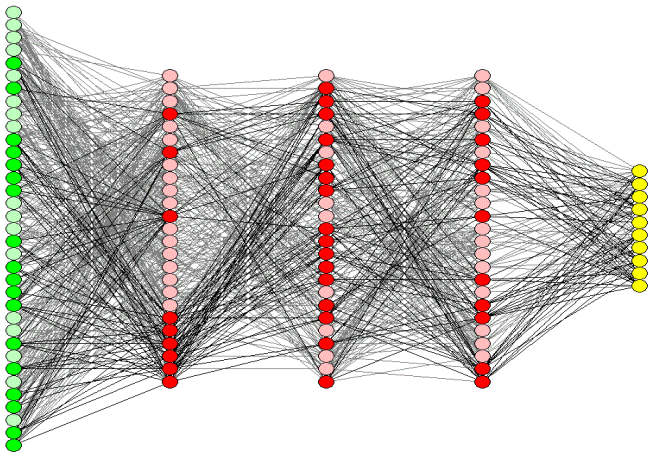
[182] A CULTURA DE STARTUP QUE TRANSFORMOU A NVIDIA EM UMA GIGANTE DO VALE DO SILÍCIO. STARTSE. Disponivel em: <https://startse.com/noticia/cultura-de-startup-que-transformou-nvidia-em-uma-gigante-do-vale-do-silicio/>. Acesso em: 02 out. 2018.

[183] WHAT'S THE DIFFERENCE BETWEEN ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND DEEP LEARNING?. NVIDIA. Disponível em: <https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/> . Acesso em: 02 out. 2018.

[184] WHAT IS MACHINE LEARNING?. TECHEMERGENCE. Disponível em: <https://www.techemergence.com/what-is-machine-learning/>. Acesso em: 02 out. 2018.



Árvore de Decisão



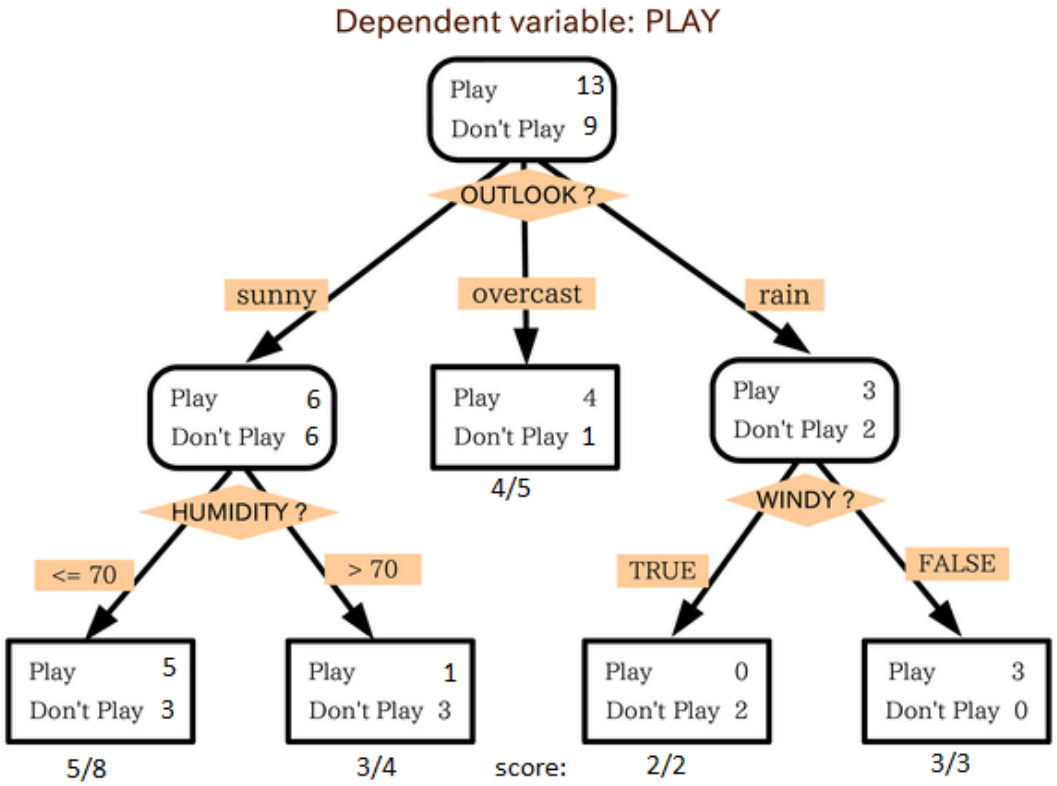
Rede Neural

Fonte: SIEGEL, Eric. Análise Preditiva. Rio de Janeiro: Alta Books, 2017. p. 131

Estes são os mecanismos propriamente ditos, que predizem o comportamento de um indivíduo, como clicar, comprar, mentir ou morrer, nos quais o método matemático aplica as características (variáveis) como entrada e oferece uma pontuação, escore, como saída. Quanto maior o escore, maior a probabilidade de que o indivíduo ou grupo exibirá o comportamento previsto quando submetido ao modelo[185].

Figura 3 – Árvore de decisão – Stack Exchange

[185] SIEGEL, Eric. **Análise Preditiva**. Revisto e Atualizado. Rio de Janeiro: Alta Books, 2017. p. 131.



Fonte:https://stats.stackexchange.com/questions/105760/how-we-can-draw-an-roc-curve-for-decision-trees

Como exemplo, pode-se observar a árvore de decisão acima, bem como a pontuação final desdobrada nas diferentes combinações submetidas aos dados.

2.1. Predições

Após todo o processo de criação do modelo preditivo, bem como sua preparação, o passo seguinte será a aplicação propriamente dita.

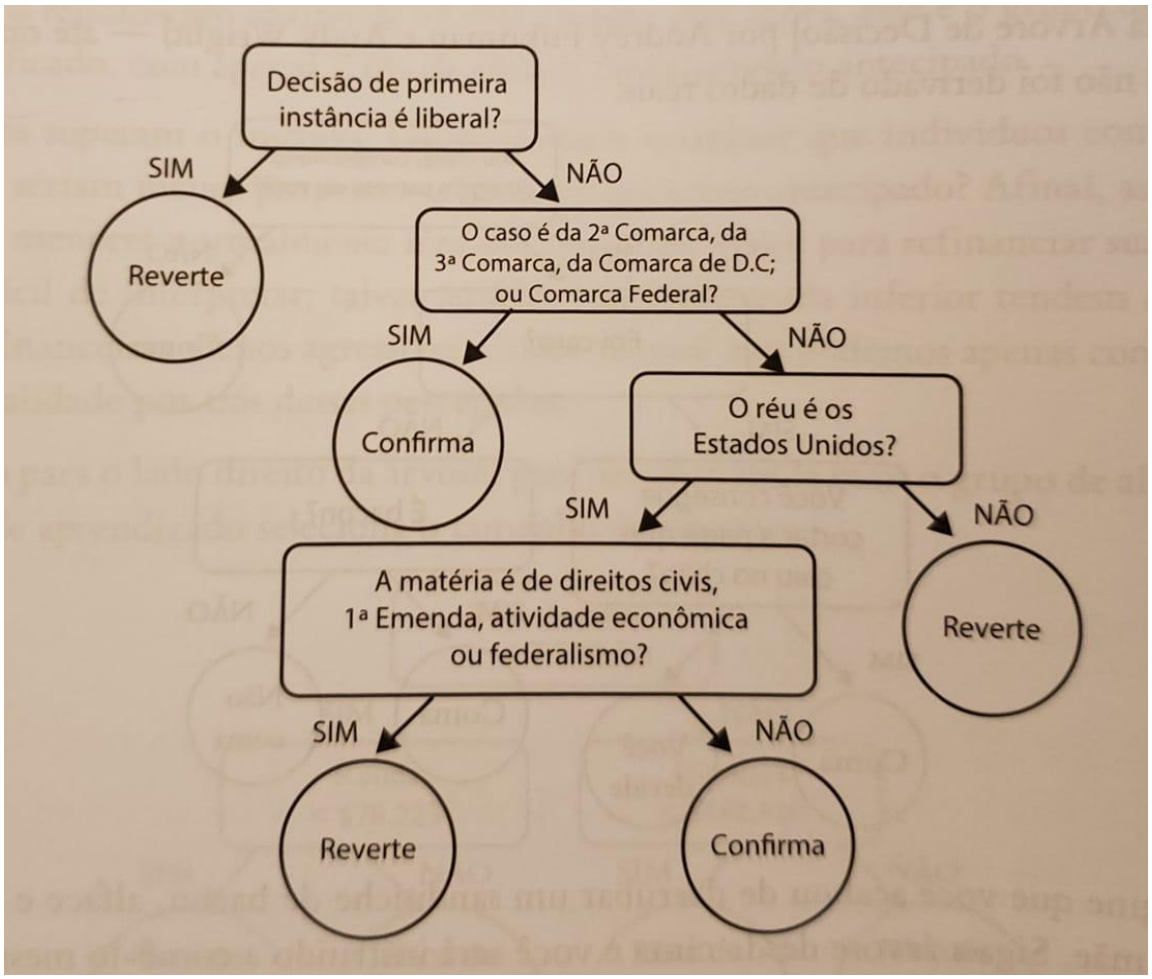
Com ajuda de softwares específicos de desenvolvimento, ou programas integrados a estes, basta carregar ou "rodar" os novos dados ao modelo ou conjunto de modelos criados e obter a predição tão desejada.

Este conjunto de dados passará, por exemplo, pela árvore de decisão e, com base em todo o fluxo, determinará a previsão em percentual ou escore.

A título de exemplo, abaixo se demonstra uma árvore de decisão treinada para prever votos nas decisões de uma ex-juíza da Suprema Corte dos Estados Unidos, Sandra Day O'Connor. A pesquisa, utilizando a referida árvore, superou o desempenho de especialistas na predição das decisões da referida Corte, já que ao aplicar o modelo preditivo, obteve eficiência de 75% na previsão das decisões futuras, enquanto especialistas jurídicos humanos, operaram com apenas 59% de acerto[186].

[186] SIEGEL, Eric. 2017, página 221.

Figura 4 – Árvore de decisão – Erik Siegel



Desta forma, fica evidente o potencial desta nova tecnologia para guiar decisões baseadas em dados, maximizando resultados e obtendo maior assertividade.

3. ANÁLISE PREDITIVA E APLICAÇÕES NO DIREITO

A Análise Preditiva distingue-se do roubo ou do vazamento de dados, porque parte de dados já existentes para a geração de novos dados, cuja predição pode se confirmar ou não. Há uma probabilística envolvida na aplicação concreta da Análise de Dados, uma vez que apresenta uma margem de erro.

> "É a geração de novos dados, a descoberta indireta de verdades oferecidas involuntariamente sobre as pessoas. Organizações prevêem visões poderosas a partir de dados inofensivos existentes, como se tivessem sido criado do nada. Elas estão equipadas para lidar com a sua própria criação?"[187]

A repercussão quanto ao acerto ou erro da predição é que se traduz em aplicação prática para o Direito. Uma predição assertiva pode gerar efeitos positivos ou negativos na esfera individual ou coletiva, tanto quanto uma predição que não se confirmou.

A liberdade do indivíduo pode ser colocada em cheque pela eventual capacidade de a máquina antever determinados comportamentos humanos dentro de um padrão capaz de ser lido.

A forma como os dados navegam pela internet possibilita um alcance a um número infindável de agentes capazes de manipulá-lo. A exposição de dados tornou-se uma preocupação global e clama ao direito uma solução que possibilite uma Análise Preditiva que prescinda da violação dos direitos do cidadão para alcançar à finalidade pretendida.

A questão se torna especialmente complexa ao se deparar com o fato de que o Direito, em especial o Direito Penal, se opera com base no padrão binário "lícito" e "ilícito", a partir da conduta do agente, portanto se não houver conduta, mas sim uma expectativa de conduta (ilícita) prevista com base em determinados padrões comportamentais, como seria o fato punível com uma ação "preventiva" antecipada do Estado? Pode-se dizer que haveria então, no mínimo uma interferência na esfera individual que avançou o espectro da liberdade de agir.

A coleta de dados tem seu valor reconhecido em função da escassez. Quanto mais sigiloso o dado, mais valioso ele é. Quão valioso não seria um dado capaz de prevenir o roubo a um banco ou a uma grande empresa? E qual é o preço que, de fato estamos pagando? Seria a liberdade a moeda de troca para acesso às informações?

> "O valor dos dados – seu poder, seu significado – é justamente aquilo que os torna tão sigilosos. Quanto mais dados, mais poder. Quanto mais poderoso o dado, mais sigiloso. Assim, a tensão que sentimos é inevitável. Se ninguém se importasse com os dados, ninguém tentaria protegê-los e ninguém ia querer acessá-los ou mesmo se preocupar em guardá-los para o começo de conversa"[188].

Como se pode perceber, a Análise de Dados tem potencial para atingir diversas áreas do Direito, considerando a forma como seus dados podem ser obtidos, utilizados e manipulados. Algumas hipóteses de aplicação prática passarão a ser analisadas.

---

[187] SIEGEL, Eric. 2017, página 43.
[188] SIEGEL, Eric. 2017, página 49

3.1 Análise Preditiva e Privacidade

No que diz respeito à esfera da privacidade, Siegel afirma que a Análise Preditiva por si só não invade a privacidade e tampouco ocupa-se de um detalhamento, com a finalidade de espionar os dados do indivíduo. Ao contrário, busca identificar padrões de aprendizado gerados a partir do processamento de grandes quantidades de dados[189].

O que ocorre, de fato, é a transformação de dados, que antes era algo abstrato, em algo concreto, dando significado a um conjunto de informações que isoladamente não produziam sentido.

Todavia, conforme já se mencionou, a Análise Preditiva gera um novo dado, antes inexistente. A exposição do referido dado pode ter repercussão tal, que acabe por violar a esfera da intimidade individual.

A harmonização da Análise Preditiva com o cenário brasileiro deve ser feita tendo-se como base a inviolabilidade da intimidade e da vida privada, prevista no rol de garantias fundamentais do artigo 5º da Constituição Brasileira de 1988 (inciso X).

Em uma leitura conjunta com o inciso XLI do mesmo artigo, percebe-se a atribuição que se faz ao legislador de punir eventual discriminação que a atente aos direitos fundamentais. É nessa medida que a proteção da vida íntima do indivíduo liga-se à noção de liberdade prevista no caput do artigo 5º.

A liberdade, entendida como a capacidade de o indivíduo dirigir a própria vida, não pode ser tolhida pela Análise de Dados, seja pelo risco que a simples coleta do dado possa oferecer, seja pelo resultado que a Análise Preditiva possa gerar, expondo um desejo ou um pensamento não autorizado pelo indivíduo.

A distopia prevista no episódio *Hangg de DJ* da série *Black Mirror* se torna em parte realidade com o aplicativo de relacionamentos Tinder, em sua versão paga, Tinder Gold. A função Picks dentro do aplicativo sugere parceiros e parceiras com bases algorítmicas de preferências pessoais na busca pelo *match* perfeito.

O aplicativo ainda não se arrisca a detalhar quanto tempo o casal permaneceria junto, mas seguramente, haveria aplicação de Análise Preditiva nesse caso de modo a limitar as escolhas pessoais dos indivíduos.

3.2. Análise Preditiva no Direito Penal

A tradicional Escola de Chicago cuidou de examinar o fenômeno da desorganização social na tentativa de compreender melhor a ocorrência dos crimes por meio de métodos estatísticos, considerando, especialmente, o ambiente como fator de criminalidade[190].

As críticas feitas ao modelo são amplamente conhecidas, em especial aos fatores biológico e geográfico como determinísticos para o crime. O biotipo de um ser humano como fator de

[189] Idem, página 51

[190] LAVOR, Isabelle Lucena. A Escola de Chicago: Afinal, o ambiente influencia o comportamento criminoso? Disponível em <https://canalcienciascriminais.com.br/escola-de-chicago/>. Acesso em: 23 set. 2018.

criminalidade ou ainda a localidade onde os crimes reincidem em maior volume são verdadeiras excrescências na análise da criminalidade.

O uso de Análise Preditiva no âmbito criminal deve partilhar das mesmas preocupações ao utilizar, por exemplo, um dado de etnia na composição do algoritmo.

Neste campo parece haver, de fato, um choque entre o que se entende por Análise Preditiva e Determinismo. A Análise Preditiva, entendida como elemento utilizado para tomada de decisão, assume um caráter objetivo, pois parte da análise de dados concretos e históricos. Embora os dados tenham razoável confiabilidade, tentar prever a taxa de reincidência de um criminoso parece estar fora do alcance da Análise Preditiva, pois atinge o âmago da subjetividade humana.

Considerar a Análise Preditiva para tomar ações preventivas frente ao indivíduo, sem que este tenha realizado qualquer conduta delituosa, importa em violação indevida à sua liberdade.

É preciso lembrar que a Análise Preditiva, ao final, é um modelo probabilístico. Uma das principais críticas feitas à Escola de Chicago foi o fato de trabalhar apenas com os dados registrados, concentrando-se sobre as ocorrências de violação de direito com registro nas delegacias. A mesma crítica, em alguma medida pode ser feita à Análise de Dados no que tange à sua utilização em relação à criminalidade.

As teorias ecológicas de Robert Park e Ernest Burguess que fizeram análise das zonas concêntricas nas zonas imigratórias denominadas *chinatown* e *littleitaly,* receberam críticas ao tornar evidente a impossibilidade de comparação entre as zonas sugeridas no modelo, pelo simples fato de os agentes estarem concentrados nas zonas 1 e 2 (zonas com maior nível de desorganização social). O reflexo estatístico é bastante simples, os dados produzidos estatisticamente sempre serão maiores naquelas regiões consideradas anômalas.

Análise Preditiva parte de um modelo estatístico associado ao aprendizado da máquina para tentar predizer eventos futuros. Logo, seu aprendizado se torna limitado, na medida em que as estatísticas se revelem incompletas, podendo levar à conclusões incondizentes com a realidade concreta no mundo da criminalidade.

A Análise Preditiva é sim um instrumento de combate à criminalidade, todavia, é preciso compreender que a seletividade por traz da coleta de dados acaba sendo elemento que pode passar a compor o espírito da máquina de tal forma que ela passe a reproduzir o comportamento subjetivo humano limitado em suas crenças.

É por isso que a sua utilização como instrumento de combate ao crime é possível e de grande importância, mas sob a ótica de instrumento auxiliar, evitando a punição do agente apenas pela expectativa da ocorrência de um crime.

3.2.1. Casos Práticos - Predição de Crimes – Policiamento Preditivo

Na cidade de Santa Cruz, Califórnia, a utilização de análise preditiva conseguiu prever corretamente os locais de 25% dos furtos. Hoje esse sistema orienta o patrulhamento, informando todos os dias dez locais de alta probabilidade de ocorrência de crimes para onde envia os carros de polícia. Essa iniciativa foi premiada pela revista Time como uma das melhores invenções de 2011.

Outro sistema semelhante foi implementado em Richmond, Virgínia, que abastece um monitor de combate ao crime que assinala um mapa com o risco de crime iminente e lista as delegacias, vizinhanças e tipos de crime por nível de risco. Sistemas similares também estão sendo

desenvolvidos em Chicago, Los Angeles, Vineland, Nova Jersey e Memphis, onde a análise preditiva é responsável pela redução de crimes em 31%[191].

Nesses casos a partir de dados passados sobre o cometimento de crimes, foi possível direcionar o patrulhamento para as áreas de maior incidência, a fim de prevenir novas ocorrências.

3.2.2. Casos Práticos - Predição de Reincidência na aplicação da Lei

No Estado do Oregon, com o objetivo de tentar prever se algum criminoso reincidirá, o aprendizado de máquina criou um modelo de análise preditiva a partir do processamento de registros de 55 mil criminosos em cinco anos de dados. O modelo foi validado com 350 mil registros de criminosos em 30 anos de história. Entre os 10% de criminosos de menor risco (com escores mais baixos previstos pelo sistema), a reincidência é de apenas 20%. E, entre os 20% que receberam os maiores escores, há uma grande probabilidade de reincidência[192].

3.2.3. Casos Práticos - Predição para aumento da pena

No Estado de Wisconsin, um Juiz definiu o patamar da pena de um réu, condenado por furto e por se envolver em um tiroteio após um acidente de trânsito, que possuía uma condenação anterior por delito de agressão sexual, a partir de um algoritmo gerado por um software privado, denominado COMPAS (Correctional Offender Management Profiling for AlternativeSanctions), que funciona a partir de um algoritmo secreto, ao qual nem os juízes que o utilizam têm acesso.

Segundo esse algoritmo, o réu representaria alto risco de reincidência, violência e evasão.

O advogado do réu questionou a utilização desse algoritmo e pediu para ter acesso aos critérios que levaram o software a chegar a essa conclusão.

Durante o julgamento, algumas questões sensíveis foram levantadas, como o relatório da ONG ProPublica, sobre a utilização do software contra afro-americanos.

O pedido da defesa do réu foi negado pela Suprema Corte de Winsconsin, sob o argumento de que ele teria recebido a mesma sentença a partir de uma análise humana dos fatores usuais: seu crime e seus antecedentes.

A Suprema Corte Americana também negou o pleito defensivo e o réu permanecerá preso até 2019 [193].

---

[191] SIEGEL, Eric. **Análise Preditiva**. Revisto e atualizado. Rio de Janeiro: Alta Books, 2017. p. 59.
[192] Idem, página 67.
[193] FERRARI, Isabela; BECKER, Daniel e WOLKART, Erick Navarro. **ARBITRIUM EX MACHINA: PANORAMA, RISCOS E A NECESSIDADE DE REGULAÇÃO DAS DECISÕES INFORMADAS POR ALGORITMOS**. RT, São Paulo, v. 107, n. 995, p. 635-655, set. 2018.

4. ANÁLISE PREDITIVA E O SIGILO DE EMPRESA

A utilização da Análise Preditiva para prever o comportamento de determinada ação na Bolsa de Valores não aparenta nenhuma estranheza sob uma ótica superficial.

Porém, uma questão que pode gerar polêmica neste caso é a forma de obtenção dos dados utilizados na análise. A forma como as máquinas são configuradas para aprender a coletar dados de forma não supervisionada pode possibilitar uma conclusão que invariavelmente caracterizaria fraude ou espionagem industrial.

Assim como o roubo de informações pode ser mascarado pelo argumento de utilização da máquina para se chegar a uma eventual conclusão mirabolante, o contrário também pode ser verdadeiro.

A ausência da possibilidade de se conseguir explicar a decorrência lógica que levou à máquina à determinada conclusão torna bastante complexo esse cenário.

Uma informação privilegiada obtida com base no resultado de uma Análise Preditiva poderia ser instrumento para ensejar a responsabilidade daquilo que não poderia ou não deveria ser predito para fins de se configurar concorrência desleal? Se é possível identificar que grampeadores são sinal de uma nova contratação[194], quando mais a solvência de uma empresa, ou o lançamento de um novo produto.

Se a ausência de limites para a coleta de dados dos indivíduos implica em violação da sua esfera individual, também pode implicar em violação a dados de sigilo empresarial, vez que os indivíduos carregam tais dados consigo.

A assimetria informacional capaz de ser implementada pelo uso de Análise Preditiva no meio empresarial pode, ao final, tornar o mercado menos eficiente nas transações em que uma das partes fizer uso de Análise Preditiva e outra não, vez que, a parte detentora da informação seria capaz de contornar os custos de transação da negociação fazendo uso da informação obtida a seu favor.

[194] SIEGEL, Eric. **Análise Preditiva**. Revisto e atualizado. Rio de Janeiro: Alta Books, 2017. p. 99.

5. ANÁLISE PREDITIVA E O SEGREDO DE ESTADO

As conclusões à que chegou o Estado brasileiro após as revelações feitas por Edward Snowden em 2013 foram de que, de fato, houve monitoramento de cidadãos brasileiros pela Agência de Segurança Nacional dos Estados Unidos da América (NSA). A justificativa para tanto seria o combate ao terrorismo. Postas as críticas dos apoiadores da NSA e dos defensores da privacidade, Siegel (2017, p. 75) conclui que:

> "Ambos os lados não conseguem lidar com o que está realmente em questão para as autoridades judiciárias: os dados possibilitam não apenas a investigação de suspeitos já conhecidos, mas também a descoberta de novos suspeitos"[195].

Isto, segundo o autor, decorreria do que intitula *Descoberta Automática de Suspeitos (DAS).* A partir dos dados coletados e fazendo uso da Análise Preditiva, a inteligência dos EUA conseguia identificar suspeitos não apontados com os dados primários.

Todavia a NSA não conseguiu explicar adequadamente a investigação das autoridades brasileiras, como a presidenta Dilma Rousseff e seus assessores, e negou uma possível utilização dos dados obtidos ilicitamente da Petrobrás nas aquisições relativas ao pré-sal.

Veja-se que a informação que era de sigilo do governo brasileiro ou de empresa brasileira, assumiu o caráter de segredo de Estado perante o governo estadunidense. Dados passam a ter um valor inestimável a partir do seu potencial uso em combinação com outros no uso da Análise Preditiva.

Em maio de 2018 a SERPRO, Serviço Federal de Processamento de Dados, foi acusada pelo Ministério Público Federal de comercializar dados de cidadãos brasileiros constantes na base de Receita Federal[196].

A obtenção e utilização de dados de um governo ou para determinado governo são de absoluta relevância no uso de Análise Preditiva. Assim, cabe ao direito a prescrição de regras que, de um lado possibilitem a análise de tendências, mas que, de outro, inviabilize a invasão da privacidade do indivíduo.

---

[195] Idem, página 75.

[196] Ofício nº20/2018 – CPDP – MPDFT. Acessado em 30 set. 2018. Disponível em:<https://www.conjur.com.br/dl/oficio-mpf-base-dados.pdf>

6. ANÁLISE PREDITIVA E LEI GERAL DE PROTEÇÃO DE DADOS

A Lei nº 13.709/2018, que recentemente foi publicada (dia 14/08/2018), entra em vigor em 24 (vinte e quatro) meses a partir da sua data de publicação, conforme alterado pela Medida Provisória nº 869 de 2018. Essa Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa física ou pessoa jurídica de direito privado ou público, tendo como objetivo a proteção dos direitos de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A proteção de dados pessoais tem como fundamentos o direito à privacidade, a intimidade, a dignidade da pessoa humana, a liberdade de expressão, de informação, da honra e da imagem, o desenvolvimento econômico e tecnológico, a inovação, dentre outros. Ou seja, ela é uma Lei que protege os dados pessoais, honrando os princípios da privacidade, intimidade, dignidade da pessoa humana, mas por outro lado, também quer desenvolver e regulamentar o desenvolvimento tecnológico e a inovação.

Para que se possa entender os pontos principais e críticos desta Lei para depois os contrastar com a Análise Preditiva (AP), importante que se conceitue ao que e a quem a Lei se aplica.

A LGPD, como é vulgarmente chamada aplica-se a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica (de direito privado ou público), independendo do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que alguns requisitos sejam cumpridos.

Os requisitos são os seguintes: que a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional e que os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Entretanto, já surgem algumas dúvidas decorrentes desses requisitos, que os parágrafos do artigo 3º vem elucidar. Consideram-se "coletados no território nacional" os dados pessoais cujo titular nele se encontre no momento da coleta.

Quanto a não aplicação da Lei, temos que a LGPD não se aplicará ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, e aquele tratamento realizado para fins exclusivamente jornalístico e artísticos ou acadêmicos, de segurança pública, defesa nacional, segurança de Estado, ou atividades de investigação e repressão de infrações penais ou aquelas provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.[197]

Para uma compreensão correta da Lei, necessário também que se conceitue alguns tipos de dados e agentes que a Lei cita, para facilitar a visualização desses conceitos, cria-se a tabela abaixo:

[197] BRASIL. LEI Nº 13.709, 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).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 26 set. 2018.

Conceito	Significado
dado pessoal 	informação relacionada a pessoa natural identificada ou identificável
dado pessoal sensível	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;
Dado anonimizado 	dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
banco de dados	conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico
Titular	pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Controlador 	pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
operador	pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoas em nome do controlador
encarregado	pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o

	controlador e os titulares e a autoridade nacional;
agentes de tratamento	o controlador e o operador
Tratamento	toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração[198]

Entendidos esses conceitos básicos que a Lei traz, passa-se agora à análise da LGPD quando em contraste com a análise preditiva.

A LGPD seguiu os moldes da Lei da União Europeia e veio para regulamentar a proteção de dados no Brasil, algo que vai ser de muito valor para a economia digital e para os titulares de dados, gerando segurança jurídica.

Como já exposto acima, a análise preditiva é a tecnologia que aprende a partir de dados para prever comportamentos futuros de indivíduos, empresas, e outros entes organizacionais, a fim de gerar melhores decisões.[199]

Entretanto, a proteção de dados está de um lado e a análise preditiva de outro, pois a para a AP existir deve haver um volume muito grande de dados. Em muitos exemplos estudados, ela é bem duvidosa, invadindo a personalidade humana, características pessoais ou empresariais bem delicadas.

Vários casos relatados no livro de Eric Siegel exemplificam como a análise preditiva pode ser invasiva e gerar problemas, e até danos morais ao indivíduo. Um dos exemplos é o case da Target, no qual uma menina que estava grávida (mas sua família ainda não sabia) acabou surpreendida em sua casa por uma correspondência da rede americana de varejo, parabenizando-a pela gravidez, sendo que a moça nem havia contado para seus pais.

Como a Target descobriu isso? Clarividência? Chute? Não! Análise preditiva! Eles analisaram inúmeros dados de consumidoras grávidas, seus históricos de compras, quais produtos uma grávida compra no início/descoberta da gravidez, e aplicando a análise preditiva, "descobriram" a gravidez dessa menina.

Aí vem a polêmica: esses dados são sensíveis? Com certeza. São íntimos? Também. Porém, em uma análise nua e crua, são dados que a Target tem acesso e pode usá-los. Aí que a LGPD entraria

[198] BRASIL. LEI Nº 13.709, 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).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 14 mar. 2019

[199] SIEGEL, Eric. Análise Preditiva: Alta Books, 2017. Pg. 13.

regulamentando de que forma a empresa poderia utilizar os dados do cliente, quais os limites para esse uso.

Com a entrada em vigor da Lei, as empresas públicas e privadas precisarão do consentimento dos seus clientes para coletar e usar os seus dados pessoais, além de ter que dar a opção de visualização, correção e exclusão de determinados dados. Isso de alguma forma poderia prejudicar as aplicações da AP no âmbito das empresas, pois elas não teriam a quantidade/qualidade de dados, para aplicar os modelos preditivos e chegar em conclusões, para a tomada de decisões, ações de *marketing*, entre outros.

Como a pesquisa feita neste artigo refere-se à "Análise Preditiva de Dados e suas Aplicações no Direito", importante ressaltar que além das opções de implantação para análise de dados de clientes de escritórios para melhor oferta de produtos e serviços, soluções a clientes corporativos, os advogados comercialistas terão um grande trabalho: em elucidar os pontos da LGPD, bem como indicar aos seus clientes como implantar os novos regramentos que a Lei traz.

Esse será um trabalho que os advogados terão de fazer (ou farão de forma mais adequada e aplicada ao cliente) em conjunto com cientistas da computação, programadores, profissionais da área da segurança da informação, pois são estes que conhecem tecnicamente as formas e estratégias de proteger os dados. Porém, não pode haver uma orientação técnica sem o respaldo jurídico, que vai ser necessário. Dessa forma, os juristas deverão se debruçar sobre a Lei e estudá-la a fundo, para orientarem seus clientes do melhor modo.

Também como aplicação da AP no direito, podemos citar os aplicativos que se revestem na forma de *lawtechs* (termo utilizado para denominar *startups* jurídicas que oferecem novas ideias, em forma de produto ou serviço, que buscam aprimorar e resolver os principais problemas do universo jurídico)[200] que utilizam da análise preditiva para prever comportamentos futuros de clientes de escritórios, de juízes que vão julgar as causas de seus clientes, e mais inúmeras soluções e predições que auxiliariam os advogados na condução de seus processos e trabalhos.

Tendo em vista o disposto acima sobre a LGPD e a Análise Preditiva, imagina-se que com a entrada em vigor da Lei, será restringido o campo de atuação da Análise Preditiva pelas instituições de forma geral, principalmente pelas empresas, que não vão poder dispor e utilizar dos dados de seus clientes de forma tão livre para fins de *marketing*, por exemplo.

[200]CÂMARA, Isabella. **Lawtech: o que é e como está o mercado para essas startups?** Disponível em: <https://startse.com/noticia/o-que-e-lawtech>. Acesso em: 27 de setembro de 2018.

7. CONSIDERAÇÕES FINAIS

A partir do estudo realizado verifica-se possível esboçar as seguintes considerações: 1. A Análise Preditiva com base em Análise de Dados já ocorre há algum tempo e o legislador, tardiamente busca regular tão somente a proteção de dados pessoais, ficando as demais aplicações à margem da proteção legal; 2. O uso de Inteligência Artificial em Análise de Dados se verifica como tendência. Sua aplicação já ocorre na prática, todavia, o desenvolvimento da tecnologia tende a aprimorar a técnica em assertividade a partir do machine learning; 3. A Análise de Dados possuí inúmeras aplicações, ora em uso benéfico para a sociedade, ora em uso não benéfico. Entende-se que a Constituição atribuiu ao legislador o dever de regular a matéria em relação à proteção da intimidade e da privacidade. Nas demais aplicações da Análise de Dados, caberá ao operador do Direito o esforço por adotar as ferramentas já existentes para prevenir o uso abusivo do instrumento.

8. REFERÊNCIAS

Análise Preditiva Mathworks. Disponível em: <https://www.mathworks.com /discovery/predictive-analytics.html>. Acesso em: 26 set. 2018.

BRASIL. LEI Nº 13.709, 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). Disponível em: <http://www.planalto.gov.br/ccivil_03 /_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 26 set. 2018

DATA NEVER SLEEPS 6.0. DOMO. Disponível em: <https://www.domo.com/blog/data-never-sleeps-6/>. Acesso em: 26 set. 2018

FERRARI, Isabela;BECKER, Daniel e WOLKART, Erick Navarro. **Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos**. RT, São Paulo, v. 107, n. 995, p. 635-655, set. 2018.

CÂMARA, Isabella. **Lawtech: o que é e como está o mercado para essas startups?** Disponível em: <https://startse.com/noticia/o-que-e-lawtech>. Acesso em: 27 de setembro de 2018.

Ofício nº20/2018 – CPDP – MPDFT. Acessado em 30 set. 2018. Disponível em: <https://www.conjur.com.br/dl/oficio-mpf-base-dados.pdf>

RICHE., **Artificial Intelligence**, McGraw-Hill, N.Y., 1983.

SHMUELI, G. et all. **Data Mining for Business Analytics** - Concepts, Techniques, andApplications in R. 1 ed. Editora Wiley, 2017. p. 19.

SIEGEL, Eric – **AI, Machine Learning, and the Basics of Predictive Analytics for Process Management,** Agosto de 2018. Disponível em: <https://www.predictiveanalyticsworld.com/patimes/ai-machine-learning-and-the-basics-of-predictive-analytics-for-process-management/9632/> Acessado em 23/09/2018

SIEGEL, Eric. **Análise Preditiva**. Revisto e Atualizado. Alta Books. 2017.

INTELIGÊNCIA ARTIFICIAL E O DIREITO: CASES ATUAIS E CENÁRIOS FUTUROS

GUILHERME HIDEO OSHIMA

Pesquisador do Núcleo de Estudos em Direito Civil-Constitucional da UFPR ("Virada de Copérnico"). Pós-graduando em Direito Imobiliário pela Universidade Positivo. Membro da Câmara de Inovação e Tecnologia do Instituto de Engenharia do Paraná.

STEFANO ÁVILA PAVAN

Pós-graduando em Direito Constitucional pela ABDCONST. Membro da Comissão de Inovação e Gestão da OAB/PR. Advogado.

RESUMO:
A evolução da inteligência artificial impacta de forma cada vez mais intensa e abrangente as relações sociais e econômicas, sendo certo que o Direito também será afetado, de modo que mudanças massivas na prática da advocacia acontecerão, com impactos ainda incertos sobre o mercado de trabalho. Nesse sentido, o presente artigo busca apresentar algumas soluções já existentes no contexto brasileiro e americano, de impactos da inteligência artificial no Direito de forma geral e no trabalho dos advogados em específico. Ainda, são apresentados alguns cenários hipotéticos de evolução com reflexões sobre o impacto da tecnologia no Direito a longo prazo, através da análise dos fenômenos da computação quântica e do transhumanismo.

Palavras chave: Inteligência artificial; Advocacia. Integração; Direito e tecnologia.

1. INTRODUÇÃO

A escalada de novas tecnologias coloca em xeque diversas concepções sobre a organização do mercado de trabalho e da sociedade como um todo. O receio de que o avanço da automação pudesse gerar desemprego massivo existe desde o séc. XIX, mas de fato nunca se materializou, e sempre esteve restrito às áreas que envolviam atividades mecânicas e repetitivas.

No entanto, à medida que a máquina passa a desenvolver progressivamente atividades de capacidade cognitiva, por meio da inteligência artificial (IA) e suas ramificações, tais como *machine learning*, *natural language processing (NLP)*, etc., há que se questionar sobre os reais impactos desta nova revolução, isto é, as consequências da Indústria 4.0. Ademais, repercutiriam estes efeitos na seara dos serviços jurídicos?

Nesse sentido, descreve Yuval Noah Harari:

> É crucial entender que a revolução da IA não envolve apenas tornar os computadores mais rápidos e mais inteligentes. Ela se abastece de avanços nas ciências da vida e nas ciências sociais também. Quanto mais compreendemos os mecanismos bioquímicos que sustentam as emoções, os desejos e as escolhas humanas, melhores podem se tornar os computadores na análise do comportamento humano, na previsão de decisões humanas, e na substituição de motoristas, profissionais de finanças e advogados humanos.[201]

Seria simplesmente impensável conceber a IA como um possível motor de mudança em diversas áreas da economia e sociedade e não a relacionar da mesma forma à advocacia e a prática do Direito.

Certamente, tanto a implementação de soluções em IA para as profissões jurídicas como as implicações jurídicas do uso da IA nas diversas relações econômicas e sociais exige repensar o ensino[202] do Direito de forma mais holística e interdisciplinar, englobando áreas que poderiam parecer até estranhas a um advogado, como por exemplo, a ciência da computação. Refletir sobre o impacto da IA e das demais tecnologias sobre a sociedade é imprescindível e criar modelos regulatórios que maximizem seus impactos positivos é urgente.

Sendo assim, o presente artigo busca trabalhar alguns casos de utilização, bem como impactos da IA na advocacia e no Direito já existentes, e quais os possíveis paradigmas para o futuro das profissões jurídicas.

Para tanto, primeiramente, apresentar-se-á o panorama atual envolvendo a aplicação de novas tecnologias, em especial, a inteligência artificial no cenário jurídico, nos segmentos da advocacia, Administração Pública e Poder Judiciário. Em sequência, demonstrar-se-á as tecnologias emergentes e futuras do mercado, bem como seus possíveis impactos no Direito.

I. Cases atuais

---

[201] HARARI, Yuval Noah. 21 lições para o século 21 / Yuval Noah Harari ; tradução Paulo Geiger. — 1a ed. — São Paulo : Companhia das Letras, 2018. Pg. 41.

[202] MARANHÃO, Juliano. A inteligência artificial e o ensino do direito. JOTA, 19 de dez. 2017. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/inteligencia-artificial-e-o-ensino-do-direito-19122017 >. Acesso em: 25 de outubro de 2018.

Novas plataformas e tecnologias emergentes no mercado desafiam a concepção de que a atividade da advocacia - e porque não das profissões jurídicas como um todo - são intrinsecamente humanas. Certamente, o incremento da IA no direito influenciará de formas ainda não inteiramente compreendidas, a maneira de se praticar a advocacia.

Nessa esteira, sob a perspectiva de áreas como a bancária[203], logística e medicina[204], o exercício de atividades consideradas de desempenho exclusivamente humano, foram automatizadas, acarretando não somente na redução de custos, como também resultados de maior precisão e acurácia[205].

Desse modo, a absorção da tecnologia pelo mercado, demonstra-se ferramenta efetiva para tomada de decisões, gerenciamento de risco e gestão do negócio, conceitos e práticas já importados e constantemente remodelados ao cenário jurídico tecnológico, como será demonstrado a seguir.

Se de um lado, há grande potencial quanto a automatização de determinadas tarefas, por outro, isso não necessariamente implicará na substituição de advogados por máquinas, e sim na exigência de que esses busquem se capacitar cada vez mais com relação as novas tecnologias, além de dedicar seu tempo às atividades mais complexas[206], as quais, pelo menos no curto e médio prazo, ainda não foram assumidas por algoritmos.

Os usos da inteligência artificial são variados e se distinguem tanto pelos impactos legais da IA em diversas áreas da sociedade, como pelo uso destas em tarefas jurídicas, criando novas formas de se trabalhar com o direito e novos campos de atuação para os profissionais que se disponham a pesquisá-los.

Preliminarmente ao debate sobre as ferramentas jurídicas e inovadoras disponíveis atualmente no mercado, em virtude da urgente necessidade do profissional do Direito absorver e compreender a tecnologia, cumpre elucidar e demonstrar o porquê o *machine learning* e a *natural language processing* (NLP), ramos da inteligência artificial, desempenham um papel elementar nesta revolução tecnológica.

O *machine learning* é uma técnica de análise preditiva, por meio da análise de uma grande quantidade de dados[207]. Destaca-se a desnecessidade de reprogramação, cabendo à própria máquina o desenvolvimento de algoritmos para a reprodução de resultados confiáveis e

---

[203] A BIA (Bradesco Inteligência Artificial), desenvolvida pelo Banco Bradesco em parceria com a IBM é capaz de providenciar a consulta do saldo bancário e pagamento de contas. Disponível em: http://banco.bradesco/html/classic/promocoes/bia/ e https://exame.abril.com.br/tecnologia/bradesco-usa-inteligencia-artificial-no-atendimento-a-clientes/

[204] O ADAM Robô é capaz de fazer um pré-diagnóstico rápido e preciso da saúde dos olhos. Pauta-se na utilização de técnicas de inteligência artificial para detecção de cataratas. Disponível em: http://www.adamrobo.com.br/home/ e https://epocanegocios.globo.com/Tecnologia/noticia/2018/08/robo-brasileiro-usa-inteligencia-artificial-para-testes-de-vista-e-deteccao-de-catarata.html.

[205] ALARIE, Benjamin; NIBLETT, Anthony and YOON, Albert. How Artificial Intelligence Will Affect the Practice of Law. University of Toronto Law Journal, v. 68, jan. 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.3066816. p. 02.

[206] LOHR, Steve. A.I. Is Doing Legal Work. But It Won't Replace Lawyers, Yet. New York Times. 03 mar. 2017. Disponível em: <https://www.nytimes.com/2017/03/19/technology/lawyers-artificial-intelligence.html?_r=0>. Acesso em: 25 de outubro de 2018.

[207] ALARIE, Benjamin; NIBLETT, Anthony and YOON, Albert. *op. cit.* P. 9.

repetitivos[208]. Deste método, pode-se inferir, por exemplo, a análise da repercussão geral de recursos.

Já o *natural language processing* (NLP) remete-se a competência da máquina em estabelecer conexões e a relevância entre palavras ou frases em um determinado contexto[209]. Nesse contexto, o NLP é o poder da máquina em identificar e extrair informações de arquivos e documentos[210].

Tendo em vista o potencial destes mecanismos, nota-se a capacidade e a inegável direção da tecnologia em aprimorar e reinventar as profissões jurídicas. É sob este contexto que, em seguida, serão apresentadas as principais e emergentes ferramentas pautadas em IA que auxiliarão os segmentos da advocacia e o Poder Judiciário, bem como as consequências de suas adoções.

A. Advocacia

A basilar e essencial atualização e inovação do departamento jurídico, além de representar uma economia na gestão interna do escritório, é acompanhada da indispensabilidade em fornecer ao cliente uma previsibilidade de custos, celeridade e *expertise* profissional e a constante necessidade do advogado em acompanhar o contexto legislativo e jurisprudencial[211].

Em que pese, a prestação de consultoria, redação de pareceres, negociações e participações em audiências, por enquanto, ainda se demonstrarem inalcançáveis de realização autônoma pela computação[212], a inteligência artificial já demonstra-se capaz em auxiliar nestas tarefas, bem como ser ferramenta para substituir trabalhos anteriormente considerados exclusivos de humanos.

Softwares de IA podem providenciar soluções específicas em determinado caso, oferecer recomendações e planejamento de atuação estratégica, *checklists* para assessoria em *compliance* e governança corporativa e elaborar modelos de petições, com base nas informações da demanda[213].

Dessa forma, as ferramentas de auxílio delineadas em inteligência artificial podem ser designadas em cinco grandes áreas: (*i*) pesquisa legal, (*ii*) *e-discovery*/ produção probatória (*iii*) predição de resultados, (*iv*) análise e geração de contratos ou documentos jurídicos em geral e (*v*) gestão legal.

A divisão adotada não é estanque e não exclui outros campos de aplicação para a IA na advocacia, que porventura possam assumir maior protagonismo no mercado das *lawtechs* e *legaltechs*. Por fim, cabe ressaltar que tais ferramentas não se excluem da apreciação e utilização pelo Poder Judiciário e Administração Pública.

---

[208] ASSUNÇÃO, Luis. MACHINE LEARNING, BIG DATA E INTELIGÊNCIA ARTIFICIAL: qual o benefício para empresas e aplicações no direito? 11 dez. 2017. Disponível em: <https://www.ab2l.org.br/machine-learning-big-data-e-inteligencia-artificial-qual-o-beneficio-para-empresas-e-aplicacoes-no-direito/>. Acesso em: 25 de outubro de 2018.

[209] ALARIE, Benjamin; NIBLETT, Anthony and YOON, Albert. *op. cit.* P. 8.

[210] ALARIE, Benjamin; NIBLETT, Anthony and YOON, Albert. *Op. Cit.* P. 9.

[211] ALARIE, Benjamin; NIBLETT, Anthony and YOON, Albert. *Op. Cit.* P. 5-7.

[212] LOHR, Steve. A.I. Is Doing Legal Work. But It Won't Replace Lawyers, Yet. New York Times. 03 mar. 2017. Disponível em: <https://www.nytimes.com/2017/03/19/technology/lawyers-artificial-intelligence.html?_r=0>. Acesso em: 25 de outubro de 2018.

[213] KRAUSOVÁ, Alžbeta. Intersections between Law and Artificial Intelligence. International Journal of Computer (IJC), Vol. 27, nº 01, 2017. Disponível em: http://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1071/464 p. 56-57

1. Pesquisa Jurídica

A pesquisa jurídica não é um serviço inédito, sendo disponibilizada de forma gratuita a pesquisa de jurisprudência nos portais de todos os tribunais brasileiros e algumas plataformas comerciais.

O desafio (e diferencial) abordado pelas tecnologias de pesquisa legal baseadas em IA está na utilização de tecnologias de processamento de linguagem natural para construir sistemas de "pesquisa legal inteligente", que permitam a comparação entre resultados de casos, busca precisa por termos em sentido contextual e pragmático, vinculados à prática efetiva e não apenas sintático. Exemplos deste tipo de serviço são o casetext[214], Digesto[215], e o ROSS[216].

2. E-discovery

O *discovery* remete-se ao processo de revelação de provas e dados relacionados à elucidação de determinado caso. Para tanto, "o advogado de uma das partes pode, caso lhe interesse, coletar as provas a serem utilizadas e tem acesso às provas eventualmente obtidas pela parte contrária e que podem ser utilizadas no processo"[217].

Nesse contexto, o *eletronic discovery* (*e-discovery*) é um desdobramento deste processo, especificamente delineado para identificar dados e informações eletrônicas (*electronically stored information*).

No intuito de aprimorar a efetividade das atividades no âmbito do *e-discovery*, programas denominados *predictive coding* pautam-se em na combinação de técnicas de *machine learning* e algoritmos para a identificação de documentos relevantes para cada caso[218].

Desta maneira, o advogado é responsável por alimentar dados e ensinar a máquina, demonstrando o grau de relevância de determinado documento, bem como instruindo a máquina a organizá-los por grau de importância e de conteúdo[219].

Precedentes dos tribunais americanos atestam a confiabilidade na ferramenta do *predictive coding*[220]. No entanto, a *Court of Chancery*, do estado de Delaware (EUA), destacou que, nos casos

---

[214] CASE TEXT. Disponível em: <https://casetext.com/ >. Acesso em: 25 de outubro de 2018.
[215] DIGESTO. . Disponível em: <https://www.digesto.com.br/ >. Acesso em: 25 de outubro de 2018.
[216] ROSS. Disponível em: <https://rossintelligence.com/ross/>. Acesso em 25 de outubro de 2018.
[217] CAMBI, Eduardo. Discovery no processo civil norte-americano e efetividade da justiça brasileira. Revista de Processo. v. 245, Julho 2015. Disponível em: < http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RPro_n.245.16.PDF>. Acesso em: 10 de novembro de 2018.
[218] HAMPTON, Wallis M. Predictive Coding: It's Here to Stay. E-Discovery Bulletin, June/ July, 2014. Disponível em: < https://www.skadden.com/insights/publications/2014/06/predictive-coding-its-here-to-stay>. p. 29. Acesso em: 28 de outubro de 2018.
[219] *Ibid*. p. 29.
[220] Acerca do e-discovery e precedentes nos Tribunais Americanos, destacam-se os casos: *Moore v. Publicis Groupe; National Day Laborer Organizing Network v. US Immigration & Customs Enforcement Agency; Hinterberger v. Catholic Health Sys., Inc.; Global AeroSpace Inc. v. Landow Aviation, L.P.*

envolvendo a análise de uma pequena quantidade de documentos, não é financeiramente/ economicamente justificável a aplicação de *predictive coding*[221].

Apesar de demonstrar-se como um processo efetivo para a economia de tempo e dinheiro, a ferramenta do *predictive coding* ainda enfrenta desafios como a vistoria efetiva de conteúdos como vídeos, gráficos e arquivos de áudio. Ademais, alguns algoritmos não conseguem realizar buscas efetivas em documentos cujo arquivo não permita a busca no próprio texto do documento[222].

Na seara do *e-discovery*, a empresa OpenText fornece softwares de investigações e análises contratuais, por meio da metodologia de *machine learning*[223].

3. Predição de resultados

A análise preditiva de resultados aplicada ao Direito possibilita toda uma série de melhorias na atividade da advocacia, orientada a partir de serviços que se utilizam do aprendizado de máquina para, com base em casos passados, prever o resultado de julgamentos futuros.

Uma vez que as estimativas de resultados de processos judiciais por mecanismos utilizando aprendizado de máquina detém um alto grau de precisão (embora não sejam infalíveis), pode-se dar mais atenção a atividades como planejamento estratégico, definição de políticas de acordo, além de orientação de políticas internas de *compliance*[224].

O caso do *Case-Crunch* é bastante relevante para se compreenderem um pouco melhor os impactos da IA na advocacia. Em 2017, foi proposta uma competição que ocorreu em Londres, onde se colocaram mais de cem advogados contra o sistema operado pela empresa para preverem se certos tipos de queixas seriam ou não recebidas. Ao final, o sistema acertou com uma precisão de 86,6% e os advogados, em 66,3% das vezes[225].

4. Geração de documentos

A capacidade de automatização processual, isto é, elaboração de petições e análise de andamento processual já pode ser observada no contexto nacional. No cenário brasileiro, despontam algumas

---

[221] DELAWARE. Court of Chancery of the State of Delaware. No. 7409, 2013 WL 1960621.Reclamante: EORHB, Inc. Reclamado: HOA Holdings LLC. Disponível em: <https://ralphlosey.files.wordpress.com/2012/10/predictive_coding_order_sua_sponte_delaware.pdf>. Acesso em: 29 de outubro de 2019.

[222] HAMPTON, Wallis M. *op. cit*. P. 32.

[223] Disponível em: <https://www.opentext.com/campaigns/ediscovery/ >. Acesso em: 28 de outubro de 2018.

[224] ALARIE, Benjamin; NIBLETT, Anthony; YOON, Albert, Using Machine Learning to Predict Outcomes in Tax Law. 15 dez. 2017. Disponível em: <https://ssrn.com/abstract=2855977>. Acesso em: 05 de novembro de 2018.

[225] CELLAN-JONES, Rory. The robot lawyers are here - and they're winning. BBC. 01 de nov. de 2017. Disponível em: <https://www.bbc.com/news/technology-41829534>. Acesso em: 01 de novembro de 2018.

empresas com grande potencial disruptivo, como a LegalLabs[226], responsável pela Dra. Luzia[227], a qual tem por objetivo automatizar procedimentos de cobrança em execuções fiscais da Fazenda Pública[228].

Para tanto, esta IA trabalha com a automatização de leitura de petições e tratamento massivo de dados em grandes carteiras de processos para auxiliar a tomada de decisões[229]. Apresenta-se, por conseguinte, não só como uma ferramenta para poupar tempo, mas também de auxílio na estruturação de estratégias processuais.

No mesmo campo, porém atuando no mercado americano, são alguns exemplos as plataformas RocketLawyer e a LegalZoom.

B. Poder Judiciário

Celeridade e estratégia demonstram-se como resultados do avanço jurídico tecnológico por intermédio da inteligência artificial. Nessa esteira, tal ferramenta é de suma importância para o Poder Judiciário, uma vez que poderá auxiliar com um célere trâmite processual, economia para as partes durante o processo e até alcançar alternativas para problemas sociais, tal como o encarceramento em massa. Isto posto, estaria o sistema judiciário apto a receber, absorver e promover tais mudanças?

Atualmente, algoritmos e dados estruturados já são utilizados pelo sistema judiciário dos Estados Unidos da América para proferir decisões, sentenças, quantificar fianças e auxiliar na ponderação da condenação ou não de acusados[230].

No contexto norte-americano, a utilização destes mecanismos justifica-se pelo argumento de que os algoritmos seriam capazes de melhor classificar o potencial de risco à sociedade de determinado indivíduo, uma vez que garantem fundamentos estritamente baseados em dados, opiniões do acusado e seu histórico de antecedentes criminais[231].

---

[226] LEGAL LABS. Disponível em: <https://legalabs.com.br/>. Acesso em : 01 de novembro de 2018.

[227] SERAPIÃO, Fábio. Dra. Luiza. Folha de São Paulo. 18 mai. 2018. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/dra-luzia/>. Acesso em 05 de novembro de 2018.

[228] COELHO, João Victor de Assis Brasil Ribeiro. APLICAÇÕES E IMPLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO DIREITO. 2017. 61f. Monografia – faculdade de Direito da Universidade de Brasília, Brasília, 2017. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/aplicacoes_e_implicacoes_da_inteligencia_artificial_no_direito.pdf>. Acesso em: 28 de novembro de 2018. p. 38.

[229] *Ibid.* p. 38-39.

[230] Um relatório elaborado pela *Electronic Privacy Information Center* (EPIC), destacou a utilização de algoritmos avaliadores de risco por Juízes norte-americanos para realizar a análise preditiva do comportamento de indiciados por crimes e de presos em cometer novos crimes ou contravenções. Disponível em: < https://epic.org/algorithmic-transparency/crim-justice/ >. Acesso em: 20 de novembro de 2018.
Ainda: LIPTAK, Adam. Sent to Prison by a Software Program's Secret Algorithms. The New York Times. 01 de mai. 2017. Disponível em: < https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html >. Acesso em: 20 de novembro de 2018.

[231] SMITH, Mitch. In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. The New York Times. 22 de jun. 2016. Disponível em: <

Assim, em virtude do encarceramento massivo[232], caberia ao juiz, amparado no *ranking* estabelecido pelo algoritmo, determinar que o acusado espere em liberdade ou continue preso até o seu julgamento[233].

Nesse sentido, um estudo publicado pela *National Bureau of Economic Research* destacou que a aplicação de algoritmos programados em *machine learning* poderia reduzir a taxa de crime em 25%, sem aumentar a população carcerária, ou poderia reduzi-la em 42% sem o crescimento da taxa de crime[234].

Apesar deste estudo demonstrar um futuro promissor para a aplicação de novas tecnologias nos Tribunais estadunidenses, a prática, no entanto, evidencia questionamentos sobre o uso de algoritmos em decisões judiciais.

Em especial, evidenciou-se que o algoritmo COMPAS, desenvolvido pela empresa Northpointe, utilizado no condado de Broward, estado da Florida, EUA, para analisar e prever a possibilidade de reincidência, indicava o dobro de chances de afrodescendentes cometerem novos crimes, em comparação aos brancos[235].

Nesse contexto, tratando-se de indivíduos rotulados como de alto risco à sociedade, observou-se que o algoritmo indicou duas vezes mais afrodescendentes do que brancos neste perfil. Ocorre que, posteriormente, estes indivíduos não reincidiram em práticas criminosas ou contravenções penais[236].

Ademais, constatou-se que o algoritmo também indicava brancos duas vezes mais que afrodescendentes como indivíduos de baixo risco à sociedade. Entretanto, nestes casos houve reincidência[237]. Cumpre esclarecer que os dados alimentados a este algoritmo baseiam-se em apenas duas características biológicas do acusado, quais sejam: idade e gênero[238].

Além de questionamentos envolvendo preconceito, insurgem-se questões referentes à violação do devido processo legal em julgamentos pautados em decisões de logaritmos.

---

https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?module=inline >. Acesso em: 20 de novembro de 2018.

[232] Segundo o Federal Bureau of Investigation (FBI), somente no ano de 2015, o número de presos nos EUA foi de 10,797,088 pessoas. FBI (2016), Crime in the United States, 2015. Washington, DC: Criminal Justice Information Services Division, Federal Bureau of Investigation, US Department of Justice. Disponível em: https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015.

[233] Cumpre ressaltar que no procedimento norte-americano, após a detenção do acusado, o mesmo imediatamente é submetido ao *bail hearing*, oportunidade em que o juiz determinará se este aguardará ao seu julgamento preso ou em Liberdade. Em: KLEINBER, Jon, *et. al.* Human Decisions and Machine Predictions. National Bureau of Economic Research Working Paper Series. Working Paper 23180. Fevereiro, 2017. Disponível em: https://www.nber.org/papers/w23180.pdf. p. 03.

[234] KLEINBER, Jon, *et. al. op. cit.* p. 40.

[235] ANGWIN, Julia, *et. al.* Machine Bias. ProPublica. 23 de maio, 2016. Disponível em: < https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 20 de novembro de 2018.

[236] *Ibid*.

[237] *Ibid*.

[238] A triagem de dados utilizados no algoritmo COMPAS compreende 137 questões envolvendo o histórico criminal do autor, de sua família, de seus conhecidos, histórico escolar, temperamento emocional, etc. Um exemplar do questionário encontra-se disponível em: < https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html >. Acesso em: 30 de novembro de 2018.

Em *Loomis v. Wisconsin*[239], a defesa de Eric L. Loomis destacou a inconstitucionalidade do julgamento baseado no algoritmo COMPAS, por violação do devido processo legal.

Nessa esteira, o apelante sustentou que não é possível obter informações sobre a acurácia e informações de fundamentação da condenação, tendo em vista a indisponibilidade ao acusado de acesso à metodologia utilizada pelo algoritmo.

Inobstante a deliberação da Suprema Corte do estado de Wisconsin, EUA, no entendimento da constitucionalidade do algoritmo COMPAS, a Corte determinou restrições na utilização desta ferramenta.

Desse modo, deliberou-se que o algoritmo não poderia ser ferramenta exclusiva de fundamentação de sentença de condenação ou para a dosimetria da pena. Outrossim, sua utilização deve ser acompanhada de motivação e fundamentação formulada de forma independente pelo juiz.

Independentemente dos questionamentos levantados pelo uso de logaritmos e inteligência artificial no âmbito do Poder Judiciário, observa-se que este movimento tende a crescer exponencialmente.

Somente no cenário brasileiro, o que certamente impactará a prática do Direito em um cenário de curto a médio prazo é a introdução do VICTOR[240]. Trata-se da IA desenvolvida em parceria entre o Supremo Tribunal Federal e a Universidade de Brasília, cujo objetivo é analisar por meio de inteligência artificial sobre a existência ou não de repercussão geral nos recursos que chegam ao tribunal.

Além disso, em que pese não vinculado ao Poder Judiciário, o Tribunal de Contas da União (TCU) automatizou a avaliação preventiva de editais de licitação e atas de pregão por meio do sistema Alice (Análise de Licitações e Editais)[241].

Diante deste contexto, a robô Alice é capaz de verificar indícios de irregularidades ou riscos em licitações, uma vez que é capaz de coletar e testar os dados de editais de licitações e atas de pregão eletrônico[242].

Após a análise desta imersão tecnológica no meio jurídico é inegável que ferramentas como algoritmos, inteligência artificial e suas ramificações, determinarão as novas competências do profissional do Direito.

---

[239] WISCONSIN. Supreme Court of Wisconsin. Apelante: Eric L. Loomis. Apelado: State of Wisconsin. Chief Justice Patience Roggensack; Justice Shirley Abrahamson. Wisconsin, 13 de julho de 2016. Disponível em: < https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690 >. Acesso em: 30 de novembro de 2018.

[240] SUPREMO TRIBUNAL FEDERAL. Projeto VICTOR do STF é apresentado em congresso internacional sobre tecnologia. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=390818&tip=UN Acesso em 06 de novembro de 2018.

[241] GOMES, Helton Simões. Como as robôs Alice, Sofia e Monica ajudam o TCU a caçar irregularidades em licitações. G1, 18 de março de 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/como-as-robos-alice-sofia-e-monica-ajudam-o-tcu-a-cacar-irregularidades-em-licitacoes.ghtml>. Acesso em: 28/11/2018.

[242] TRIBUNAL DE CONTAS DA UNIÃO. Prêmio Reconhe-ser. Brasília, v. 3, n. 3, 2018. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F61E31021016205A9D253413C>. p. 11.

Dessa forma, situado o contexto jurídico tecnológico atual, como pode-se vislumbrar a interligação entre Direito e tecnologia em cenários futuros?

III. Cenários futuros

Ainda que em embrionárias na pauta do Direito, as tecnologias abordadas em sequência já possuem *insights* avançados em diversos segmentos econômicos.

Portanto, a seguir, apresenta-se um panorama hipotético com reflexões sobre o impacto da tecnologia no Direito a longo prazo, abordando ferramentas em desenvolvimento capazes de remodelar a estrutura de diversos mercados, tais como a computação quântica e o transhumanismo.

A computação quântica dedica-se ao estudo de aplicação de princípios da física quântica na ciência da computação. Nesse sentido, um computador quântico seria capaz de atuar manipulando a superposição de dois estados[243].

Isto significa um aumento colossal na capacidade de processamento das máquinas, as quais, atualmente, operam por meio da lógica binária, isto é, pela assunção de apenas um estado[244]. Nessa esteira, dispensadas a abordagem das sensíveis questões técnicas, a computação quântica revolucionará a compreensão sobre criptografia e inteligência artificial.

Em virtude da excelente e imensurável capacidade de processamento, o computador quântico será capaz de fornecer criptografias mais seguras aos usuários da internet[245]. Essencial destacar que, por outro lado, esta tecnologia é capaz de derrubar com facilidade a criptografia desenvolvida pela computação binária.

Em um momento em que se tornam cada vez mais comuns transferências de valores pelo meio eletrônico, especialmente, moedas virtuais (criptoativos), as quais pautam sua segurança em criptografias, é basilar atentar-se aos desdobramentos da computação quântica e seu utilização ética.

Ademais, tendo em vista o potencial de processamento do computador quântico, vislumbram-se alternativas de aplicação dos mesmos na medicina. Desse modo, o possível desenvolvimento de uma inteligência artificial pautada em um processador quântico, testaria um maior número de combinações genéticas em menor tempo, alcançando-se, portanto, explicações para doenças, bem como desenvolvimento de novos e efetivos medicamentos[246].

Nesta seara da medicina e biologia, intrínseca é a relação do transhumanismo com estas matérias. É certo que este ramo impactará de forma inimaginável no futuro da advocacia e do Direito enquanto atividade e sistema de organização social essencialmente humanos. A imbricação entre

---

[243] HAAS, Fernando. Computação Quântica: Desafios para o Século XXI. Cadernos Instituto Humanitas Unisinos ideias. São Leopoldo, Rio Grande do Sul, ano 4, n. 53, 2006. Disponível em: < http://professor.ufrgs.br/fernando-haas/files/computacao_quantica.pdf >. Acesso em: 30/11/2018. p. 16.

[244] *Ibid*, p. 15.

[245] MÖLLER, Matthias; VUIK, Cornelis. On the impact of quantum computing technology on future developments in high-performance scientific computing. Ethics and Information Technology. v. 19, n. 4, 2017. p. 253-269. Disponível em: < https://link.springer.com/article/10.1007/s10676-017-9438-0 >. Acesso em: 30/11/2018. p. 264.

[246] *Ibid*, p. 264.

genética, nanotecnologia e robótica certamente exigirá profundas reflexões problematizando a extensão dos fenômenos jurídicos e seus limites.

Longe de se tratar de um tema apenas para a ficção científica, à medida que a fusão entre humanos e máquinas se tornar uma realidade palpável conceitos como direitos de personalidade, direitos fundamentais e dignidade da pessoa humana se tornarão desatualizados.

Na data de 28 de agosto de 2012, a Corte Europeia de Direitos Humanos julgou favoravelmente aos reclamantes Costa e Pavan em face da Itália reconhecendo o "direito a um filho geneticamente saudável", uma vez que ambos são portadores de uma doença chamada fibrose cística, tendo um filho já acometido por essa condição.

Essencialmente, a Corte garantiu ao casal o direito a seleção genética de um embrião livre dessa condição médico a ser implantado na mãe por meio de reprodução assistida.

O autor Grégor Puppinck reconhece na decisão da Corte um primeiro passo no reconhecimento legal do transhumanismo, inclusive com impacto direto na própria concepção do que seriam os direitos humanos, já não apenas destinados à proteção da raça humana, mas sim à sua melhoria[247].

Os impactos da IA e da biotecnologia no Direito, e na sociedade de forma geral, serão profundos e certamente irão envolver debates intensos a respeito de quais formas de implantação da tecnologia serão aceitas.

Conforme reflexão proposta por Susskind[248], códigos legislativos inteiros poderiam ser transmutados em microchips e redes, possibilitando que estes fossem implantados diretamente em nossas máquinas ou em nossos cérebros.

Assim, é essencial que haja esforços metodológicos nas áreas da Filosofia e Teoria do Direito de modo a atualizar estes conceitos, ou até mesmo de abandoná-los em face de exigências da sociedade futura, especialmente porque, conforme menciona Eliseu Raphael Venturi[249]: "*as biotécnicas podem representar o aperfeiçoamento e a extensão da qualidade de vida, pode determinar controle de massas e ruptura plena de qualquer possibilidade de isonomia social.*"

Assim, qualquer que seja o papel futuro atribuído à IA e seus impacto na vida social e na prática do Direito, estes devem ser direcionados para resultados positivos, combatendo-se o aprofundamento das desigualdades, que deixariam de ser apenas sociais e econômicas, para se tornarem genéticas.

Ainda que de primeiro momento a computação quântica e o transhumanismo aparentem aplicações em ramos diversos ao Direito, certamente denota-se que suas consequências são suficientes para que juristas se antecipem, bem como acompanhem e participem dos desdobramentos éticos e legais promovidos por estas inovações.

---

[247] PUPPINCK, Gregor. The Case of Costa and Pavan v. Italy and the Convergence between Human Rights and Biotechnologies. Commentary on the ECHR Ruling in Costa and Pavan v. Italy, No. 54270/10, 28th August 2012. Quaderni di Diritto Mercato Tecnologia - N°3, Anno III. Disponível em SSRN: <https://ssrn.com/abstract=2348142>. Acesso em 16 de novembro de 2018.

[248] SUSSKIND, R. E. (2013). Tomorrow's lawyers: an introduction to your future. Oxford, United Kingdom: Oxford University Press, 2017. 2. ed. ps. 191-192.

[249] VENTURI, Eliseu Raphael. INTERFACES DO HUMANISMO JURÍDICO, TRANSHUMANISMO E FUTURO PÓS-HUMANO. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=d65631146921df3b>. Acesso em 12 de novembro de 2018.

IV. A expectativa da Inteligência Artificial integrada ao Direito

A princípio, a aplicação da inteligência artificial está diretamente relacionada ao alcance de resultados de maneira célere e econômica. Não somente uma ferramenta capaz de proporcionar tais resultados, a tecnologia, de maneira geral, proporciona o redescobrimento de competências profissionais.

Dentre tecnologias já aplicadas, em desenvolvimento, ou até mesmo embrionárias, o fato é que as mesmas modelam e demandam um novo profissional, isto é, um indivíduo de competência multidisciplinar e de capacidade cada vez mais racional e criativa, desvirtuando-se daquele designado a realizar tarefas puramente repetitivas.

Mais do que a simples automação de tarefas repetitivas, segundo uma visão mais enfática de Richard Susskind[250], o impacto de novas tecnologias (aqui incluindo as aplicações em IA) no Direito não deve ser pensado somente em termos de automação, e sim de inovação, permitindo aos advogados a prática de tarefas antes impensadas. O desafio posto aos profissionais que queiram se manter relevantes então, é o de encontrar novas e melhores formas de se praticar o direito a partir das novas tecnologias.

Portanto, o desenvolvimento de inteligências artificiais jurídicas não se remete à derrocada e extinção das atividades advocatícias e judiciais. Pelo contrário, trata-se de um processo constante de aprendizado e redescoberta de alternativas de atuação e soluções céleres, eficientes e inteligentes aplicadas ao Direito.

[250] SUSSKIND, R. E. (2013). Tomorrow's lawyers: an introduction to your future. Oxford, United Kingdom: Oxford University Press, 2017. 2. ed. ps. 14-15.

REFERÊNCIAS BIBLIOGRÁFICAS:

ALARIE, Benjamin; NIBLETT, Anthony and YOON, Albert. How Artificial Intelligence Will Affect the Practice of Law. University of Toronto Law Journal, v. 68, jan. 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.3066816. Acesso em:

ALARIE, Benjamin; NIBLETT, Anthony; YOON, Albert, Using Machine Learning to Predict Outcomes in Tax Law. 15 dez. 2017. Disponível em: <https://ssrn.com/abstract=2855977>. Acesso em: 05 de novembro de 2018.

CAMBI, Eduardo. Discovery no processo civil norte-americano e efetividade da justiça brasileira. Revista de Processo. v. 245, Julho 2015. Disponível em: < http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RPro_n.245.16.PDF>. Acesso em: 22 de novembro de 2018.

COELHO, João Victor de Assis Brasil Ribeiro. APLICAÇÕES E IMPLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO DIREITO. 2017. 61f. Monografia – faculdade de Direito da Universidade de Brasília, Brasília, 2017. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/aplicacoes_e_implicacoes_da_inteligencia_artificial_no_direito.pdf>. Acesso em: 28 de novembro de 2018.

DELAWARE. Court of Chancery of the State of Delaware. No. 7409, 2013 WL 1960621.Reclamante: EORHB, Inc. Reclamado: HOA Holdings LLC. Disponível em: <https://ralphlosey.files.wordpress.com/2012/10/predictive_coding_order_sua_sponte_delaware.pdf>. Acesso em: 29 de outubro de 2019.

HAAS, Fernando. Computação Quântica: Desafios para o Século XXI. Cadernos Instituto Humanitas Unisinos ideias. São Leopoldo, Rio Grande do Sul, ano 4, n. 53, 2006. Disponível em: < http://professor.ufrgs.br/fernando-haas/files/computacao_quantica.pdf >. Acesso em: 30/11/2018.

HAMPTON, Wallis M. Predictive Coding: It's Here to Stay. E-Discovery Bulletin, June/ July, 2014. Disponível em: < https://www.skadden.com/insights/publications/2014/06/predictive-coding-its-here-to-stay>. p. 29. Acesso em: 28 de outubro de 2018.

HARARI, Yuval Noah. 21 lições para o século 21 / Yuval Noah Harari ; tradução Paulo Geiger. — 1a ed. — São Paulo : Companhia das Letras, 2018.

KLEINBER, Jon, *et. al.* Human Decisions and Machine Predictions. National Bureau of Economic Research Working Paper Series. Working Paper 23180. Fevereiro, 2017. Disponível em: https://www.nber.org/papers/w23180.pdf.

KRAUSOVÁ, Alžbeta. Intersections between Law and Artificial Intelligence. International Journal of Computer (IJC), Vol. 27, nº 01, 2017. Disponível em: http://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1071/464 p. 56-57

MÖLLER, Matthias; VUIK, Cornelis. On the impact of quantum computing technology on future developments in high-performance scientific computing. Ethics and Information Technology. v. 19, n. 4, 2017. p. 253-269. Disponível em: < https://link.springer.com/article/10.1007/s10676-017-9438-0 >. Acesso em: 30/11/2018.

PUPPINCK, Gregor. The Case of Costa and Pavan v. Italy and the Convergence between Human Rights and Biotechnologies. Commentary on the ECHR Ruling in Costa and Pavan v. Italy, No. 54270/10, 28th August 2012. Quaderni di Diritto Mercato Tecnologia - N°3, Anno III. Disponível em SSRN: <https://ssrn.com/abstract=2348142>. Acesso em 16 de novembro de 2018.

TRIBUNAL DE CONTAS DA UNIÃO. Prêmio Reconhe-ser. Brasília, v. 3, n. 3, 2018. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F61E31021016205A9D253413C>.

SUSSKIND, R. E. (2013). Tomorrow's lawyers: an introduction to your future. Oxford, United Kingdom: Oxford University Press, 2017.

VENTURI, Eliseu Raphael. Interfaces do Humanismo Jurídico, Transhumanismo e Futuro Pós-Humano. Disponível em <http://www.publicadireito.com.br/artigos/?cod=d65631146921df3b>. Acesso em: 12 de novembro de 2018.

WISCONSIN. Supreme Court of Wisconsin. Apelante: Eric L. Loomis. Apelado: State of Wisconsin. Chief Justice Patience Roggensack; Justice Shirley Abrahamson. Wisconsin, 13 de julho de 2016. Disponível em: <https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690>. Acesso em: 30 de novembro de 2018.

INTELIGÊNCIA ARTIFICIAL: MITOS E REALIDADE

ARTIFICIAL INTELLIGENCE: MYTHS AND REALITY

Bruno Vinícius Nassar

Advogado graduado pela Universidade Estácio de Sá. bruno.nassar@outlook.com

Lucas Willian Farias

Advogado graduado pelo Centro Universitário do Brasil – UNIBRASIL, membro da Comissão de Inovação e Gestão da Ordem dos Advogados do Brasil – Seccional do Paraná. fariassolus@gmail.com

Marcelo Sampaio Pissetti

Advogado graduado pela Universidade Curitiba, especializado em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários - IBET, membro das Comissões de Direito Tributário e de Inovação e Gestão da Ordem dos Advogados do Brasil - Seccional do Paraná. marcelo@mpac.adv.br

Mayara Guibor Spaler

Advogada, graduada pela Universidade Federal do Paraná - UFPR. Pós-graduanda em Direito Digital e Compliance pela Faculdade IBMEC – SP. Atualmente é integrante da Comissão de Inovação e Gestão da Ordem dos Advogados do Brasil - Seccional do Paraná. mayaraspaler@gmail.com

RESUMO:

O presente artigo tem por finalidade introduzir o conceito de inteligência artificial, abordando a definição estabelecida pela bibliografia básica e suas principais áreas de aplicação. Superada a fase inicial, realizar-se-á análise da realidade atual do campo e perspectivas para o futuro, com base em doutrinadores e entusiastas atuantes no setor. Por fim, considerando a realidade e perspectivas para o futuro, realizar-se-á análise crítica acerca das atuais medidas de prevenção de riscos.

Palavras-chave: inteligência artificial, mitos, impactos, superinteligência, inteligência artificial genérica.

ABSTRACT

This article aims to introduce the concept of artificial intelligence, addressing the definition established by the basic bibliography and its main areas of application. Once the initial phase is over, an analysis of the current reality of the field and perspectives for the future will be carried out, based on the indoctrinators and enthusiasts active in the sector. Finally, considering the reality and perspectives for the future, a critical analysis will be carried out on the current measures of risk prevention.

Keywords: artificial intelligence, myths, impacts, superintelligence, artificial generic intelligence.

SUMÁRIO: 1. Introdução. 2. Inteligência artificial na atualidade. 3. Perspectivas futuras. 4. Análise crítica e jurídica. 5. Considerações finais. 6. Referências bibliográficas.

1. INTRODUÇÃO

O termo 'inteligência artificial' (IA), ou '*artificial intelligence' (IA),* foi cunhado e usado pela primeira vez pelo cientista da computação John McCarthy[251], em uma conferência de especialistas realizada no ano de 1956, em *Dartmouth College*, na cidade de Hanover, nos Estados Unidos.

A partir de então, diante do entendimento de que os estudos e atividades desenvolvidas na área representavam um campo próprio de atuação, passou-se a questionar cientificamente em que consiste, efetivamente, a inteligência artificial.

Embora a doutrina – e mesmo a prática – possua diversas abordagens, não se podendo chegar a uma única concepção, as principais definições do conceito de inteligência artificial baseiam-se no cruzamento de quatro critérios: o saber, o pensar *versus* agir e o humano *versus* racional[252], adiante explanados.

A primeira abordagem considera que a inteligência artificial está presente quando o agente pensa como humano, o que pode ser verificado, basicamente, por meio de três métodos: a) ato de introspecção realizado por um humano, a fim de realizar autoanálise para identificar padrões e, então, contrapô-los com as atividades do agente; b) realização de experimentos psicológicos em humanos, identificando-se padrões e, igualmente, contrapondo-os com as atividades do agente (máquina, robô, *software*, aplicativo e afins, que tenham por finalidade exercer/auxiliar a atividade humana); e c) análise neurológica da atividade cerebral humana, com a conseguinte comparação com o processamento da máquina.

A segunda abordagem tem como presente a inteligência artificial quando o agente pensa racionalmente: a principal forma de verificação do pensamento racional remete à lógica aristotélica, com a presença da atividade de proposições com conteúdo, basicamente, de verdadeiro ou falso e conjuntos (exemplo: se João é homem e todo homem é humano, então João é humano).

A terceira abordagem tem como presente a inteligência artificial quando o agente atua como ser humano. Tal verificação tem por principal referência o 'teste de Turin', idealizado pelo matemático, lógico criptoanalista e cientista da computação britânico Alan Turin, no qual o agente "(...) passará no teste se um interrogador humano, depois de propor algumas perguntas por escrito, não conseguir descobrir se as respostas escritas vêm de uma pessoa ou de um computador."[253].

A quarta abordagem tem como presente a inteligência artificial quando o agente atua de forma racional, tendo-se por agente racional aquele que age para alcançar o melhor resultado ou, quando há incerteza, o melhor resultado esperado.

Postas as quatro formas de abordagem, verifica-se que o campo da inteligência artificial se desdobra em diversos subcampos/facetas, destacando-se, adiante, as seis principais.

No campo de 'aprendizado', busca-se a criação de algoritmos e técnicas que permitam ao agente aprender com suas experiências no ambiente em que está situado. À medida em que o agente aprende mais sobre o ambiente, ele é capaz de desempenhar melhor as tarefas naquele contexto.

---

[251]GUBERN, Román. **O Eros eletrônico.** Disponível em: <https://www.scribd.com/document/124062697/O-Eros-Eletronico-Roman-Gubern>. Acesso em: 28 nov. 2018. p. 87.

[252] NORVIG, Peter; RUSSEL, Stuart. **Inteligência Artificial.** Rio de Janeiro: Elsevier Editora Ltda., 2013. p. 25.

[253] NORVIG, Peter; RUSSEL, Stuart. **Inteligência Artificial.** Rio de Janeiro: Elsevier Editora Ltda., 2013. p. 25.

No campo da representação de conhecimento (armazenagem), estuda-se a forma como o agente armazena/representa as experiências/conhecimento que tem do mundo, o que é, majoritariamente, baseado em fatos e regras. A título exemplificativo, destaca-se que em um processamento de linguagem natural o conhecimento é armazenado pela classificação do alfabeto em vogais ou consoantes.

No campo do raciocínio, estuda-se a exposição, pelo agente, do raciocínio humano por meio de fórmulas/proposições lógicas (principalmente a lógica aristotélica) ou, ainda, formulação de probabilidades, com base nas redes bayesianas.

No campo do processamento de linguagem, a atuação é principalmente na criação de geradores e processadores de textos, tal como os atualmente muito conhecidos *chatbots*, nos quais a máquina interage, textualmente ou oralmente, com o ser humano.

No campo da percepção, atua-se no sentido de conferir ao agente a capacidade de perceber o mundo fisicamente, por meio de sensores, atuadores e efetuadores.

No campo da robótica, atua-se no sentido de que o agente seja capaz de manipulação e manter interação física com o meio.

Considerando que, como se verá adiante, o principal objetivo dos subcampos de atuação da inteligência artificial, e da área em geral, é se chegar ao estado da 'Inteligência Artificial Genérica', no qual o agente está desenvolvido o suficiente para se equiparar ao ser humano. Para esse estudo, tem-se que é inteligente o agente que possua habilidades satisfatórias nesses seis campos de atuação e, igualmente, passem ao crivo das quatro definições (pensar como humano, pensar racionalmente, agir como humano e agir racionalmente).

Os agentes que, por outro lado, não cumprirem tais requisitos de forma integral, são considerados apenas facetas da inteligência artificial, que se utilizam de alguns de seus recursos, pontualmente, para realizar tarefas ou cumprir objetivos específicos, com pouca ou nenhuma autonomia. Portanto, de acordo com os critérios adotados eles não podem ser considerados inteligentes.

Com base nessas premissas, passa-se à análise do estado atual da inteligência artificial.

2. INTELIGÊNCIA ARTIFICIAL NA ATUALIDADE

Pretende-se, nos próximos parágrafos, exemplificar como a inteligência artificial se propaga na contemporaneidade e como as empresas ao redor do mundo estão lidando com seus avanços.

Inicialmente, destaque-se que, quando se fala em consciência de máquina, alguns pesquisadores trazem à tona as discussões sobre cognição, que é uma expressão velha e, portanto, já conhecida pela sociedade. No entanto, é importante registrar o espaço que a expressão "Computação Cognitiva" vem ganhando nos fóruns de discussão ao redor do mundo.

É notório que a inteligência artificial é a capacidade de as máquinas pensarem como seres humanos e, em certos aspectos, raciocinarem e tomarem decisões como as pessoas o fazem. Para isso, é imprescindível fornecer à máquina uma estrutura organizada de dados e um universo recheado de informações (*big data*) para viabilizar seu desenvolvimento.

A Inteligência Artificial Cognitiva, apesar de assemelhar-se ao conceito anterior, possui como ponto crucial de diferenciação o fato de que, neste modelo, a máquina é capaz de, cada vez mais, aprimorar seu aprendizado. Nesse aspecto, o *machine learning* tem papel fundamental, eis que torna o processo de aprendizagem da máquina muito mais eficaz, com o objetivo de aproximar-se do cérebro humano.

Um grande exemplo de Inteligência Artificial Cognitiva é o *Watson*, da IBM, que utiliza um sistema sofisticado de dados para apoiar médicos em diagnósticos e tratamentos para doenças como o câncer, por exemplo. A tecnologia apresentada pela empresa é resumida da seguinte maneira:

> Todos os dias, líderes e porta-vozes de oncologia trabalham para aprimorar o tratamento contra o câncer em uma era de transformação da saúde. Watson Health está trazendo uma combinação sem precedentes de recursos e tecnologias para ajudar a superar os desafios que eles enfrentam. Com Watson, as equipes de assistência médica em todo o mundo estão implementando um modelo de tratamento contra o câncer mais centrado no paciente, melhorando as experiências tanto para os provedores quanto para os pacientes.[254]

Outro *case* atual, recentemente divulgado na imprensa, é a plataforma de relacionamento com clientes da empresa PGMais. A ferramenta de inteligência artificial cognitiva é capaz de falar e escrever ao mesmo tempo. No entanto, foi desenvolvida de modo que seus *scripts* customizados sejam automaticamente modificados durante o processo de conversa com o cliente. Desde quando a empresa brasileira implantou a ferramenta, colhe seus frutos, conforme se vê adiante:

> A PGMais, em parceria com a Bellinati Perez, é finalista do Prêmio Best Performance 2018, que reconhece as melhores práticas do mercado de crédito, cobrança e televendas. O case "Kami – Unidade Integrada de Cobrança Cognitiva" se destacou na categoria "Excelência em cobrança digital: aplicação de assistentes virtuais/chatbot" ao mostrar os resultados obtidos com a implantação de Kami, uma plataforma cognitiva de

[254] Oncology and Genomics. **IBM**, 2018. Disponível em: <https://www.ibm.com/watson/br-pt/health/oncology-and-genomics/>. Acesso em: 27 nov. 2018.

> inteligência artificial que passou a fazer análise e resposta do retorno de clientes por meio de SMS.[255]

Nessa mesma linha, o então Corregedor Nacional de Justiça, Humberto Martins, reafirmou[256] que as formas tradicionais de trabalho serão suprimidas muito rapidamente e que, por isso, faz-se necessário o investimento em profissionais do Direito que saibam lidar com as novas tecnologias. Segundo ele, "estamos em meio a uma revolução causada pela digitalização da vida. Todos os processos produtivos estão sendo alterados com base na aplicação do aprendizado de máquina. É a quarta revolução industrial."[257]

Recentemente, a empresa brasileira Tembici – responsável pelos serviços de aluguel de bicicleta nos estados de São Paulo e Rio de Janeiro – decidiu investir em uma plataforma de inteligência artificial. Em síntese, o serviço é capaz de detectar o exato momento em que a demanda em determinada estação aumenta e, automaticamente, dispara um comando para deslocar maior número de bicicletas para lá.

> As empresas de compartilhamento de bikes investem em inteligência artificial para entender em detalhes o comportamento dos ciclistas e, assim, tentar prever onde haverá pedidos, minuto a minuto. Com isso, buscam evitar que o usuário se frustre ao buscar uma bicicleta e não encontrar por perto. O processamento desses dados é feito em servidores remotos, na nuvem. [258]

Embora seja possível listar empresas brasileiras que se preocupam com as novidades tecnológicas, vale ressaltar que as grandes corporações internacionais, em especial as norte-americanas, já estão demasiadamente avançadas quando o assunto é inteligência artificial.

O *Facebook*, por exemplo, desenvolveu uma ferramenta capaz de remover e bloquear nudez infantil compartilhada através de fotos em sua rede social. A ideia principal da empresa é combater a exploração sexual de crianças, banindo de sua plataforma os usuários que insistem em distribuir conteúdo proibido. A empresa esclareceu que a iniciativa buscou alinhar "inteligência artificial e *machine learning* para detectar nudez infantil, bloqueando o conteúdo no momento em que é postado. Estima-se que a rede social já removeu 8,7 milhões de publicações que violavam as políticas de nudez infantil."[259]

---

[255] Uso de inteligência artificial leva PGMais e Bellinati Perez para final do Prêmio Best Performance. **Pgmais**, 2018. Disponível em: <http://pgmais.com.br/noticias/uso-de-inteligencia-artificial-leva-pgmais-e-bellinati-perez-para-final-do-premio-best-performance/>. Acesso em: 25 nov. 2018.

[256] Em palestra ministrada para o auditório do XX Congresso Brasileiro de Direito Notarial e de Registro.

[257] CNJ: Corregedor fala sobre os impactos da inteligência artificial no Direito. **TRF2**, 2018. Disponível em: <http://www10.trf2.jus.br/portal/cnj-corregedor-fala-sobre-os-impactos-da-inteligencia-artificial-no-direito/>. Acesso em: 29 nov. 2018.

[258] BALAGO, Rafael. Empresas de aluguel de bike sofisticam serviço com inteligência artificial. **Folha de S. Paulo**, 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/10/empresas-de-aluguel-de-bike-sofisticam-servico-com-inteligencia-artificial.shtml>. Acesso em: 20 nov. 2018.

[259] PARESH, Dave. Facebook removes 8.7 million sexual photos of kids in last three months. **REUTERS**, 2018. Disponível em: < https://ca.reuters.com/article/technologyNews/idCAKCN1MY1SE-OCATC>. Acesso em: 23 nov. 2018.

Diante disso, vale ressaltar que os desafios e as possibilidades que se abrem a partir do uso da inteligência artificial são inúmeros, o que enseja diversas discussões, seja no âmbito tecnológico, econômico, moral e, sobretudo, jurídico.

3. PERSPECTIVAS FUTURAS

Em 2006, Amy Webb fundou o *Future Today Institute,* que, em suas palavras, tem como missão concentrar-se "exclusivamente em como a tecnologia e a ciência emergentes vão atrapalhar os negócios, transformar a força de trabalho e inflamar a mudança geopolítica. Juntamente com (...) clientes e parceiros, a FTI usa pesquisas baseadas em dados para modelar e prototipar o futuro".[260]

Desde que foi fundado, o instituto publica anualmente um relatório[261] indicando as principais tendências tecnológicas para um futuro próximo. O relatório divulgado no primeiro trimestre de 2018 possuía 225 tendências que envolvem, entre outras tecnologias, a inteligência artificial, robôs autônomos e viagens espaciais.

O relatório confere relevante destaque para inteligência artificial. Já em sua parte inicial, indica que o desenvolvimento de tal tecnologia é a versão moderna da corrida armamentista, colocando a China como a possível potência futura no assunto. Aponta também a computação cognitiva – que une técnica de processamento de linguagem natural e aprendizado de máquina – como tendência já para o ano seguinte. A previsão é que no futuro essa tecnologia esteja mais presente em atividades intelectuais e tarefas "pensantes", inclusive auxiliando na rotina de advogados e de empresas como a *Microsoft Office* ou o *Google Docs*.

Outra tendência indicada no relatório é a criação de algoritmos altamente técnicos e com interface simples, para que mesmo um usuário não especializado em inteligência artificial possa utilizá-lo e criar, a título de exemplo, seus próprios modelos preditivos.

Também ganhou destaque a tecnologia conhecida como "*Zero Uis*"[262], que promete uma nova geração de *smartphones*, completamente diferente dos modelos que conhecemos atualmente. Ela permite menor atrito com os aparelhos, com interação de maneira mais natural, como por comando de voz, de movimento, visão computacional etc. De acordo com Amy, até o ano de 2021, metade das pessoas em países desenvolvidos interagirão com as máquinas utilizando apenas suas vozes. A *Alexa* – assistente virtual da Amazon acionada por comando de voz – é um exemplo do avanço no desenvolvimento da *Zero UI*.

Está cada vez mais difícil distinguir a ficção da realidade. Em 2013, um episódio da série *Black Mirror*, retratou a história de uma mulher que perdeu seu companheiro em um acidente de carro e buscou uma empresa que, por meio de registros deixados na rede pelo *de cujus*, criou um robô dotado de inteligência artificial, que passou a reproduzir o comportamento do falecido.

No mesmo sentido, há uma *startup* portuguesa que está desenvolvendo um produto que, tal como no referido episódio, promete a eternidade – mas neste caso a eternidade cibernética. Conhecida como *ETER9*, a empresa criou uma rede social que aprende por meio da interação do usuário com a ferramenta e, em algum tempo, promete fazer postagens como se fosse o próprio usuário.

3.1 O QUE É INTELIGÊNCIA ARTIFICIAL SÓLIDA OU GERAL (IAG)

---

[260] Future Today Institute. Disponível em: <https://futuretodayinstitute.com/>. Acesso em: 30 nov. 2018.

[261] WEBB, Amy. **Tech Trends Report.** 2018. Disponível em: <https://futuretodayinstitute.com/2018-tech-trends-annual-report/>. Acesso em: 30 nov. 2018.

[262] BHARGAVA, Rohit. **O futuro das máquinas é invisível**: 2018. Disponível em: <https://gq.globo.com/Prazeres/Tecnologia/noticia/2018/02/o-futuro-das-maquinas-e-invisivel.html>. Acesso em: 30 nov. 2018.

Inteligência Artificial Limitada (fraca) nada mais é do que a construção de sistemas que, de certa forma, não são inteligentes a ponto de raciocinar por si próprios. Em outras palavras, acredita-se que essa forma de inteligência artificial é uma consolidação de regras escritas através de códigos de desenvolvimento, pautadas por '*if, then and else*' *(se, então, senão, ou etc.),* e que, portanto, condiciona a máquina a tomar decisões nos limites estipulados pelo programador.

> O *machine learning* é uma forma de criação de inteligência artificial a partir da coleta e análise de dados, cujos resultados permitem que a máquina "aprenda" uma determinada tarefa para executá-la por si só ou consiga determinar uma situação ou informação futura com base em padrões observados. A premissa é a de basicamente recriar um padrão tão complexo quanto o da inteligência humana, efetuando uma série de tarefas e aprendizados a cada momento. No entanto, o que se conseguiu até agora é o aprendizado de tarefas específicas, a chamada inteligência artificial limitada. É o caso de algoritmos que utilizam dados de um usuário para indicar filmes e músicas que poderiam ser de seu interesse.[263]

Portanto, a Inteligência Artificial Limitada – ou Fraca – é aquela desenvolvida para executar apenas uma ou poucas atividades específicas. Ela pode superar a capacidade humana na atividade para a qual foi criada, mas não o fará na execução de outras atividades. O *Deep Blue*[264], supercomputador criado pela IBM, que em 1997 ganhou uma partida de xadrez do então campeão mundial Garry Kasparov, é um exemplo de IA Fraca.

Já na Inteligência Artificial Sólida – ou Forte – as máquinas são capazes de *pensar* por si e não apenas de simular o pensamento humano. Ela corresponde ao fato do computador possuir uma espécie de consciência capaz de produzir inclusive conteúdos artísticos, sendo certo que o algoritmo saberia os motivos pelos quais desenvolveu aquela determinada arte. Nesse aspecto, importante consignar o que registrou Geoffrey Jefferson, em 1949:

> Somente quando uma máquina conseguir escrever um soneto ou compor um soneto em consequência de ter pensado e de ter sentido emoções, e não pela disposição aleatória de símbolos, podemos concordar que a máquina irá se equiparar ao cérebro humano – isto é, se ela não apenas escrever, mas souber o que escreveu.[265]

Ressalte-se ainda a posição de Searle quando afirma que "qualquer tentativa literal de criar intencionalidade artificialmente (IA Forte) não poderia obter sucesso apenas pelo desenvolvimento de programas, mas teria de duplicar os poderes causais do cérebro humano".[266]

A IA Forte corresponderia então à evolução da IA Fraca, capaz de executar atividades intelectuais características do ser humano. Atualmente, há poucos pesquisadores atuantes nesta área, dada a

---

263 Como a inteligência artificial e machine learning ajudam a segurança da informação. **Terra**, 2018. Disponível em: <https://www.terra.com.br/noticias/dino/como-a-inteligencia-artificial-e-machine-learning-ajudam-a-seguranca-da-informacao,9cfec9e8c5765408911fae2856034028frjpag2u.html>. Acesso em: 28 nov. 2018.

264 IBM. **Deep Blue**. Disponível em: <https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/> Acesso em: 30 nov. 2018.

265 CONSENTINO, Marcelo. Inteligência Artificial. **O Estado da Arte**, 2018. Disponível em: <http://oestadodaarte.com.br/inteligencia-artificial/>. Acesso em: 28 nov. 2018.

266 SEARLE, John R. Minds, brains and programs. In: ___. **Behavioral and brain sciences**. vol. 3. Cambridge University Press, 1980.

grande complexidade e a capacidade computacional necessária para o desenvolvimento de tal tecnologia. Algumas teorias apontam como alternativa para a criação da IA Geral a união de vários algoritmos desenvolvidos para atividades específicas (IA Fraca). No entanto, isso ainda não resolve o problema da alta capacidade computacional necessária.

Importante ressaltar que, de acordo com o que se sabe do cérebro humano atualmente, não se conhecem leis da física que impossibilitem a sua criação artificial. É certo que isso demandaria uma capacidade computacional que provavelmente não existe ainda, mas muitos especialistas acreditam que em um futuro próximo será possível desenvolvê-lo.

3.2 A SINGULARIDADE TECNOLÓGICA E A SUPERINTELIGÊNCIA ARTIFICIAL (SIA)

Singularidade é um termo utilizado na física para fenômenos impossíveis de se descrever. Um bom exemplo do uso desse termo é o buraco negro, no qual ocorrem eventos que, até o momento, nenhuma equação conseguiu apontar quais são.

Emprestando o termo da física, a singularidade tecnológica representa o momento em que toda a inteligência humana seria superada pela inteligência artificial, causando impactos que seriam impossíveis de se prever na atualidade. Com tal singularidade tecnológica seria criada a Superinteligência Artificial (SIA), que seria auto atualizável e teria capacidade de criar outros organismos semelhantes. O tema é muito controvertido entre a classe científica e traz inúmeros questionamentos sobre o futuro da humanidade.

Vale destacar que no final de 2017, cansado de ter que esperar seus engenheiros desenvolverem inteligência artificial, a empresa Google criou um algoritmo com capacidade de desenvolver outros algoritmos. Essa tecnologia foi batizada de *AutoML*[267] e deu origem à IA conhecida como *NASNet*.

A título de curiosidade, vale também destacar que Anthony Levandowski, engenheiro automobilístico norte-americano, fundou a primeira igreja que venera inteligência artificial (denominada *Way of the Future*). O objetivo da instituição é garantir o desenvolvimento da SIA, propondo inclusive a extensão de direitos para máquinas.

Embora muitos pensem que atribuir direitos e deveres a robôs seja assunto futurista, a realidade é outra, pois o tema já está sendo considerado e discutido pelos países mais desenvolvidos, conforme será exposto adiante.

3.3 O QUE DIZEM OS ESPECIALISTAS SOBRE O FUTURO

Nick Bostrom[268] é um filósofo sueco que desenvolve parte do seu trabalho sobre risco existencial. É diretor fundador do *Future of Humanity institut (FHI),* um centro de pesquisa criado para estudar ações que podemos adotar na contemporaneidade para garantir um futuro promissor para a humanidade.

Ele acredita que a criação da Inteligência Artificial Geral traria diversos benefícios à sociedade, mas alerta sobre os riscos de rapidamente surgir a Superinteligência, a qual, segundo ele, resultaria no

---

[267] ZOPH, Barret; VASUDEVAN, Vijay; SHLENS, Jonathon; LE, Quoc. **AutoML para classificação de imagens em grande escala e detecção de objetos.** 2017. Disponível em: <https://ai.googleblog.com/2017/11/automl-for-large-scale-image.html>. Acesso em: 30 nov. 2018.

[268] CONTEÚDO aberto. Disponível em: <https://en.wikipedia.org/wiki/Nick_Bostrom> Acesso em: 30 nov. 2018.

fim da humanidade, uma vez que a máquina teria uma condição superior à inteligência humana e conseguiria criar outros organismos semelhantes – o que acabaria por torná-la independente da espécie humana. O filósofo leva o assunto muito a sério e publica diversos artigos sobre o risco e os impactos do desenvolvimento irresponsável da IA[269]. Para ele, antes de prosseguir com o desenvolvimento da tecnologia, deveríamos delimitar princípios e limites para ela.

Stephen Hawking (1942-2018) foi um físico teórico e cosmológico, considerado um dos cientistas mais brilhantes do século[270]. Era membro consultivo do *Institute Future,* que tem como missão minimizar os riscos de extinção da nossa espécie. Em 2016 inaugurou o *Leverhulme Centre for the future of intelligence,* um centro que se dedica a pesquisar o futuro da inteligência.

Hawking demonstrava-se otimista e ao mesmo tempo muito cauteloso quando falava sobre inteligência artificial. Ele era fascinado pelos benefícios que a IA poderia trazer para a sociedade. No entanto, preocupava-se com o desenvolvimento irresponsável da tecnologia.

Segundo o físico, a criação da SIA seria a melhor ou a pior coisa para a humanidade. Durante a sua vida, realizou algumas iniciativas para que a tecnologia fosse desenvolvida sem riscos para os humanos. Em janeiro de 2015, em conjunto com diversos especialistas da área, assinaram uma carta aberta sobre o tema, requerendo uma pesquisa séria sobre os impactos da IA na sociedade.

Em sua obra final[271], aponta que as máquinas superarão a inteligência humana nos próximos 100 anos. Com um desenvolvimento responsável e criação de uma tecnologia que possa ser controlada, o físico aponta para um futuro em que a máquina poderá ser uma extensão do cérebro humano, e acredita que, com essa tecnologia, será possível erradicar a pobreza e diversas doenças, criando-se uma espécie de "admirável mundo novo".

Ray Kurzeil[272] é um futurista norte americano, especializado em fazer previsões sobre tecnologia. Em seu primeiro livro (*The Age of Intelligent Machines*) apontou que até o ano 2000 um computador superaria os melhores humanos no jogo de xadrez – fato este que ocorreu em 1997 com o *Deep Blue*. Em seu segundo livro (*The Age of Spiritual Machines*), dedicou um capÍtulo para fazer previsões para 2009, 2019, 2029 e 2099. De acordo com seu próprio levantamento, teria acertado 86% das previsões realizadas nos anos 1990.

Em suas próximas previsões[273], destaca que em 2029, 2030 e 2047 ocorrerão eventos que mudarão a sociedade que hoje conhecemos. Para 2029 aposta que as máquinas alcançarão o nível de inteligência humana, aumentando muito a capacidade da tecnologia. Para 2030, acredita que será possível conectar o cérebro humano à nuvem. Já para 2047, Kurzeil prevê a singularidade, a criação da Superinteligência artificial, ou seja, o momento em que a inteligência artificial superará toda a inteligência humana. E é neste momento que muitos especialistas temem a extinção da humanidade.

Para o futurista, o evento conhecido como singularidade tecnológica não representaria riscos à espécie humana, pois considera que a máquina seria uma extensão da humanidade, como se o cérebro humano fosse conectado à nuvem.

---

269 BOSTROM, Nick. Disponível em: <https://nickbostrom.com/> Acesso em: 30 nov. 2018.
270 CONTEÚDO aberto. Disponível em: <https://pt.wikipedia.org/wiki/Stephen_Hawking#cite_note-5> Acesso em: 30 nov. 2018.
271 HAWKING, Stephen. **Breves respostas para grandes questões**. Rio de janeiro: Editora Intrínseca LTDA, 2018.
272 CONTEÚDO aberto. Disponível em: <https://en.wikipedia.org/wiki/Ray_Kurzweil> Acesso em: 30 nov. 2018.
273 AGRELA, Lucas. **Máquinas terão inteligência humana em 2029, diz diretor do Google.** 2017. Disponível em: <https://exame.abril.com.br/tecnologia/maquinas-terao-inteligencia-humana-em-2029-diz-diretor-do-google/>. Acesso em: 30 nov. 2018.

O fato é que a tecnologia pode ser utilizada tanto para o bem, quanto para o mal. E isso dependerá de como a sociedade vai conduzir o desenvolvimento da inteligência artificial. O que já é consenso entre os especialistas é que não podemos mais voltar atrás, pois a IA já é uma realidade.

Nesse contexto, o papel dos juristas é trabalhar para que a tecnologia se desenvolva da melhor maneira possível, sem ignorar que o principal objetivo das maiores invenções da humanidade é atender as necessidades da própria sociedade como um todo.

4. ANÁLISE CRÍTICA E JURÍDICA

Tendo em vista que a inteligência artificial tem sido implementada em diversos setores da sociedade – tais como na saúde para diagnóstico de doenças, na segurança para detecção de fraude, no comércio para identificação de perfis de consumidores, dentre outros – é certo que traz consigo muitas implicações na sociedade e na vida das pessoas.

Considerando ainda que a inteligência artificial trabalha com dados e probabilidades, infere-se que pode ser muito útil para auxiliar na resolução de questões objetivas. No entanto, não se pode ignorar que vários dos dados que serão por ela utilizados são eivados de subjetividade e, não raramente, a própria inteligência artificial acaba por atuar na seara subjetiva, seja traçando o perfil de uma pessoa ou entendendo o que é lido ou ouvido de acordo com o contexto.

Além disso, é fato que a inteligência artificial precisa ser alimentada por um banco/base de dados e programada por um humano. Consequentemente, poderá *aprender* errado ou pautar-se em padrões que nem sempre se sabe quais são.

Diante dos variados desafios que o tema suscita, o presente tópico pretende apresentar um breve mapeamento de como os setores público e privado estão trabalhando com o assunto.

4.1 REGULAÇÃO, ÉTICA E CONTROLE

Paralelamente ao desenvolvimento da inteligência artificial, é muito importante que se pense em como regulá-la, de modo que se protejam as pessoas e não se crie um obstáculo à inovação.

Com a evolução de sistemas de mais avançados de inteligência artificial, é certo que se aumentará a probabilidade de danos:

> Isso porque é intrínseco à inteligência artificial: (a) o ímpeto de se autoaperfeiçoar; (b) o desejo de ser racional; (c) a busca pela preservação da utilidade das suas funções; (d) a prevenção da falsificação de seus resultados operacionais ou das suas propriedades funcionais; (e) o desejo de adquirir recursos e usá-los de forma eficiente.[274]

Torna-se imprescindível, portanto, encarar os impactos que o uso de IA pode causar na sociedade, estabelecendo limites necessários para a garantia de direitos individuais e sociais, bem como mecanismos de prevenção e reparação de danos. Ressalte-se que o termo "regulação" no Brasil normalmente está vinculado à ideia de regulação estatal, centralizada, burocrática e lenta. No entanto, quando o assunto é inovação tecnológica, deve-se ter em mente que esse modelo de regulação centralizada não é o mais adequado. Isto porque os avanços e aprimoramentos da tecnologia são muito rápidos, de modo que a lentidão no processo de regulação pode significar sua ineficácia, visto que uma norma rígida pode ficar rapidamente inócua.

Sendo assim, defende-se um modelo de regulação híbrido, em que esteja presente também a autorregulação – que é o modelo que predomina nos Estados Unidos – a qual é conduzida por

---

[274] PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 238-254. p. 244.

agentes do próprio mercado, que protagonizam a criação de normas e políticas pré-estabelecidas em acordos, melhores práticas e códigos de conduta, etc. A partir do momento em que os *players* do mercado passam a se autorregular, é mais provável que estabeleçam diretrizes atualizadas e consonantes com o *status quo* da inteligência artificial, e que passem a respeitar esses padrões impostos - inclusive como um diferencial competitivo.

Para que seja eficaz e cumpra com o seu propósito, tal regulação precisa abarcar desde a fase de desenvolvimento e programação da inteligência artificial, até o momento de implementação e utilização, considerando seus possíveis impactos. Além disso, é necessário que seja realizado um trabalho em conjunto entre empresas, governos, centros de pesquisas e instituições diversas."[275]

Ainda, ao se tutelar juridicamente a inteligência artificial, as discussões de caráter ético e moral não podem ser deixadas de lado, eis que tal tecnologia tem o potencial de interferir consideravelmente nas relações sociais, na vida e nos direitos das pessoas. Sendo assim, deve-se garantir que a IA trate a todos de forma justa e equilibrada, sem discriminar grupos ou pessoas.

Se programada adequadamente, a inteligência artificial pode auxiliar na tomar de decisões mais justas, por trabalhar com a lógica e – em tese – por não possuir preconceitos que influenciam o comportamento humano. No entanto, como os sistemas de IA são projetados por seres humanos e alimentados com dados que refletem o raciocínio humano imperfeito, a inteligência artificial também pode operar de modo injusto.[276] Deve-se ter em conta que "a IA é, de fato, uma revolução tecnológica, porque passa a possibilitar que os programas de computador sejam criativos e desenvolvam, eles próprios, a habilidade de desempenhar ações e chegar a resultados que os seus criadores não eram capazes de alcançar ou de prever. "[277]

Em uma etapa posterior à regulação, entende-se necessário que sejam criados mecanismos de controle que possibilitem uma fiscalização sobre o modo de atuação da inteligência artificial e os padrões por ela utilizados.

De acordo com a *Microsoft*, para promover a segurança e confiabilidade dos sistemas de inteligência artificial, é importante haver uma avaliação sistemática da qualidade e adequabilidade dos dados e modelos utilizados; processos para documentação e auditoria de operações de sistemas de IA; exigência de fornecer explicações adequadas da operação geral do sistema de IA, bem como de envolver especialistas de domínio no seu processo de design e operação quando for usado para fazer decisões com consequências sobre pessoas; avaliação de como e quando um sistema de IA deve procurar auxílio humano em situações críticas; um eficaz mecanismo de *feedback*, para que usuários possam relatar facilmente os problemas de performance que encontrarem."[278]

Tais medidas representam a importância de o operador de sistemas de inteligência artificial ter acesso ao modo como ela trata os dados que lhe são imputados, a fim de compreender - de forma clara e transparente - como ela chega às suas conclusões.

---

[275] ALECRIM, Emerson. Elon Musk quer regular a IA antes que seja tarde demais. **Tecnoblog.** Disponível em: <https://tecnoblog.net/219147/elon-musk-ia-regulamentacao/> Acesso em: 29 nov. 2018.

[276] MICROSOFT. **The Future Computed:** Artificial Intelligence and its role in society. Microsoft Corporation Redmond. Washington, 2018. p. 57.

[277] PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 238-254. p. 242.

[278] MICROSOFT. **The Future Computed:** Artificial Intelligence and its role in society. Microsoft Corporation Redmond. Washington, 2018. p. 64.

4.2 INICIATIVAS EXISTENTES

Do ponto de vista teórico, observa-se que principais universidades do mundo já vêm se preocupando com a necessidade de estudar o tema. O *Massachusetts Institute of Technology* (MIT), por exemplo, anuncia a criação da Universidade de Inteligência Artificial para 2019, voltada para o uso "responsável e ético" da tecnologia. Há também muitos centros de pesquisas que tem fomentado estudos parecidos, tais como o "Codex, da Universidade de Standford; o Cirsfid, centro de Informática Jurídica da Universidade de Bologna; o programa de Sistemas Inteligentes, da Universidade de Pittsburgh; o centro de Direito e Tecnologia da Informação do King's College" [279], dentre outros. Além dos centros congêneres de pesquisa, verifica-se também inovações nos currículos dos cursos de Direito, que passam a aliar o ensino de lógica jurídica ao de lógica de programação e a incubar *lawtechs*.[280]

No Brasil, destaca-se o *think tank (laboratório de ideias)* da USP, denominado *Lawgorithm***,** criado por um grupo de professores de Engenharia, Ciência da Computação, Filosofia e Direito, com o objetivo de "articular a pesquisa acadêmica e a formação universitária com as iniciativas práticas, nos setores público e privado, de desenvolvimento de ferramentas computacionais para a atividade jurídica, bem como para refletir sobre as implicações jurídicas, sociais, econômicas e culturais da inteligência artificial em geral." [281]

Do ponto de vista regulatório, verifica-se que as iniciativas relacionadas ao tratamento jurídico de inteligência artificial também estão avançando.

Na União Europeia, o Parlamento Europeu aprovou uma Resolução[282] com recomendações à Comissão Europeia, de que se crie uma espécie de personalidade jurídica para robôs autônomos e inteligentes. Seria a chamada "*e-personality*" ou "*personalidade eletrônica*".

De acordo com a Resolução, considera-se robô inteligente aquele que conta com determinadas características, tais como: aquisição de autonomia através de sensores e/ou da troca de dados com o seu ambiente (interconetividade) e da troca e análise desses dados; autoaprendizagem com a experiência e com a interação (critério opcional); um suporte físico mínimo; adaptação do seu comportamento e das suas ações ao ambiente; inexistência de vida no sentido biológico do termo.

A Resolução prevê ainda a necessidade de implementação de um sistema abrangente de registro de robôs inteligentes, bem como a criação de um regime de seguros obrigatórios, para arcar com eventuais danos causados por esses robôs. [283]

Não obstante o avanço que o Resolução representa, deve-se considerar que suas disposições se limitam a uma iniciativa voltada à reparação civil de eventuais danos causados por robôs. Além de

---

[279] MARANHÃO, Juliano. A pesquisa em inteligência artificial e Direito no Brasil. **Revista Consultor Jurídico**, 2017. Disponível em: <https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais> Acesso em: 29 nov. 2018.
[280] MARANHÃO, Juliano. A pesquisa em inteligência artificial e Direito no Brasil. **Revista Consultor Jurídico**, 2017. Disponível em: <https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais> Acesso em: 29 nov. 2018.
[281] MARANHÃO, Juliano. A pesquisa em inteligência artificial e Direito no Brasil. **Revista Consultor Jurídico**, 2017. Disponível em: <https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais> Acesso em: 29 nov. 2018.
[282] Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)).
[283] UNIÃO EUROPEIA. **Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com recomendações à Comissão de Direito Civil sobre Robótica (2015/2103(INL)).** Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//PT#BKMD-12>. Acesso em 29 nov. 2018.

não se debruçar sobre um estatuto jurídico e abrangente desses robôs, a proposta também não prevê responsabilização no âmbito criminal.

Destaque-se também que o poder legislativo de Nova York aprovou, em 2017, uma lei voltada a garantir a transparência dos algoritmos utilizados pela Administração Pública para auxiliar na tomada automatizada de decisões. O objetivo era evitar problemas relacionados a algoritmos de decisão, bem como lidar com problemas já existentes. Isso seria concretizado por meio da criação de critérios para uma auditoria; do desenvolvimento de um procedimento para esclarecimento de cidadãos afetados; da viabilização de análise sobre o uso de algoritmos, a fim de identificar se a decisão impacta desproporcionalmente em pessoas - se utiliza critérios baseados em idade, cor da pele, crenças, religião, nacionalidade de origem, gênero, deficiências, estado civil, orientação sexual, cidadania, etc. – e da criação de um procedimento para tratar de casos nos quais uma pessoa tenha sido prejudicada por um sistema de decisão automatizada. [284]

Ainda, no âmbito privado observa-se iniciativas como "*Partnership on AI*" - da qual participam empresas como a Amazon, Facebook, DeepMind, Google, Apple, IBM e Microsoft - sem fins lucrativos, que tem como finalidade "estudar e formular boas práticas para tecnologias baseadas em inteligência artificial, permitindo sua evolução para um caminho que ajude a humanidade, e não o contrário".[285]

Por fim, ressalta-se que, apesar de haver unanimidade quanto à importância de se legislar sobre inteligência artificial, não há consenso sobre a urgência de criação dessas normas. A Microsoft esclarece que as necessidades específicas a serem reguladas ainda serão descobertas.[286] Elon Musk, por outro lado, entende que precisamos ser proativos ao estabelecer uma regulamentação, pois se formos reativos, poderá ser tarde demais, visto que a IA "atingirá um nível de sofisticação tão grande que permitirá que robôs atuem absolutamente em todas as áreas que, hoje, são mantidas com trabalho humano." [287]

---

[284] INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS. Int**eligência Artificial e Regulação**: O caso de Nova York. Disponível em: **<**http://irisbh.com.br/inteligencia-artificial-e-regulacao-o-caso-de-nova-york/> Acesso em: 29 nov. 2018.

[285] PROJURIS. **Avanços de inteligência artificial exigem novas leis e regulação, diz Microsoft**. Disponível em: <https://www.projuris.com.br/inteligencia-artificial-novas-leis-regulacao-governamental-diz-microsoft/> Acesso em: 29 nov. 2018.

[286] PROJURIS. **Avanços de inteligência artificial exigem novas leis e regulação, diz Microsoft**. Disponível em: <https://www.projuris.com.br/inteligencia-artificial-novas-leis-regulacao-governamental-diz-microsoft/> Acesso em: 29 nov. 2018.

[287] ALECRIM, Emerson. Elon Musk quer regular a IA antes que seja tarde demais. **Tecnoblog.** Disponível em: <https://tecnoblog.net/219147/elon-musk-ia-regulamentacao/> Acesso em: 29 nov. 2018.

5. CONSIDERAÇÕES FINAIS

A partir das reflexões relacionadas à inteligência artificial, desde a compreensão de seu conceito, de como vem sendo implementada em diferentes setores e do que se pode dela esperar no futuro, infere-se que se trata de um campo com grande potencial de evolução e de transformação da sociedade.

A utilização de sistemas de inteligência artificial por empresas, governos e instituições diversas – cada qual com suas próprias finalidades - demonstra que, na prática, trata-se de uma ferramenta à disposição da humanidade. Portanto, é imperioso que se saiba como utilizá-los da melhor maneira possível.

Propõe-se, portanto, uma atuação multisetorial voltada ao estudo do assunto, pautando-se sempre em princípios éticos básicos, tais como os apresentados no Relatório Britânico lançado em 2018, os quais estabelecem que: os sistemas de inteligência artificial devem ser desenvolvidos para o bem comum e o benefício da humanidade; não devem ser usadas para diminuir a proteção de dados ou a privacidade dos indivíduos, famílias e comunidades; devem operar de acordo com os princípios da inteligibilidade e justiça, dentre outros.[288]

Nesse sentido, a preocupação e atuação do Direito é salutar. Os impactos e implicações do uso de tal tecnologia na vida das pessoas precisam ser analisados e, quando inadequados, mitigados. Para tanto, percebe-se que – apesar das iniciativas apresentadas – ainda há muito o que se desenvolver no campo da pesquisa, da regulação e da criação de mecanismos de controle da inteligência artificial, a fim de que seja tratada de forma totalmente responsável por todos os seus operadores, bem como por integrantes da sociedade que possam com ela contribuir.

[288] O GLOBO. **Parlamento britânico recomenda regulação da inteligência artificial.** Disponível em: <https://oglobo.globo.com/economia/parlamento-britanico-recomenda-regulacao-da-inteligencia-artificial-22595390> Acesso em: 30 nov. 2018.

6. REFERÊNCIAS BIBLIOGRÁFICAS

AGRELA, Lucas. **Máquinas terão inteligência humana em 2029, diz diretor do Google**: 2017. Disponível em: <https://exame.abril.com.br/tecnologia/maquinas-terao-inteligencia-humana-em-2029-diz-diretor-do-google/>. Acesso em: 30 nov. 2018.

ALECRIM, Emerson. Elon Musk quer regular a IA antes que seja tarde demais. **Tecnoblog.** Disponível em: <https://tecnoblog.net/219147/elon-musk-ia-regulamentacao/> Acesso em: 29 nov. 2018.

BALAGO, Rafael. Empresas de aluguel de bike sofisticam serviço com inteligência artificial. **Folha de S. Paulo**, 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/10/empresas-de-aluguel-de-bike-sofisticam-servico-com-inteligencia-artificial.shtml>. Acesso em: 20 nov. 2018.

BHARGAVA, Rohit. **O futuro das máquinas é invisível.** 2018. Disponível em: <https://gq.globo.com/Prazeres/Tecnologia/noticia/2018/02/o-futuro-das-maquinas-e-invisivel.html>. Acesso em: 30 nov. 2018.

BOSTROM, Nick. Disponível em: <https://nickbostrom.com/> Acesso em: 30 nov. 2018.

CNJ: Corregedor fala sobre os impactos da inteligência artificial no Direito. **TRF2**, 2018. Disponível em: <http://www10.trf2.jus.br/portal/cnj-corregedor-fala-sobre-os-impactos-da-inteligencia-artificial-no-direito/>. Acesso em: 29 nov. 2018.

CONSENTINO, Marcelo. Inteligência Artificial. **O Estado da Arte**, 2018. Disponível em: <http://oestadodaarte.com.br/inteligencia-artificial/>. Acesso em: 28 nov. 2018.

CONTEÚDO aberto. In: Wikipédia: a enciclopédia livre. Disponível em: <https://en.wikipedia.org/wiki/Nick_Bostrom> Acesso em: 30 nov. 2018.

CONTEÚDO aberto. In: Wikipédia: a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/Stephen_Hawking#cite_note-5> Acesso em: 30 nov. 2018.

CONTEÚDO aberto. In: Wikipédia: a enciclopédia livre. Disponível em: <https://en.wikipedia.org/wiki/Ray_Kurzweil> Acesso em: 30 nov. 2018.

Future Today Institute. Disponível em: <https://futuretodayinstitute.com/>. Acesso em: 30 nov. 2018.

GUBERN, Román. **O Eros eletrônico**. Disponível em: <https://www.scribd.com/document/124062697/O-Eros-Eletronico-Roman-Gubern>. Acesso em: 28 nov. 2018.

HAWKING, Stephen. **Breves respostas para grandes questões**. Rio de janeiro: Editora Intrínseca LTDA, 2018.

IBM. **Deep Blue**. Disponível em: <https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/> Acesso em: 30 nov. 2018

IBM. **Oncology and Genomics**. 2018. Disponível em: <https://www.ibm.com/watson/br-pt/health/oncology-and-genomics/>. Acesso em: 27 nov. de 2018.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS. Int**eligência Artificial e Regulação**: O caso de Nova York. Disponível em: **<**http://irisbh.com.br/inteligencia-artificial-e-regulacao-o-caso-de-nova-york/> Acesso em: 29 nov. 2018.

MARANHÃO, Juliano. A pesquisa em inteligência artificial e Direito no Brasil. **Revista Consultor Jurídico**, 2017. Disponível em: <https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais > Acesso em: 29 nov. 2018.

MICROSOFT. **The Future Computed:** Artificial Intelligence and its role in society. Microsoft Corporation Redmond. Washington, 2018.

NORVIG, Peter; RUSSEL, Stuart. **Inteligência Artificial**. Rio de Janeiro: Elsevier Editora Ltda., 2013.

O GLOBO. **Parlamento britânico recomenda regulação da inteligência artificial.** Disponível em: **<**https://oglobo.globo.com/economia/parlamento-britanico-recomenda-regulacao-da-inteligencia-artificial-22595390> Acesso em: 30 nov. 2018.

PARESH, Dave. Facebook removes 8.7 million sexual photos of kids in last three months. **REUTERS**, 2018. Disponível em: < https://ca.reuters.com/article/technologyNews/idCAKCN1MY1SE-OCATC>. Acesso em: 23 de nov. 2018.

PGMAIS**. Uso de inteligência artificial leva PGMais e Bellinati Perez para final do Prêmio Best Performance**. Disponível em: <http://pgmais.com.br/noticias/uso-de-inteligencia-artificial-leva-pgmais-e-bellinati-perez-para-final-do-premio-best-performance/>. Acesso em: 25 nov. 2018.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, nº 3, 2017 p. 238-254.

PROJURIS. **Avanços de inteligência artificial exigem novas leis e regulação, diz Microsoft**. Disponível em: <https://www.projuris.com.br/inteligencia-artificial-novas-leis-regulacao-governamental-diz-microsoft/> Acesso em: 29 nov. 2018.

REDAÇÃO GALILEU. **Arábia Saudita torna-se primeiro país a conceder cidadania para um robô.** 2017. Disponível em: <https://revistagalileu.globo.com/Tecnologia/noticia/2017/10/arabia-saudita-torna-se-primeiro-pais-conceder-cidadania-para-um-robo.html>. Acesso em: 30 nov. 2018.

SEARLE, John R. Minds, brains and programs. In: ____. **Behavioral and brain sciences**. vol. 3. Cambridge University Press, 1980.

TERRA. **Como a inteligência artificial e *machine learning* ajudam a segurança da informação**. 2018. Disponível em: <https://www.terra.com.br/noticias/dino/como-a-inteligencia-artificial-e-machine-learning-ajudam-a-seguranca-da-informacao,9cfec9e8c5765408911fae2856034028frjpag2u.html>. Acesso em: 28 nov. 2018.

UNIÃO EUROPEIA. **Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com recomendações à Comissão de Direito Civil sobre Robótica (2015/2103(INL)).** Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//PT#BKMD-12>. Acesso em 29 nov. 2018.

WEBB, Amy. **Tech Trends Report.** 2018. Disponível em: <https://futuretodayinstitute.com/2018-tech-trends-annual-report/>. Acesso em: 30 nov. 2018.

ZOPH, Barret; VASUDEVAN, Vijay; SHLENS, Jonathon; LE, Quoc. **AutoML para classificação de imagens em grande escala e detecção de objetos**: 2017. Disponível em: <https://ai.googleblog.com/2017/11/automl-for-large-scale-image.html>. Acesso em: 30 nov. 2018.

ONLINE DISPUTE RESOLUTION (ODR) EM PERSPECTIVA INTERNACIONAL E ANÁLISE CRÍTICA

ONLINE DISPUTE RESOLUTION (ODR) IN THE INTERNATIONAL PERSPECTIVE AND CRITICAL ANALYSIS

Guilherme Hideo Oshima

É advogado (OAB/PR n° 91.778) e pesquisador do Núcleo de Estudos em Direito Civil-Constitucional da UFPR Pós-graduando em Direito Imobiliário pela Universidade Positivo. Membro da Câmara de Inovação e Tecnologia do Instituto de Engenharia do Paraná.

Laísa Fernanda Alves Vieira

É advogada (OAB/PR n° 88.651) e mestranda em Direito das Relações Sociais pela Universidade Federal do Paraná, pós-graduada em Direito Público pela ESMAFE/PR e graduada pela Universidade Federal do Paraná. Atualmente, é Diretora Acadêmica da Comissão da Advocacia Iniciante da OAB/PR.

RESUMO:
Com a era de transformação digital trazida pela revolução 4.0, os meios eletrônicos de solução de conflitos passaram a integrar o rol de serviços oferecidos por órgãos administrativos. Por meio de plataformas digitais, de natureza pública ou privada, os cidadãos podem ter acesso, de forma virtual, aos métodos adequados de resolução de conflitos. Fomenta-se a cultura do consenso e da pacificação social em detrimento da litigância. Diante da popularização da *Online Dispute Resolution* (ODR), faz-se necessário investigar a sua correlação com o perfil do consumidor atual. Tais mudanças, amparadas pela sociedade da informação, impactaram diretamente nas cadeias produtivas das empresas. Debate-se como estas ferramentas podem atender as necessidades de urgência e imediatismo deste consumidor virtual. Assim, na primeira parte do artigo se discute acerca dessas transformações consumeristas. Na segunda parte, trata-se dos reflexos da informatização na construção de mecanismos *online* de solução de conflitos que sejam efetivos. Posteriormente, o trabalho trata de panoramas para a efetividade da ODR, refletindo sob um viés internacional.

Palavras-chave: Resolução Online de Conflitos; Perfil do Consumidor virtual; ODR na perspectiva internacional.

ABSTRACT: *With the era of digital transformation brought about by the revolution 4.0, the electronic means of conflict resolution began to integrate the list of services offered by administrative bodies. Through digital platforms, public or private, citizens can have virtual access to appropriate methods of conflict resolution. It encourages the culture of consensus and social pacification to the detriment of litigation. Faced with the popularization of Online Dispute Resolution (ODR), it is necessary to investigate its correlation with the current consumer profile. Such changes, supported by the information society, had a direct impact on the productive chains of companies. Discuss how these tools can meet the urgency and immediacy needs of this virtual consumer. Thus, the first part of the article discusses these consumerist transformations. In the second part, it is the reflexes of the computerization in the construction of online mechanisms of solution of conflicts that are effective. Subsequently, the paper deals with scenarios for the effectiveness of ODR, reflecting an international bias.*

Keywords: *Online Dispute Resolution. The profile of the virtual consumer. ODR in international perspective.*

INTRODUÇÃO

A agilidade da informação transformou as relações pessoais e profissionais. Estar conectado representa atualização, socialização, automatização e consumo.

No que tange aos impactos na vida pessoal, denota-se que este é o cenário da sociedade de hiperconsumo, em que o consumo se torna, cada vez mais, norteador da felicidade e da identidade[289]. Trata-se, portanto, de um estágio de "modernidade líquida", em que tudo é "fluido, amorfo, veloz, instantâneo, efêmero"[290].

Esta necessidade pautada, principalmente, pela celeridade, transparece também nas relações profissionais. Do mesmo modo, no que tange às carreiras jurídicas, "a agilidade passou a ser essência da profissão. E é curioso, porque isso faz com que a advocacia, que é uma profissão de pressão contínua, agora tenha a pressão cronológica, a pressão do tempo"[291].

Apesar de evidente a necessidade de celeridade e efetividade na resolução de conflitos, conforme demonstrado anteriormente, observa-se que estas demandas infelizmente não refletem na prestação do serviço jurisdicional.

Somente no ano de 2017, denota-se o ajuizamento de 1.234.983 demandas nos Juizados Especiais Cíveis, apenas sobre temas da Responsabilidade Civil do Fornecedor e Indenizações por Dano Moral, na seara do Direito do Consumidor[292]. Nessa esteira, o tempo médio até a sentença nos casos supramencionados é de 10 meses, enquanto o tempo médio até a baixa destes é de 1 ano e 9 meses[293].

Extrai-se deste contraste entre efetividade e alto número de demandas consumeristas, a imprescindibilidade de meios alternativos de solução de conflitos para suprir a carência da efetiva prestação da tutela jurisdicional.

Em paralelo ao cenário apresentado, o surgimento de novas ferramentas tecnológicas demonstra-se como meio para o alcançar "benefícios de custo, sigilo, rapidez e eficácia em relação ao processo judicial, sem necessidade de deslocamento físico"[294].

Assim, em que pese não restrita às relações de consumo virtuais, as ferramentas para resolução de disputas dotadas de ferramentas tecnológicas, ou inseridas no ambiente online, isto é, as *Online Dispute Resolution* (ODR)[295], apresentam-se como instrumentos adequados e céleres para a resolução destes conflitos.

---

289 OLIVEIRA, Andressa Jarletti Gonçalves de. *Defesa Judicial do Consumidor Bancário*. Curitiba: Rede do Consumidor. 2014. p. 27-28.

290 *Ibid*. p. 27. Ainda: BAUMAN, Zygmunt. *Modernidade Líquida*. Tradução: Plínio Dentzien – Rio de Janeiro: Zahar, 2001. p. 98.

291 HUCK, Hermes Marcelo. *O Brasil e a globalização: pensadores do direito internacional*. Organização: Maurício Almeida Prado, Renata Duarte de Santana – São Paulo: Editora de Cultura, 2013. p. 37.

292 CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números 2018: ano-base 2017*. Brasília: CNJ, 2018. p. 184.

293 CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números 2018: ano-base 2017*. Brasília: CNJ, 2018. p. 144.

294 ANDRADE, Henrique dos Santos; MARCACINI, Augusto. Os novos meios alternativos ao judiciário para a solução de conflito, apoiados pelas tecnologias da informação e comunicação. *Revista de Processo*, vol. 268/2017, Revista dos Tribunais Online, Junho. 2017. p. 587-612.

295 BHARUKA, Devashish; Online Dispute Resolution. In: VERMA, S.K.; MITTAL, Raman. Legal *Dimensions on Cyber Space*. New Delhi: Indian Law Institute, 2004. p. 309. Disponível em: < http://14.139.60.114:8080/jspui/handle/123456789/722>.

Para tanto, a seguir, faz-se necessário compreender o perfil do usuário/ consumidor virtual, para que, posteriormente, estas características sejam enquadradas e direcionadas para a construção e modelagem de meios online de resolução de conflitos.

2. O PERFIL DO CONSUMIDOR VIRTUAL

A era digital alterou radicalmente os conceitos de urgência, necessidade, individualidade e identidade. Tal fato pode ser observado sob o prisma dos novos perfis de consumidores.

Nesse contexto, a "Global Consumer Insights Survey 2018"[296], desenvolvida pela PwC, apontou que, em pesquisa realizada com 22,481 consumidores, de 2013 até 2018, a frequência com que os consumidores utilizam os celulares e *tablets* para efetuarem compras aumentou em 10% e 4%, respectivamente.

Além disso, com relação a aquisição de produtos via celular em uma frequência mensal, a pesquisa "Retail & Consumer Report 2018"[297] destacou que 41% dos consumidores que residem no Reino Unido já possuem este hábito, enquanto 83% dos consumidores chineses já atingem deste perfil.

Ainda, somente no Brasil, no primeiro semestre de 2018, os pedidos online por consumidores atingiram o número de 17,4 milhões, enquanto o faturamento do *e-commerce*, neste mesmo período, alcançou a casa de 6,7 bilhões de reais[298].

Não somente o perfil do consumidor, mas gigantes do mercado também passaram por uma transformação, em especial digital, de seus modos de operação. Empresas do varejo norte americano, como *Walmart*, reestruturaram suas estratégias de negócios e migraram para o comércio digital[299], enquanto outras empresas que não se atentaram ao novo estilo de consumo, tais como *Toys'R'Us*, *Radio Shack*, *Payless Shoesource*, declararam falência ou encerraram atividades de lojas físicas[300].

Diante deste cenário, observa-se que a conectividade transformou o comportamento do consumidor e impactou diretamente na cadeia produtiva das empresas. Permite-se descobrir e comprar quando e onde o consumidor desejar. Assim, denota-se que a tecnologia se enraizou no cotidiano dos consumidores, de modo que estes compreendem o acesso instantâneo como regra[301].

---

[296] PwC. *Global Consumer Insights Survey 2018*: New business models in the e-commerce era. Disponível em: <https://www.pwc.com/gx/en/retail-consumer/assets/business-models-global-consumer-insights-survey.pdf>. p. 06.

[297] PwC. *Retail & Consumer Report 2018*. Disponível em: < https://www.pwc.ie/publications/2018/retail-consumer-report-2018.pdf>. p. 12.

[298] Ebit. *Webshoppers Elo*. 38ª Ed., 2018. p. 12. Disponível em: < http://www.fecomercio.com.br/public/upload/editor/ws38_vfinal.pdf>

[299] Deloitte. *Global Powers of Retailing 2018*: Transformative change, reinvigorated commerce. p. 06. Disponível em: < https://www2.deloitte.com/content/dam/Deloitte/at/Documents/about-deloitte/global-powers-of-retailing-2018.pdf>.

[300] Tal evento remete-se ao "*retail apocalypse*", em que grandes empresas do varejo encerraram suas atividades em lojas físicas. Destaca-se que o movimento superveniente com foco em modular os negócios para atividades relacionadas ao e-commerce, apesar de nova estratégia, não é a causa principal destes acontecimentos envolvendo pedidos de falência e encerramento de atividades. Sobre o *retail apocalypse*: HOLMAN, Lee. BUZEK, Greg. *Debunking the retail apocalypse*. Ago. 2017. Disponível em: <https://www.business.att.com/content/dam/attbusiness/insights/campaigns/retail-apocalypse/debunking-the-retail-apocalypse.pdf>. Ainda: BARRABI, Thomas. Retail Apocalypse: These big retailers closing stores, filing for bankruptcy. FOXBusiness. 04 abr. 2018. Disponível em: <https://www.foxbusiness.com/retail/features-retail-apocalypse-bankruptcy-stores-closing>. Acesso em: 16 de março de 2019.

[301] KPMG. *Global retail trends 2018*: Global Consumer & Retail. Mar, 2018. p. 19. Disponível em: < https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/global-retail-trends-2018.pdf>.

Em que pese a revolução digital tenha impacto direto nos meios de comunicação e, cada vez mais, nos hábitos de consumo, a aproximação da tecnologia com outros segmentos, em especial o Direito, tem-se demonstrada tímida.

Nessa lógica, traduzir as demandas do consumidor virtual de instantaneidade, facilidade de acesso e interatividade para o contexto jurídico é uma alternativa para viabilizar o efetivo acesso à justiça.

Sendo estas características e vantagens das *Online Dispute Resolutions*[302], passa-se, portanto, a debater sobre como estas ferramentas podem atender efetivamente estas necessidades de urgência, imediatismo e conveniência para o consumidor virtual.

2.1 REFLEXOS DA INFORMATIZAÇÃO NA CONSTRUÇÃO DE EFETIVOS MECANISMOS ONLINE DE SOLUÇÃO DE CONFLITOS

O descompasso entre a celeridade de resolução das demandas e a instantaneidade, regra da sociedade da informação, é o reflexo do atual sistema judiciário brasileiro[303]. Soma-se a este congestionamento, o fato da extrema judicialização, em que os litigantes cogitam que "o direito de ação teria sido convertido em espécie de dever de promovê-la"[304].

Além disso, no âmbito nacional, pode-se considerar três obstáculos para o acesso à justiça, quais sejam: a barreira econômica, o âmbito geográfico e a burocracia[305].

A primeira refere-se aos custos e o tempo dispendido no processo, de modo que tais despesas, cumuladas ao procedimento temporalmente prolongado, ultrapassem até o valor e a necessidade do bem objeto da demanda[306].

Por sua vez, as dificuldades de âmbito geográfico residem na impossibilidade do indivíduo identificar e defender direitos da coletividade, em razão da incomunicabilidade dos mesmos sujeitos de direito, os quais não podem se beneficiar de uma estratégia jurídica comum[307].

Por fim, a barreira de ordem burocrática é aquela em que o cidadão comum esbarra ao tentar formular sua pretensão em face de litigantes experientes, bem como desconhecer as peculiaridades de cunho procedimental[308].

Diante deste contexto, preconizou-se o estímulo aos meios alternativos de solução de conflitos, nos termos do art. 3º, do Código de Processo Civil de 2015. Dessa forma, o incentivo para que as partes

---

302 LIMA, Gabriel Vasconcelos. FEITOSA, Gustavo Raposo Pereira. Online Dispute Resolution (ODR): a solução de conflitos e as novas tecnologias. *Revista do Direito*. Santa Cruz do Sul, v. 3, n. 50, p. 53-70, set./ dez/ 2016. Disponível em: < https://online.unisc.br/seer/index.php/direito/index>.

303 COUTO, Mônica Bonetti. CRUZ, Luana Pedrosa de Figueiredo. Desjudicialização e Novo Código de Processo Civil: análise à luz das técnicas inseridas no sistema processual brasileiro. Revista de Processo. Vol. 271/2017. p. 405-425. Set. 2017. Revista dos Tribunais Online.

304 *Ibid*.

305 PINHO, Humberto Dalla Bernardina de. STANCATI, Maria Martins Silva. A Ressignificação do Princípio do Acesso à Justiça à luz do Art. 3º do CPC/2015. Revista de Processo, vol. 256/2016. p. 17-44. Abr. 2016. Revista dos Tribunais Online.

306 *Ibid*.

307 *Ibid.*

308 *Ibid*.

adotem uma das múltiplas portas para resolução do conflito, é reflexo de que a via judicial, apesar de sempre aberta, não necessariamente deve ser adotada como primeira opção[309].

Nessa esteira, é ascendente a utilização de mecanismos alternativos de solução de conflitos (ADR), uma vez que, além de ultrapassar a barreira burocrática, salvando tempo e dinheiro por meio de soluções eficientes extrajudiciais, as ADRs apresentam-se como soluções amigáveis, com viés de composição e manutenção do vínculo jurídico entre as partes[310].

Adiciona-se aos benefícios supramencionados a demanda por conectividade e soluções instantâneas, em que o acesso à justiça possa ser concretizado a qualquer tempo e de qualquer lugar. É em virtude destas características que emergem as plataformas *online* de solução de conflitos, as ODRs[311].

Apesar de se caracterizar como ferramenta prática e efetiva para a solução de conflitos de partes que encontram-se compelidas ao acesso à justiça, ora por questões geográficas, ora por questões econômicas[312], o acesso aos meios online de solução de conflitos também apresentam dificuldades para acesso e aceitação.

Não se ignora o fato de que, no Brasil, um dos pilares desta dificuldade é a própria integração do cidadão aos canais online. Somente 64,7% da população brasileira acima de 10 anos encontra-se conectada à internet[313].

Outrossim, a doutrina aponta que a adesão da ODR depende, principalmente, da demonstração de segurança, confiança e juridicamente eficaz, com decisões vinculantes[314].

Nesse sentido, a seguir, passar-se-á a demonstrar como diversas instituições e o poder judiciário procuram efetivar a confiança em plataformas ODR, de modo a transformarem o procedimento de solução de conflitos online seguro e fornecedor de decisões vinculantes.

---

309 NASCIMBENI, Asdrubal Franco. Os meios extrajudiciais de solução de conflitos como forma adequada de pacificação social e a tendência à desjudicialiazação. Revista de Arbitragem e Mediação. Vol. 52/2017. p. 221-258. Jan. – Mar., 2017. Revista dos Tribunais Online.

310 KATSH, Ethan. RIFKIN, Janet. Online Dispute Resolution: resolving conflicts in cyberspace. San Francisco: Jossey-Bass, 2001. p. 29.

311 Ibid. p. 26-27.

312 KATSH. Ethan. Online Dispute Resolution: some implications for the emergence of law in cyberspace. Lex Electronica. Vol. 10, nº 3, 2006. Disponível em: < http://www.lex-electronica.org/articles/v10-3/katsh.htm>.

313 GOMES, Helton Simões. Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. G1. 21 fev. 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>.

314 KATSH, Ethan. RIFKIN, Janet. *Op. cit*. p. 23. BHARUKA, Devashish. *Op. cit.* p. 318. KATSH, Ethan. *Op. cit*. p. 06.

3. CREDIBILIDADE E ACESSIBILIDADE – PANORAMAS PARA A EFETIVIDADE DA ODR

O interesse na adoção de ferramentas online para a solução de conflitos, conforme abordado anteriormente, deve apresentar confiança, segurança, celeridade e conveniência ao usuário, isto é, a ODR deve ser modelada para fornecer uma confortável jornada ao consumidor/ usuário *online*.

Em razão destes princípios, observa-se um movimento global de difusão e adoção destas plataformas, bem como o estabelecimento de boas práticas para que a solução de conflitos online garanta o efetivo e célere acesso à justiça.

Assim, em sequência, será demonstrado como e quais as medidas adotadas por instituições e governos para concretizar a ODR como ferramenta de garantia de direitos.

3.1 A NECESSÁRIA CHANCELA INSTITUCIONAL E GOVERNAMENTAL SOB A PERSPECTIVA INTERNACIONAL

O debate acerca de boas práticas em solução de conflitos por meio de plataformas online tem destaque em 2002, em virtude da publicação do "*Addressing Disputes in Electronic Commerce*" pela *American Bar Association's Task Force on Electronic Commerce and Alternative Dispute Resolution*.

Neste parecer, examinou-se as principais causas e disputas decorrentes de transações efetuadas via *e-commerce*, bem como prevenir ou remediar tais impasses[315].

Para tanto, primeiramente, a *Task Force* identificou as principais preocupações do consumidor virtual em face de transações via comércio eletrônico, quais sejam: falta de confiança nos serviços financeiros online, possibilidade de fraude, omissões sobre custos, procedimentos e utilização de dados, bem como indisponibilidade de linguagem de fácil compreensão e acessível ao consumidor[316].

Em virtude deste cenário e da necessidade de propagar a ODR como mecanismo de solução de conflito, o relatório apresentou um guia de boas práticas para atingir este fim.

Diante disso, o anexo "A", do "Recommended Best Practices by Online Dispute Resolution Service Providers", do "*Addressing Disputes in Electronic Commerce*", destacou a necessidade das plataformas ODR apresentarem transparência, informação, acessibilidade à tecnologia, privacidade, confidencialidade e limitações jurisdicionais.

Com relação ao direito à informação e transparência, as ferramentas online de solução de conflitos devem priorizar a demonstração de resultados obtidos por meio da plataforma, informações para contato, tratamento de dados pessoais, termos e condições de uso, com destaque para a descrição dos serviços oferecidos e o procedimento adotado pela plataforma[317].

---

315 AMERICAN BAR ASSOCIATION'S TASK FORCE ON ELECTRONIC COMMERCE AND ALTERNATIVE DISPUTE RESOLUTION IN COOPERATION WITH THE SHIDLER CENTER FOR LAW, COMMERCE AND TECHNOLOGY, UNIVERSITY OF WASHINGTON SCHOOL OF LAW. Addressing Disputes in Electronic Commerce: Final Recommendations and Report. *The Business Lawyer*, vol. 58, no. 1, 2002, pp. 415–477. *JSTOR*. Disponível em: <www.jstor.org/stable/40688128>. p. 422-423.

316 *Ibid*. p. 10.

317 AMERICAN BAR ASSOCIATION'S TASK FORCE ON ELECTRONIC COMMERCE AND ALTERNATIVE DISPUTE RESOLUTION IN COOPERATION WITH THE SHIDLER CENTER FOR LAW, COMMERCE AND TECHNOLOGY, UNIVERSITY OF WASHINGTON SCHOOL OF LAW. *Op. cit.* p. 460-462.

Ademais, preconiza-se pela transparência e informação acerca dos custos referentes ao uso da plataforma, bem como da nomeação, independência e imparcialidade de eventuais terceiros indicados pela plataforma para mediarem conflitos[318].

Além disso, recomenda-se a inclusão de diversas tecnologias, tais como áudio, vídeo e texto, para que também ocorra a inclusão de pessoas com deficiências físicas, visuais ou auditivas[319].

Por fim, sugere-se a indicação dos limites jurisdicionais dos acordos ou decisões firmadas no âmbito das ODR, no intuito de providenciar a devida eficácia e validade do acordo ou decisão[320].

Tais parâmetros também foram observados na redação do Regulamento nº 524/2013, do Parlamento Europeu, em que estabeleceu-se parâmetros para a criação deu uma plataforma ODR europeia para a solução de conflitos consumeristas[321].

Desta iniciativa, tanto fornecedores, como consumidores podem submeter a solução de seus conflitos para apreciação por uma plataforma ODR endossada e providenciada pela Comissão Europeia[322].

Cumpre destacar que, sob o prisma das transações internacionais, a *United Nations Commission on International Trade Law* (UNCITRAL) também se preocupou em desenvolver parâmetros técnicos para assegurar a simplicidade, celeridade, flexibilidade e segurança das ODR.

Nessa esteira, a instituição publicou, em 2017, a "UNCITRAL Technical Notes on Online Dispute Resolution", em que, em síntese, preconizou os princípios da independência, transparência e consentimento, para assegurar o devido processo legal por meio destas plataformas *online*[323]. Estas notas técnicas ainda estabeleceram parâmetros acerca dos estágios de negociação e mediação a serem considerados pelos provedores de ODR[324].

Previsões e expectativas sobre a ODR também são veiculadas pelo sistema judiciário do Reino Unido. Para tanto, o *Civil Justice Council's Advisory Group on Online Dispute Resolution* publicou, em fevereiro de 2015, como as ferramentas tecnológicas, em especial a ODR, podem repensar o acesso à justiça.

Assim, recomendou-se a criação da HM *Online Court* (HMOC), isto é, um sistema *online* para a resolução de demandas cujo valor da causa é abaixo de £10.000,00 (dez mil libras) e de baixo grau de complexidade[325].

Nesse contexto, o HMOC, baseado em um sistema online de solução de conflitos, atuaria de modo a evitar o conceito de disputa e prevenindo a criação de impasses jurídicos.

---

318 *Ibid*. p. 463-467.
319 *Ibid*. p. 462.
320 *Ibid*. p. 468.
321 UNIÃO EUROPEIA. Regulamento (UE) nº 524/2013 do Parlamento Europeu e do Conselho, de 21 de maio de 2013. Disponível em: < https://www.triave.pt/wp-content/uploads/Regulamento-UE.pdf>.
322 Sobre o procedimento da ODR fornecida pela Comissão Europeia, acesse: < https://ec.europa.eu/consumers/odr/main/?event=main.trader.register#inline-nav-4> e < https://ec.europa.eu/consumers/odr/userguide/pdf/MA/userguide-en.pdf>.
323 UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL). UNCITRAL Technichal Notes on Online Dispute Resolution. New York, 2017. Disponível em: < https://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf>. p. 02-03.
324 *Ibid*. p. 06-07.
325 CIVIL JUSTICE COUNCIL'S ADVISORY GROUP ON ONLINE DISPUTE RESOLUTION. Online Dispute Resolution for Low Value Civil Claims. Fev., 2015. Disponível em: < https://www.judiciary.uk/wp-content/uploads/2015/02/Online-Dispute-Resolution-Final-Web-Version1.pdf>. p. 22-23.

Para tanto, o sistema atuaria por meio de três camadas: *online evaluation*, *online facilitation* e *online judges*[326]. Dessa forma, em um primeiro momento, o sistema realizaria uma avaliação gratuita sobre o problema, de modo que, ao informar os usuários do cenário fático e suas consequências legais, estes possam evitar litígios ou resolve-los sem acionar o judiciário[327].

Na hipótese de insucesso da primeira camada, a *online facilitation* procederá com a condução, por meio de um facilitador, pautado por técnicas de ADR (*alternative dispute resolution*) e EDR (*early dispute resolution*), de uma tentativa de alcance de acordo entre as partes[328].

Já na hipótese de necessidade de decisão vinculante e executável, a camada de *online judges* indicará juízes competentes, por meio de julgamento online, para decidirem sobre o feito[329].

Observa-se, portanto, que o estabelecimento de diretrizes acerca das plataformas ODR, bem como seu endossamento por instituições e autoridades estatais, visam mais que celeridade e economia, procuram viabilizar o acesso à justiça.

[326] CIVIL JUSTICE COUNCIL'S ADVISORY GROUP ON ONLINE DISPUTE RESOLUTION. *Op. cit*. p. 19-20.
[327] *Ibid*., p. 19.
[328] *Ibid*., p. 20.
[329] *Ibid*., p. 20.

4. PANORAMA BRASILEIRO

O incentivo ao acesso à meios alternativos de solução de disputas, no contexto nacional, apresenta um salto em seu incentivo e divulgação, a partir de 2010. A edição da Resolução nº 125/2010, pelo Conselho Nacional de Justiça, possibilitou o direito à resolução dos conflitos por meios adequados à sua natureza e à sua peculiaridade.

A Emenda nº 1 à esta Resolução, datada de 31 de janeiro de 2013, dispôs sobre a responsabilidade dos órgãos judiciários em "oferecer mecanismos alternativos de solução de controvérsias como a mediação e a conciliação"[330].

Ademais, a Emenda nº 2, de 08 de março de 2016, estabeleceu a criação Sistema de Mediação e Conciliação Digital ou a distância para atuação pré-processual de conflitos.

Soma-se a isto o incentivo aos meios alternativos de solução de conflitos, destacados no art. 3º do Código de Processo Civil de 2015.

Não somente assegurar o acesso à justiça por meio destes métodos alternativos, como também viabilizar o direito à informação é pauta do Conselho Nacional de Justiça. A Resolução Conjunta nº 02/2011, editada pelo CNJ em parceria com o Ministério Público, previu a criação de um "sistema informatizado onde fossem reunidos inquéritos civis, termos de ajustamento de conduta e ações coletivas"[331].

Desta iniciativa, observa-se a criação do portal "Consumidor Vencedor", no intuito de assegurar acesso aos cidadãos a informações sobre vitórias obtidas na defesa coletiva dos consumidores.

Em paralelo ao direito à informação, cuja tangibilidade é preconizada pelos meios virtuais, denota-se a também iniciativas, tanto de caráter privado, como de chancela governamental/ institucional, para o acesso à justiça por meio de plataformas online de solução de conflitos.

Por um lado, emergem iniciativas digitais institucionais, como a plataforma consumidor.gov e a mediação online, determinada pelo CNJ. Enquanto sob o viés da iniciativa privada, destaca-se a ascensão do ecossistema de lawtechs ou *legaltechs*, cujo propósito é a resolução extrajudicial e online de conflitos, como por exemplo a Justto, Acordo Fechado, Sem Processo, etc.

Reconhece-se que o acesso à informação, em especial o acesso à internet, ainda é obstáculo para a interação entre as plataformas ODR e cidadãos no Brasil.

No entanto, as iniciativas nacionais também acompanham a tendência da desjudicialização internacional e o incentivo aos meios alternativos de solução de conflitos como forma de alcance da justiça e seus princípios de celeridade e efetividade.

---

[330] PORTO, Antônio José Maristrello. NOGUEIRA, Rafaela. QUIRINO, Carina de Castro. Resolução de Conflitos On-line no Brasil: um mecanismo em construção. *Revista de Direito do Consumidor*, vol. 114/2017. p. 295-318. Nov. – Dez. / 2017. Revista dos Tribunais Online.

[331] JUNIOR, Marcos Cunha Orofino. Ministério Público – entraves judiciais e meios alternativos de defesa dos direitos individuais homogêneos. *Revista de Direito do Consumidor*. Vol. 105/2016. P. 371-393. Maio – Jun. 2016. Revista dos Tribunais Online.

5. CONCLUSÃO

O congestionamento do sistema judiciário não é exclusivamente brasileiro. Acionar este mecanismo, conforme a teoria das múltiplas portas, seria viável somente na hipótese de que o conflito somente possa ser resolvido pelo Estado-Juiz.

Desse modo, apesar da via judicial encontrar-se sempre disponível, esta não necessariamente deve ser adotada como primeira opção. Inclusive, deve o juiz assumir seu novo papel no conflito e indicar os meios alternativos de solução de conflito.

Em paralelo à ascensão da desjudicialização, nota-se que o desenvolvimento tecnológico pode ser aliado da celeridade e efetividade na batalha pelo efetivo acesso à justiça.

Apesar de recentes regulamentações e elaborações de guias de boas práticas, o movimento global endossa a *Online Dispute Resolution* como efetivas plataformas para solução de conflitos, atendendo a necessidade atual do consumidor e usuário virtual por baixo custo, atendimento e linguagem de fácil compreensão, celeridade e segurança.

6. REFERÊNCIAS

AMERICAN BAR ASSOCIATION'S TASK FORCE ON ELECTRONIC COMMERCE AND ALTERNATIVE DISPUTE RESOLUTION IN COOPERATION WITH THE SHIDLER CENTER FOR LAW, COMMERCE AND TECHNOLOGY, UNIVERSITY OF WASHINGTON SCHOOL OF LAW. Addressing Disputes in Electronic Commerce: Final Recommendations and Report. *The Business Lawyer*, vol. 58, no. 1, 2002, pp. 415–477. *JSTOR*. Disponível em: <www.jstor.org/stable/40688128>. p. 422-423.

ANDRADE, Henrique dos Santos; MARCACINI, Augusto. Os novos meios alternativos ao judiciário para a solução de conflito, apoiados pelas tecnologias da informação e comunicação. Revista de Processo, vol. 268/2017, Revista dos Tribunais Online, Junho. 2017. p. 587-612.

BAUMAN, Zygmunt. Modernidade Líquida. Tradução: Plínio Dentzien – Rio de Janeiro: Zahar, 2001.

BHARUKA, Devashish; Online Dispute Resolution. In: VERMA, S.K.; MITTAL, Raman. Legal Dimensions on Cyber Space. New Delhi: Indian Law Institute, 2004. Disponível em: < http://14.139.60.114:8080/jspui/handle/123456789/722>.

CIVIL JUSTICE COUNCIL'S ADVISORY GROUP ON ONLINE DISPUTE RESOLUTION. Online Dispute Resolution for Low Value Civil Claims. Fev., 2015. Disponível em: < https://www.judiciary.uk/wp-content/uploads/2015/02/Online-Dispute-Resolution-Final-Web-Version1.pdf>.

CONSELHO NACIONAL DE JUSTIÇA. Justiça em Números 2018: ano-base 2017. Brasília: CNJ, 2018.

COUTO, Mônica Bonetti. CRUZ, Luana Pedrosa de Figueiredo. Desjudicialização e Novo Código de Processo Civil: análise à luz das técnicas inseridas no sistema processual brasileiro. Revista de Processo. Vol. 271/2017. p. 405-425. Set. 2017. Revista dos Tribunais Online.

Deloitte. Global Powers of Retailing 2018: Transformative change, reinvigorated commerce. Disponível em: < https://www2.deloitte.com/content/dam/Deloitte/at/Documents/about-deloitte/global-powers-of-retailing-2018.pdf>.

Ebit. Webshoppers Elo. 38ª Ed., 2018. p. 12. Disponível em: < http://www.fecomercio.com.br/public/upload/editor/ws38_vfinal.pdf>

GOMES, Helton Simões. Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. G1. 21 fev. 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>.

HOLMAN, Lee. BUZEK, Greg. Debunking the retail apocalypse. Ago. 2017. Disponível em: <https://www.business.att.com/content/dam/attbusiness/insights/campaigns/retail-apocalypse/debunking-the-retail-apocalypse.pdf>

HUCK, Hermes Marcelo. O Brasil e a globalização: pensadores do direito internacional. Organização: Maurício Almeida Prado, Renata Duarte de Santana – São Paulo: Editora de Cultura, 2013.

KATSH. Ethan. Online Dispute Resolution: some implications for the emergence of law in cyberspace. Lex Electronica. Vol. 10, nº 3, 2006. Disponível em: < http://www.lex-electronica.org/articles/v10-3/katsh.htm>.

KATSH, Ethan. RIFKIN, Janet. Online Dispute Resolution: resolving conflicts in cyberspace. San Francisco: Jossey-Bass, 2001.

KPMG. Global retail trends 2018: Global Consumer & Retail. Mar, 2018. Disponível em: < https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/global-retail-trends-2018.pdf>.

LIMA, Gabriel Vasconcelos. FEITOSA, Gustavo Raposo Pereira. Online Dispute Resolution (ODR): a solução de conflitos e as novas tecnologias. Revista do Direito. Santa Cruz do Sul, v. 3, n. 50, p. 53-70, set./ dez/ 2016. Disponível em: < https://online.unisc.br/seer/index.php/direito/index>.

NASCIMBENI, Asdrubal Franco. Os meios extrajudiciais de solução de conflitos como forma adequada de pacificação social e a tendência à desjudicialiazação. Revista de Arbitragem e Mediação. Vol. 52/2017. p. 221-258. Jan. – Mar., 2017. Revista dos Tribunais Online.

OLIVEIRA, Andressa Jarletti Gonçalves de. Defesa Judicial do Consumidor Bancário. Curitiba: Rede do Consumidor. 2014.

PINHO, Humberto Dalla Bernardina de. STANCATI, Maria Martins Silva. A Ressignificação do Princípio do Acesso à Justiça à luz do Art. 3º do CPC/2015. Revista de Processo, vol. 256/2016. p. 17-44. Abr. 2016. Revista dos Tribunais Online.

PwC. Global Consumer Insights Survey 2018: New business models in the e-commerce era. Disponível em: <https://www.pwc.com/gx/en/retail-consumer/assets/business-models-global-consumer-insights-survey.pdf>.

PwC. Retail & Consumer Report 2018. Disponível em: < https://www.pwc.ie/publications/2018/retail-consumer-report-2018.pdf>.

UNIÃO EUROPEIA. Regulamento (UE) nº 524/2013 do Parlamento Europeu e do Conselho, de 21 de maio de 2013. Disponível em: < https://www.triave.pt/wp-content/uploads/Regulamento-UE.pdf>.

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL). UNCITRAL Technichal Notes on Online Dispute Resolution. New York, 2017. Disponível em: < https://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf>.