VOLUME 7

DIREITO E INOVAÇÃO

ORGANIZAÇÃO

Dayana de Carvalho Uhdre
André Guskow Cardoso
Rafaela Vialle Strobel Dantas
Luís Felipe Pilagallo da Silva Mäder Gonçalves
Maryam Lima Kadri
Vitor Pereira Pacheco

Rhodrigo Deda Gomes
Rafael Aggens Ferreira da Silva
Patricia Rodriguez Franco
Cynzia Carla Fontana
Kael Nery de Lima Moro
Ana Lúcia Barella
Guilherme Hideo Oshima

REVISÃO

Ana Lúcia Barella
Sabrina Cavallari
Stefano Avila Pavan

Cinthia Obladen de Almendra Freitas
Gilmara Pesquero Fernandes Mohr Funes
Felipe Emanoel Pacheco Jensen

OAB PARANÁ 90 ANOS | OAB PARANÁ | COMISSÃO DE INOVAÇÃO E GESTÃO | COMISSÃO DE DIREITO DIGITAL E PROTEÇÃO DE DADOS | COMISSÃO DE GESTÃO E EMPREENDEDORISMO | ESA ESCOLA SUPERIOR DE ADVOCACIA

Catalogação da Publicação na Fonte
Bibliotecária: Rosilaine Ap. Pereira CRB-9/1448
Ordem dos Advogados do Brasil. Seção do Paraná

D598 Direito e inovação / Organizado por Rhodrigo Deda Gomes et al. -- Curitiba : OABPR, 2022. (Coleção Comissões).
323 p. ; v.7.

ISBN (versão online):

Vários autores
Inclui Bibliografia

1. Direito. 2. Inovação. 3. Direito digital. 4. eSports. 5. LGPD. 6. ANPD. 7. Direito penal. 8. Blockchain. 9. Novas tecnologias. 10. Regulação e Governança. 11. Proteção de Dados. I. Gomes, Rhodrigo Deda. II. Silva, Rafael Aggens Ferreira da. III. Franco, Patricia Rodriguez. IV. Fontana, Cynzia Carla. V. Uhdre, Dayana de Carvalho. VI. Moro, Kael Nery de Lima. VII. Barella, Ana Lícia. VIII. Oshima, Guilherme Hideo. IX. Cardoso, André Guskow. X. Dantas, Rafaela Vialle Strobel. XI. Oliveira, Ana Paula de. XII. Kadri, Maryam Lima. XIII. Pacheco, Vitor Pereira. XIV. Coleção Comissões. XV. Comissão de Inovação e Gestão da OAB/PR. XVI. Comissão de Direito Digital e Proteção de Dados. XVII. Comissão de Gestão e Empreendedorismo. XVIII. 12. OABPR.

CDD: 340.0285

Índice para catálogo sistemático:

1. Direito eletrônico – 340.0285
2. Direito à privacidade – 341.2732

PREFÁCIO

Em continuidade à apresentação dos resultados promovidos pelos Grupos Permanentes de Discussão da Comissão de Inovação e Gestão da Ordem dos Advogados do Paraná – OAB/PR, esta Comissão, em parceria com a Escola Superior da Advocacia – ESA/PR, apresenta, neste 7º volume do Ebook Direito e Inovação, artigos sobre os temas mais relevantes do mundo jurídico, no período em que foram escritos.

Esta obra condensa seis meses de pesquisa, discussão, insights e construção nos Grupos Permanentes de Discussão dos seguintes eixos temáticos: (i) eSports Games e o Direito; (ii) Regulação e Governança de Blockchains; (iii) LGPD e ANPD, e; (iv) Direito Penal e Novas Tecnologias.

Os artigos escritos sob a ótica do eSports Games e o Direito exploram os desafios encontrados com o crescimento da modalidade do esporte eletrônico, em estudos aprofundados sobre cláusulas anticheat, punições de banimentos e a expansão do poker online.

O resultado da produção do Grupo Permanente de Discussão de Regulação e Governança de *Blockchains* aborda o *SandBox* Regulatório, novo mecanismo de desenvolvimento de projetos experimentais e inovadores, que funciona sob a supervisão próxima do ente regulador, em ambiente controlado. Tal estrutura, muito utilizada em países estrangeiros, é de extrema relevância para o avanço no mercado financeiro no Brasil.

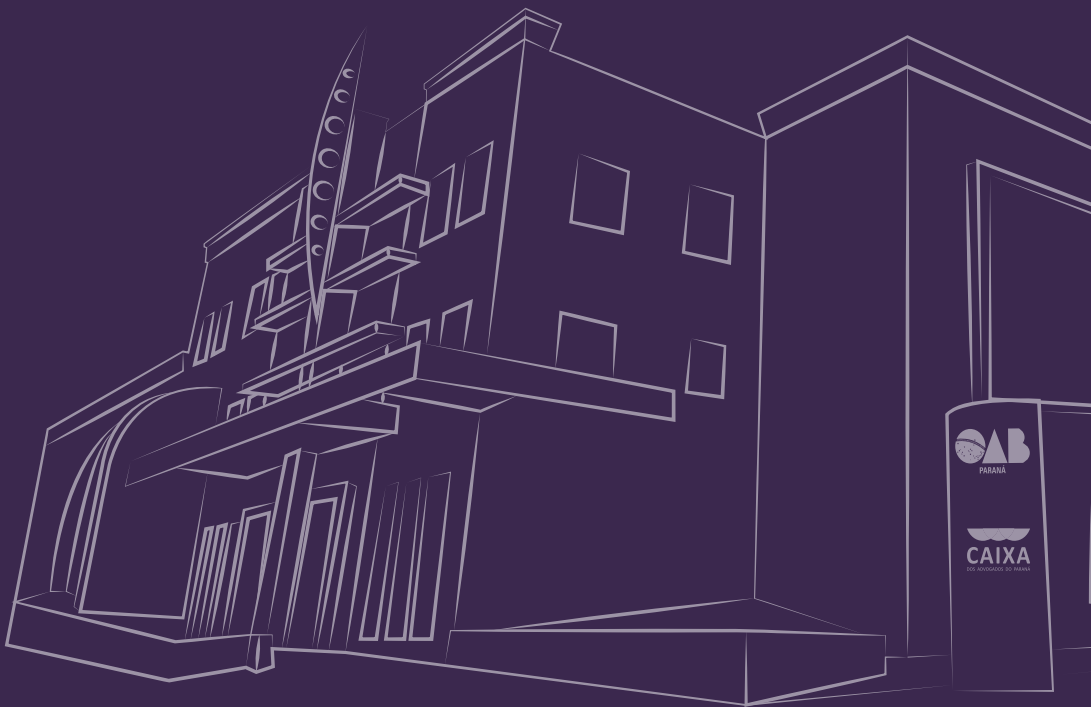
O Grupo Permanente de Discussão sobre Proteção de Dados (LGPD e ANPD) oferece uma gama de discussões contemporâneas que resultaram em artigos de altíssima relevância, com estudos de caso e abordagens únicas, desde análise sobre o Relatório

de Impacto à Proteção de Dados Pessoais, garantias contratuais para transferência internacional de dados e direitos do titular.

Os artigos relacionados ao Grupo Permanente de Discussão sobre Direito Penal e Novas Tecnologias, reúnem temas de relevância global que incitam curiosidade, como *Cyber Grooming*, crimes virtuais contra a mulher e o monitoramento eletrônico de pessoas presas na pandemia.

Frente ao cenário atual, rico em inovação, no qual o mundo jurídico experimenta reflexos profundos, o presente compêndio tem o objetivo de contribuir com a construção de conhecimentos para que, não só os advogados, mas toda a sociedade, possam enfrentar os desafios de Gestão e Inovação com maior propriedade e lastro.

Boa Leitura!



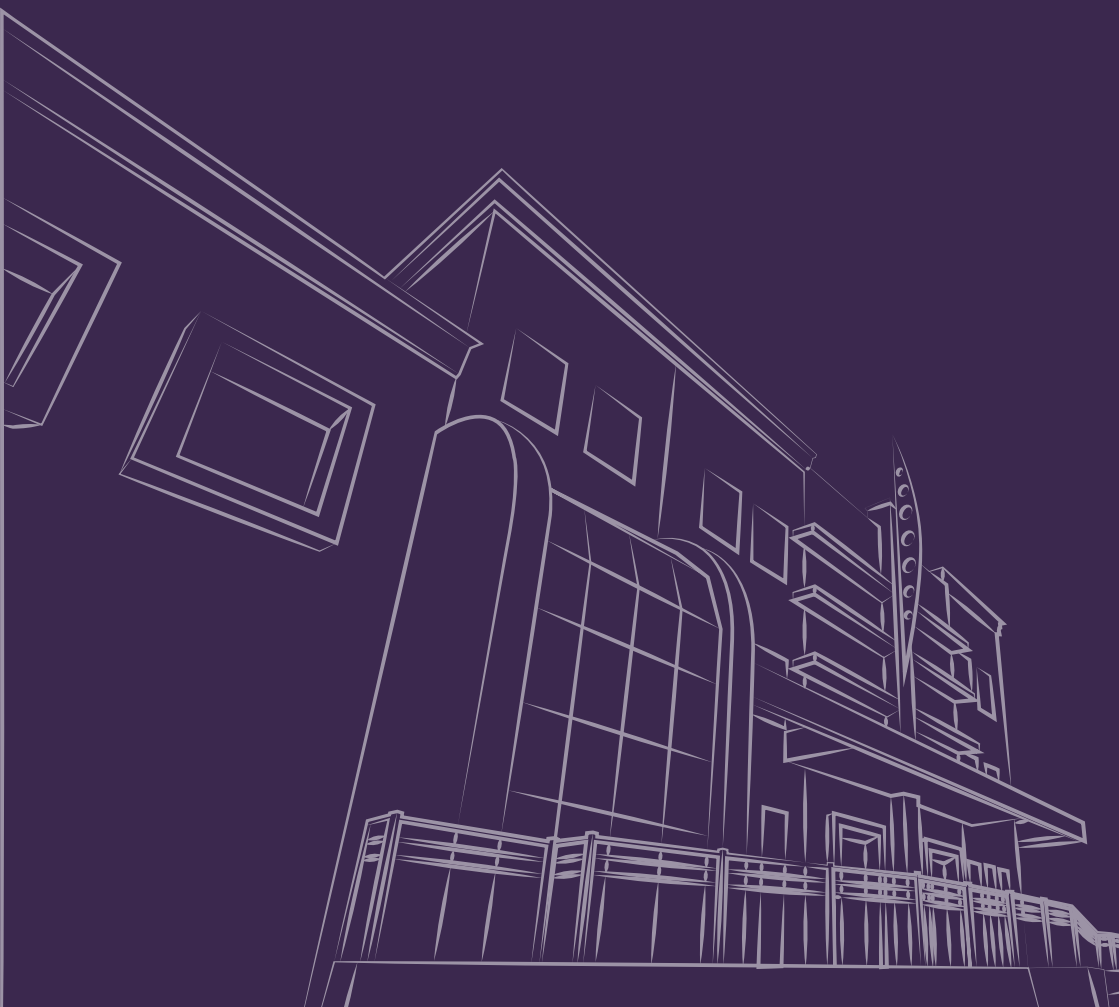
ORGANIZAÇÃO

Rhodrigo Deda Gomes
Rafael Aggens Ferreira da Silva
Patricia Rodriguez Franco
Cynzia Carla Fontana
Kael Nery de Lima Moro
Ana Lúcia Barella
Guilherme Hideo Oshima
Dayana de Carvalho Uhdre
André Guskow Cardoso
Rafaela Vialle Strobel Dantas
Luís Felipe Pilagallo da Silva Mäder Gonçalves
Maryam Lima Kadri
Vitor Pereira Pacheco

REVISÃO

Cinthia Obladen de Almendra Freitas
Gilmara Pesquero Fernandes Mohr Funes
Felipe Emanoel Pacheco Jensen
Ana Lúcia Barella
Sabrina Cavallari
Stefano Avila Pavan

SUMÁRIO



PLANEJAMENTO SOCIETÁRIO NO E-SPORT A PARTIR DO EXEMPLO DO PÔQUER NO BRASIL

CORPORATE PLANNING IN E-SPORTS THROUGH THE EXAMPLE OF POKER IN BRAZIL

Pedro de Perdigão Lana
Professor (ISULPAR), Mestre em Direito Empresarial pela Universidade de Coimbra, graduado pela UFPR
pedrop@lana.email

Ramon Prestes Bentivenha
Mestrando em Direito pela Universidade Federal do Paraná
bentivenha@AdvocaciaSocial.com

RESUMO:
O presente artigo tem por objetivo abordar alguns dos efeitos e cuidados necessários em relação à explosão econômica dos *e-sports* e analisar brevemente o cenário regulatório sobre o tema no Brasil. Apontando o crescimento de um espaço inicialmente menosprezado, mas que movimenta cifras bilionárias, será analisada a evolução do mercado do ponto de vista financeiro e os seus respectivos reflexos econômicos. Com especial ênfase, são abordadas informações relativas ao mercado de pôquer e suas incertezas. Para exemplificar o argumento, são trazidos ao texto aspectos societários, fiscais e de propriedade intelectual, abordando alguns dos pontos relevantes que compõem o planejamento empresarial nessa indústria. Objetiva-se contribuir com o debate acerca dos projetos legislativos e ponderar itens pertinentes aos e-atletas. A metodologia do artigo é baseada em uma revisão bibliográfica e estudos analíticos.

Palavras-Chave: Pôquer. Poker. Planejamento societário. Empresarial. Regulação.

Sumário: 1. O Avanço Dos E-Sports: O "Joguinho" Que Se Transformou em Mercado Bilionário; 2. Um Cenário De Incertezas Jurídico-Regulatórias; 3. O Planejamento Societário Do E-Sports, Com Destaque Ao Pôquer; 4. Tópicos Específicos Do Planejamento: Questões De Propriedade Intelectual; 5. Conclusão; Referências Bibliográficas.

ABSTRACT:
This article aims to address some of the effects and necessary precautions in relation to the economic explosion of e-sports and to briefly analyze the regulatory scenario on the subject in Brazil. Pointing out the growth of a field initially undervalued, but that operates multi-billion sums, the evolution of the market will be analyzed from the financial point of view and its respective economic reflexes. With special emphasis, information concerning the poker market and its uncertainties is addressed. To exemplify the argument, corporate, tax and intellectual property aspects are brought to the text, addressing some of the relevant points that make up corporate planning in this industry. The objective is to contribute to the debate about the legislative projects and ponder items pertinent to e-athletes. The methodology of the article is based on a bibliographical review and analytical studies.

Keywords: *Poker; Corporate Planning; Business; Regulation.*

Summary: *1. E-Sports Progress: The Little Game That Became A Billion-Dollar Market; 2. The Scenario Of Legal/Regulatory Uncertainty; 3. E-Sports Corporate Planning, With Emphasis On Poker; 4. Specific Topics For Planning: Intellectual Property Issues; 5. Conclusion; Bibliographical References.*

1. O AVANÇO DOS E-SPORTS: O "JOGUINHO" QUE SE TRANSFORMOU EM MERCADO BILIONÁRIO

Recorrendo às definições lexicológicas para iniciar a discussão, o esporte eletrônico ou *e-sport* é definido pelo Dicionário de Cambridge, em tradução livre, "a atividade de jogar jogos de computador contra outras pessoas na Internet, muitas vezes por dinheiro, e muitas vezes assistido por outras pessoas usando a Internet, às vezes em eventos organizados especiais" (CAMBRIDGE DICTIONARY, 2021). A definição dicionaresca é importante aqui como ponto de partida do senso comum sobre o tema.

Há poucos anos, era considerado apenas um joguinho de computador. Um passatempo. Entretanto, o mercado dos e-sports cresce a cada dia. Atualmente, representa um mercado tão relevante como em outros esportes tradicionais tais como futebol, basquete e beisebol.

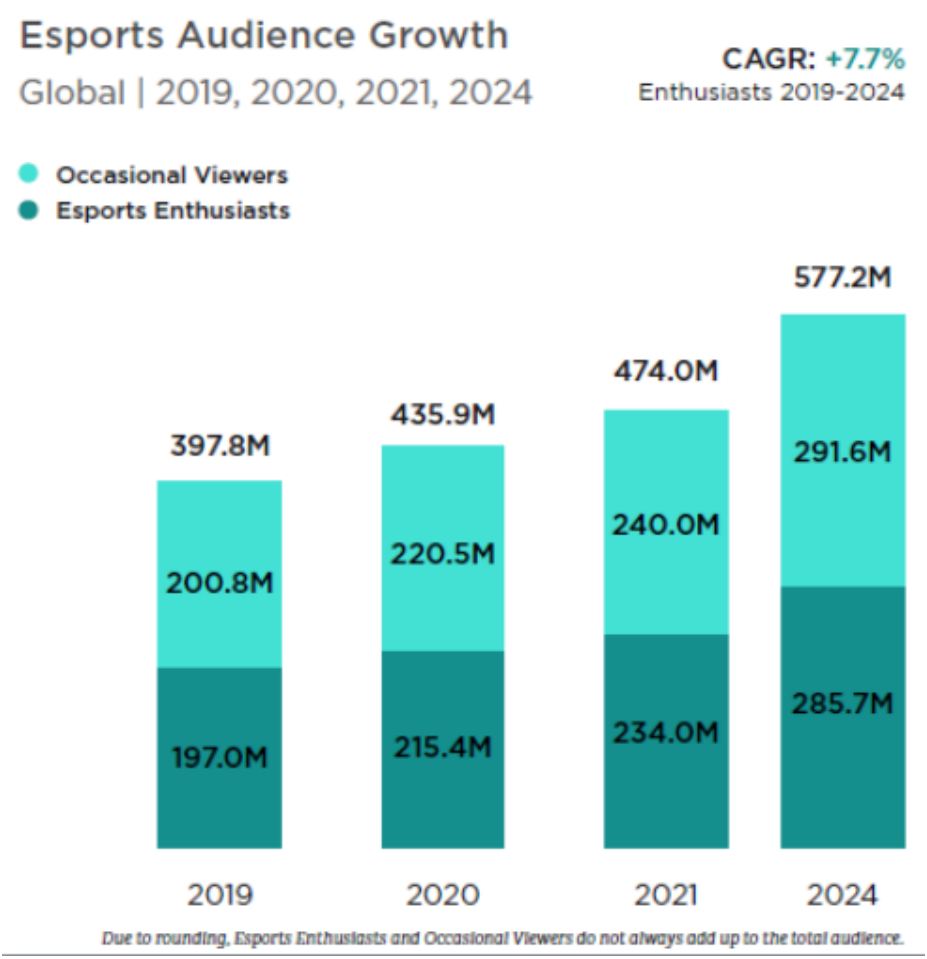
Para melhor introduzir a temática, necessário questionar se o *e-sport* pode ser considerado esporte, ou, mais precisamente, uma modalidade desportiva. Isso é, um jogador em frente ao computador poderia ser equiparado a um atleta que corre atrás de uma bola em um estádio de futebol?

Para responder à questão acima, é necessário indicar que, do ponto de vista conceitual, um esporte é caracterizado quando estão presente cinco requisitos (CASTRO, 2017, p. 17), elaborados pela doutrina principalmente a partir de escrito clássico de Bernard Suits (SUITS, 2007). São eles: a existência de uma atividade física; o desenvolvimento de relações interpessoais; a existência de regras pré-determinadas; competições organizadas; e um objetivo competitivo e não meramente artístico (MIGUEL, 2018, p. 6-14).

A primeira característica, a necessidade de uma atividade física talvez fosse o aspecto que mais poderia gerar dúvidas. Afinal, qual a atividade física poderia ser desempenhada em frente a um teclado? Qual o esforço físico ao apertar um simples botão? Ao pensar em analogias, poderia-se rememorar outras modalidades esportivas, como, por exemplo, o tiro esportivo. Uma modalidade olímpica, onde o atleta com um simples apertar de botão/gatilho tenta atingir um alvo pré-estabelecido. Se o tiro é considerado uma atividade esportiva, qual a dificuldade de identificar que um e-atleta também preenche o mesmo requisito?

Os demais requisitos (atividades interpessoais, regras, competições e um objetivo não meramente artístico) se evidenciam quando se observam as acirradas competições entre times de diferentes modalidades. Equipes tradicionais de futebol, como Corinthians e Flamengo, organizam equipes de e-atletas para participar de campeonatos no Brasil e no mundo. A final do campeonato mundial de *League of Legends (LoL)* de 2018 foi assistida por um público equivalente a final do *Super Bowl* do mesmo ano.

Segundo o mais recente relatório da Newzoo (uma das principais consultorias do mercado de esportes eletrônicos no mundo), o público global dos *e-sports* foi de cerca de 474 milhões de espectadores em 2021. Desses, 234 milhões (cerca de 49%) são entusiastas, aqueles que acompanham times e e-atletas com a mesma paixão que um torcedor fanático que vai aos estádios de futebol toda semana. Estima-se que em 2024, o público chegue a mais de meio bilhão de pessoas (NEWZOO, 2021, p. 31–32).



(Gráficos do relatório da Newzoo, 2021, p. 29 e 31, simplificados)

(Gráficos do relatório da Newzoo, 2021, p. 29 e 31, simplificados)

A audiência cativa dos *e-sports* pode ser notada também no Brasil – o terceiro maior mercado consumidor, atrás apenas dos EUA e da China. Em 2020, o número de horas assistidas em *lives* (transmissões ao vivo de partidas online) chegou a impressionantes 1,1 bilhão de horas. Isso considerando apenas as *lives* narradas em português. Esse público tem reflexo direto no faturamento do setor. A mesma consultoria, estima que em 2021 as receitas do setor tenham chegado a impressionantes 1,084 bilhões de dólares americanos. Apesar da crise, que impossibilitou a realização de eventos presenciais com a venda de ingressos em estádios, o setor cresceu próximo a 11% (NEWZOO, 2021, p. 29–30).

Com tantos recursos envolvidos e em franco crescimento, é natural que a profissionalização do setor leve também à uma intensificada "empresarialização", que poder-se-ia também chamar de uma profissionalização comercial, de todos os envolvidos nesse tipo de esporte. Isso ocorre em busca de maior eficiência, especialmente quando nos referimos a utilização de recursos, e de uma perenização da atividade desenvolvida, inclusive para gerar rendimentos a médio e longo prazo para os envolvidos que capitaneiam esses projetos.

Esse movimento de institucionalização já ocorreu com os grandes esportes tradicionais no passado (ABANAZIR, 2019, p. 2–3), e se estende para os esportes eletrônicos a exigência de se alcançar um comportamento administrativo fundamentado em modernas técnicas e atitudes capazes de reduzir os riscos e aumentar as possibilidades de sucesso do empreendimento (AZEVÊDO, 2009). Não é à toa que diversas alterações da Lei Pelé abordaram o regime jurídico das entidades de prática desportivas prevista no art. 27, muitas vezes contando com um curto período de tempo entre as reformas (vide, por exemplo, Lei nº 9.981/ 2000; MP nº 2.141/ 2001; Lei nº 10.672/2003; Lei nº 12.395/2011; e Lei nº 13.155/2015), comumente em prol de maior facilidade para conversão das entidades em um modelo empresarial.

Todavia, os esportes eletrônicos apresentam uma participação intensiva de capital e de grandes empresas já em seus primeiros anos, sendo esse um diferencial em relação aos esportes tradicionais (SUMMERLEY, 2020, p. 58). A "empresarialização" do ramo surge quase como uma imposição aos participantes para acompanhar o ritmo desse setor.

Quando se fala no avanço dessa participação em jogos eletrônicos, é comum pensar em eventos que ficaram famosos por sua grandiosidade recente, como os estádios lotados das finais de

League of Legends. No entanto, outro exemplo se destaca, ainda mais após o isolamento resultante da pandemia, em um caso em que já existia um jogo profundamente comercial que foi migrando aos poucos para o mundo digital. Trata-se do pôquer (que também é chamado cotidianamente pelo anglicismo *poker*), que já existia há muitas décadas envolvendo quantias elevadas de dinheiro e campeonatos altamente profissionalizados. Hoje em dia, por outro lado, percebe-se uma dominância da versão eletrônica desse esporte da mente tanto para entretenimento quanto para fins profissionais, com um amplo mercado de plataformas alternativas que são ou concorrentes diretas, numa perspectiva mais generalista, ou apresentam funcionamento e público-alvo muito distintos entre si.

É esse cenário, de crescimento da importância das empresas nos *e-sports*, que estará na base da pesquisa a seguir.

2. UM CENÁRIO DE INCERTEZAS JURÍDICO-REGULATÓRIAS

Um planejamento societário para os *e-sports* não se difere na essência de outros planejamentos empresariais – que buscam otimizar resultados, traçar metas realistas, identificar e reduzir riscos, dentre outros. A partir de estudos e organização de processos, se procuraria analisar e se anteceder a possíveis problemas ou oportunidades, verificar a legislação aplicável e definir o modelo societário mais adequado. Algumas perguntas clássicas permanecem, como a definição dos procedimentos deliberativos dos sócios e da administração, a possibilidade e procedimentos extrajudiciais de exclusão dos sócios, normas próprias para a deliberação dos sócios e tópicos da prestação de contas (CARVALHO, 2014, p. 460). Mas, no caso dos *e-sports*, é preciso ir um pouco além.

Afinal, este é um cenário muito pouco regulamentado e, assim, que oferece pouca segurança jurídica para se fazer planejamentos efetivos baseados apenas em normas e entendimentos pré-estabelecidos.

Traz-se novamente o pôquer como exemplo que expõe essa situação de forma cristalina. Nele, encontra-se uma profunda dificuldade dos esportistas em seguirem fielmente as regras e orientações legais relacionadas à sua atividade, como de tributação e organização de eventos, mesmo que tenham toda a intenção de fazê-lo.

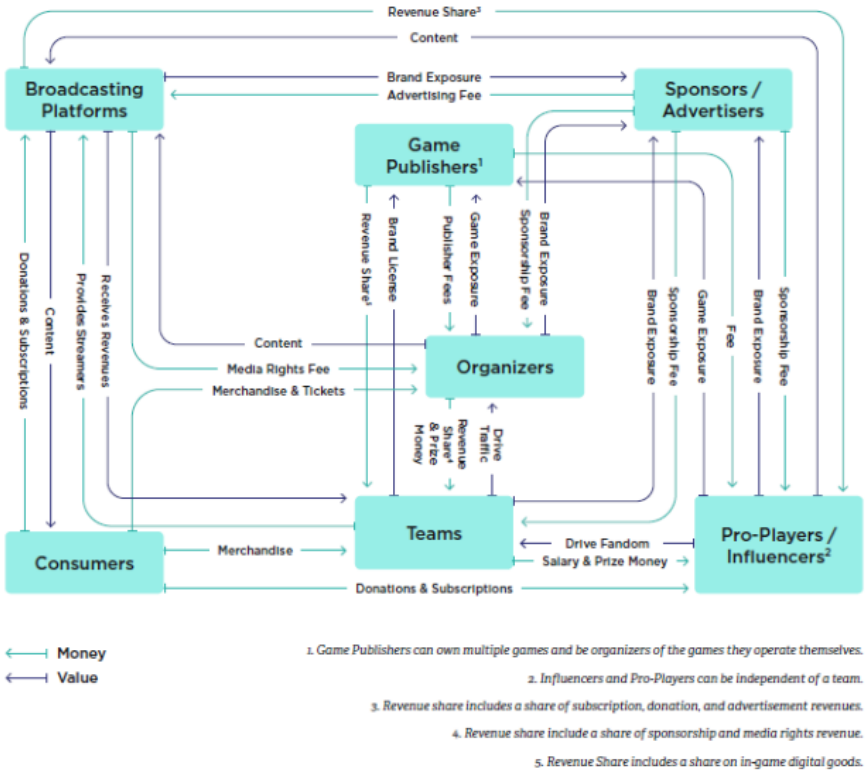
Isso é resultado direto das ambiguidades e lacunas por parte do poder público, por não se encontrarem orientações firmes e claras específicas, ou outras de caráter mais geral que se adequem de forma razoável às dinâmicas da atividade, até mesmo por uma opção do legislador à época de associar a atividade econômica do pôquer como algo ilícito. Quando esse esporte é transposto para o cenário digital, que tem dificuldades regulatórias próprias, a situação se agrava. É visível que a legislação esportiva brasileira (assim como outras normas, como as tributárias) está hoje muito afastada da realidade dos jogadores de pôquer.

Em verdade, muito do arcabouço da legislação esportiva brasileira busca disciplinar situações típicas do futebol, algo completamente diferente de um esporte intelectual como o pôquer. Algo compreensível, pois, afinal, se trata de uma paixão nacional, mas que se difere em forma e substância quanto as demais modalidades esportivas. Imaginar que a Lei Pelé (Lei 9.615/1998) poderia ser aplicável para um jogador de pôquer seria o mesmo que imaginar que uma pessoa vestiria uma armadura medieval para passear no shopping. A roupagem não vestiria bem, dificultaria a locomoção e o desenvolvimento das atividades mais simples do dia a dia, como agachar para amarrar o sapato.

Atualmente parlamentares buscam reduzir essas incertezas a partir de iniciativas legislativas. Existe no Congresso Nacional um acalorado debate quanto à regulamentação dos e-sports no Brasil. Na Câmara dos Deputados tramita o Projeto de Lei (PL) 3.450/2015 (BRASIL, 2015a) em apensado ao PL 7747/2017 (BRASIL, 2017a). Eles aguardam parecer do relator, Deputado Felipe Carreras (PSB-PE). No Senado, está em debate o PLS 383/2017, pronto para análise do plenário desde 2019 (BRASIL, 2017b).

Em ambas as iniciativas legislativas existem problemas conceituais e práticos ao desconsiderarem o complexo ecossistema dos *e-sports*. Apenas para ilustrar, se poderia criticar a necessidade de "federações" ou "confederações" para organização de competições oficiais. Em um cenário futebolístico isso seria perfeitamente possível, mas é algo dispensável no cenário dos *e-sports*, como demonstrar-se-á, centralizador que as *publishers* podem assumir (e frequentemente o fazem).

Afinal, lembra-se do envolvimento de diferentes atores em um sistema multisetorial, com papéis muito diversos. Sem aprofundar nesse item, para demonstrar rapidamente a complexidade do ecossistema que poderia parecer simples em uma primeira visão, retoma-se o relatório do Newzoo, em relação à estrutura comercial dos *e-sports*.



(NEWZOO, 2021, p. 9)

Como se observa acima, apesar de encontrar-se várias similaridades entre os atores que já estão consolidados há décadas (como os patrocinadores e as plataformas de transmissão), o ecossistema no *e-sports* de forma geral é bastante divergente dos esportes tradicionais, como o futebol, em especial pela introdução central dos *game publishers* e da relação mais direta entre consumidores e jogadores individuais. Embora louváveis as iniciativas parlamentares, a incerteza legislativa não parece ser reduzida com a aprovação dos PLs atualmente em trâmite, até porque esse é um cenário que ainda está em construção e não deve ser tomado por normas que resultem em um maior enrijecimento.

Para se discutir o planejamento societário nos *e-sports*, assim, é necessário considerar as ferramentas que o sistema jurídico já disponibiliza no Brasil e fundamentar as suas ações e planos nelas, mas sempre tendo noção que esse é um mercado que ainda será muito pautado pelos padrões internacionais e pelos atos de auto regulação do setor privado. Agir de forma engessada, almejando sempre enquadrar as empresas de *e-sports* em modelos que foram pensados para outros tipos de esporte, seria profundamente danoso para as empresas do setor de jogos eletrônicos com intenções competitivas.

Esse cenário de incertezas é agravado exponencialmente no caso do pôquer, em que a própria regularidade e licitude desse esporte da mente é colocado em dúvida e ainda hoje é visto com ressalvas por vários setores da sociedade, incluindo alguns órgãos públicos.

Isso porque o art. 50 da Lei de Contravenções Penais (Decreto-Lei n.º3.688, de 03 de outubro de 1941) tipifica o ato de "estabelecer ou explorar jogo de azar em lugar público ou acessível ao público, mediante o pagamento de entrada ou sem ele", considerando jogos de azar no inciso a) como "o jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte", e, no inciso c), como "as apostas sobre qualquer outra competição esportiva". Porém, a própria descrição legal explicita que essa classificação não abarcaria o pôquer, embora no passado o entendimento jurisprudencial tenha majoritariamente firmado esse errôneo enquadramento (BRASIL, 2003)[1].

1 Decisões posteriores de Tribunais de Justiça são quase todas em sentido contrário, com exceção dos casos de *cash game*, em que se faz as apostas diretamente com dinheiro. Ver, por ex. TJRS, MS 70025424086, Primeira Câmara Cível, rel. Des. Irineu Mariani, j. 17.12.2008; TJSC, MS 2010.047810-1, Rel. Des. Sérgio Roberto Baasch Luz, Grupo de Câmaras de Direito Público, j. 08/11/2011; TJPR, AI N.º 1.041.205-2, 5ª Câmara Cível, Rel. Jorge Xisto Pereira, j. 29.05.2013. Mais recentemente, cf. TJSC, autos n. 0004033-2420138240005, 4ª Câmara de

No âmbito do Mandado de Segurança n.º 2010.047810-1/SC, encontra-se parecer de Miguel Reale Junior sobre a questão que se tornou um documento fundamental para o tema no país. Nele o jurista descreve minuciosamente o trabalho intelectual e o grau de dificuldade para consistentemente vencer seus competidores no pôquer, indicando os seus efeitos jurídico-regulatórios. Essas exigências pessoais incluem a capacidade de fazer análises matemáticas complexas, um conhecimento sobre o psicológico próprio e de terceiros e um profundo controle da própria face e do próprio corpo (REALE JR., 2010).

Embora dependa também de sorte, percebe-se, até pela constância de certos jogadores nos melhores lugares dos campeonatos regionais e globais, que a habilidade do jogador é um fator preponderante. A equivalência mais próxima seria apostar com um colega que você conseguiria vencê-lo em uma partida de dominó – e não, como comumente é feito, em uma aposta que conseguiria vencê-lo jogando "vinte e um" (MARQUES, 2012, p. 202–204).

É importante observar que o bom uso do blefe como parte desse esporte intelectual depende dos jogadores terem algo que lhes é minimamente caro em jogo (NESSON; WOODS, 2008, p. 18), mesmo que isso seja uma recompensa final não monetária. Curiosamente, uma outra comparação que já foi feita com certa frequência é com a atividade dos advogados, para o bem e para o mal, incluindo algumas das habilidades intelectuais exigidas em ambas os exercícios profissionais (LUBET, 2005).

Isso tudo caracterizaria o pôquer como um esporte da mente, em vez de um jogo de azar. Essa modalidade está aos poucos ganhando espaço internacional como uma categoria de esporte reconhecida e objeto de competições cada vez maiores, embora encontrem alguma dificuldade em serem inseridas nos eventos

Direito Público, rel. Des. Betina Maria Maresch de Moura, j. 08.04.2021.

de grande porte clássicos como as Olimpíadas (STEFANI, 2017)

O pôquer online mantém esse requisito de habilidade, e alguns dizem que ele até o exponencia, pois a exigência de uma disciplina para respeitar princípios matemáticos no seu método de jogo aumenta. A existência de sinais que indicam boas ou más mãos a partir dos atos de seus adversários continua existindo, mas de forma muito mais sútil e difícil de captar (NESSON; WOODS, 2008, p. 16).

Nesse mesmo sentido, lembra-se que o dispositivo de contravenção penal citado acima impede as apostas no território brasileiro. Todavia, a aposta virtual ocorre por meio de empresas e servidores localizados em outros países onde ela é permitida, sendo comum há muito tempo no país. Depois de algumas tentativas infrutíferas de proibir também essa modalidade, foi promulgada a Lei n. 13.756/2018, que permitiu o licenciamento da exploração de apostas esportivas de cota fixa no país.

Apesar de, aos poucos, estarem aparecendo projetos normativos e movimentos administrativos para preencher as lacunas, como os Projetos de Lei citado acima, ainda permanecem muitas áreas cinzentas, causando problemas indevidos principalmente para novatos e agentes novos nesse mercado.

3. O PLANEJAMENTO SOCIETÁRIO DE E-SPORTS, COM DESTAQUE AO PÔQUER

Quando se fala de planejamento societário (ou empresarial) nos *e-sports* e no pôquer, é preciso primeiro lembrar que o planejamento societário básico, apesar de todas as diferenças acima citadas, não vai se afastar radicalmente dos princípios do planejamento societário de empresas tradicionais. Várias das preocupações que empresas de 50 anos atrás tinham, inclusive no

momento de sua formulação, continuam valendo para empresas que envolvem atividades esportivas mentais no cenário virtual.

Afinal, questões como a estrutura jurídica do time não são diretamente dependentes do tipo de atividade praticada pela empresa, independendo se é algo mais tradicional ou um esporte eletrônico – sendo as mais notórias exceções da lista de atividades permitidas para ser Microempreendedor Individual, ou, quando pensa-se na escolha de regimes jurídicos, as vedações da Lei 9.718/1998 da opção pelo lucro presumido para uma gama de atividades[2]. É a forma como estes modelos serão utilizados que deve ser inovadora, e não os modelos em si.

Como ocorre em geral no Brasil, o caminho mais comum será o da sociedade limitada. Mas assim como em outros tipos de empresas, no momento de elaboração do contrato social e do primeiro planejamento será necessário averiguar qual a situação concreta do empreendimento que está surgindo. Até mesmo o registro do time como uma associação poder ser uma opção não só útil, como necessária (MIGUEL, 2018, p. 30). As perguntas a serem feitas capazes de direcionar o caminho são variadas, como ser ou não uma filial, a quantia do capital inicial, a existência de investidores, a existência de sócio pessoa jurídica, dentre outros. No caso do pôquer ou de jogos eletrônicos marcadamente individuais, a opção pela Sociedade Limitada Unipessoal prevista na

2 Art. 14. Estão obrigadas à apuração do lucro real as pessoas jurídicas: (...)
II - cujas atividades sejam de bancos comerciais, bancos de investimentos, bancos de desenvolvimento, caixas econômicas, sociedades de crédito, financiamento e investimento, sociedades de crédito imobiliário, sociedades corretoras de títulos, valores mobiliários e câmbio, distribuidoras de títulos e valores mobiliários, empresas de arrendamento mercantil, cooperativas de crédito, empresas de seguros privados e de capitalização e entidades de previdência privada aberta;
III - que tiverem lucros, rendimentos ou ganhos de capital oriundos do exterior;

Lei da Liberdade Econômica (Lei. 13.874/2019) é também bastante atraente, porque esses jogadores nem sempre fazem partes de times.

Aqui, porém, um cuidado é importante. Uma parte central do planejamento é evitar que as atividades do esportista como pessoa física se confundam de maneira indistinguível com as atividades da pessoa jurídica. Essa mistura engendra vários riscos, como um entendimento de simulação por parte da Receita Federal ou a impossibilidade de acesso a outros benefícios comerciais reservados para as empresas.

Nesse sentido, as empresas de *e-sports* brasileiras, por ser esse um mercado que está ainda em ascensão, não raramente precisarão de um planejamento específico de empresas de pequeno porte. Vale notar que esse é um termo ambíguo (OLIVEIRA; TERENCE; ESCRIVÃO FILHO, 2010, p. 121), com diferentes classificações a partir de diferentes fatores ao redor do mundo e mesmo para fins diversos no ordenamento brasileiro, a exemplo de classificações por receita bruta ou por quantia de pessoas empregadas[3]. Nos referimos aqui, portanto, ao primeiro tipo de classificações citada, de renda bruta anual entre R$360.000,00 e igual ou inferior a R$4.800.000,00.

Isso ocorrerá principalmente nos casos de planejamento para as empresas que estão dando seus primeiros passos e de jogadores que atuam sozinhos ou em times de tamanho muito reduzido.

3 A LC nº 123 de 2006 (Lei Geral da Micro e Pequena Empresa) vai definir, no art. 3º, II, que pequena empresa é a que "aufira, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais)". A ANVISA segue esse padrão na MP nº 2.190-34. No entanto, o SEBRAE e o IBGE também definem como pequena empresa, a depender do setor de atuação, de 20 a 99 funcionários (se indústria) ou de 10 a 49 funcionários (se comércio ou prestação de serviços), assumindo parâmetro diverso (SEBRAE, 2011)

Também parece ser o caso de empresa voltadas apenas para o jogo em si, sem maiores investimentos na venda de produtos e serviços associados à marca do negócio. Essas situações vão ocorrer com elevada frequência para jogadores de pôquer, excluídos os casos dos times maiores.

Por isso, como dito, noções gerais de planejamento societário também se aplicarão às empresas de *e-sports*. Isso inclui a noção de que empresas pequenas não podem partir dos mesmos princípios estratégicos ou operacionais que os das empresas grandes, considerando a menor estabilidade e a consequente maior necessidade de adaptação e revisão de objetivos e metas a médio e longo prazo, o que ensejaria também uma menor preocupação com a formalização do planejamento (OLIVEIRA; TERENCE; ESCRIVÃO FILHO, 2010, p. 121–124 e 130–131).

Contudo, no caso dos *e-sports*, a visível ausência de regulamentação aparece como uma benção e uma maldição. O advogado ou o administrador dogmático terá dificuldades em encontrar fundamentos seguros de onde partir, mas o profissional criativo, que domine a área e tenha capacidade de inovar terá também muito espaço para fazer a empresa ter uma vantagem concorrencial enorme ao implementar novas ideias. A diferenciação de um planejamento societário excepcional é principalmente uma questão de antever as dinâmicas de mercado, o que se amplifica no caso dos *e-sports*. Ser o primeiro a elaborar boas estruturas significa, na verdade, que a empresa terá maior força para direcionar as práticas padrões do mercado à medida que forem sendo regulamentadas, liderando pelo exemplo.

O planejamento societário no *e-sports* vai quase sempre ter como segunda base (após as determinações legais e regulamentares) as regulações e orientações estabelecidas por entidades do setor privado. Isso é necessário para garantir a participação

em campeonatos ou mesmo nos jogos cotidianos dos e-sportistas, quando, por exemplo, alguém pensa em *streaming*.

No caso do pôquer, em que o dinheiro não está apenas em campeonatos que ocorrem poucas vezes ao ano, a conformidade do funcionamento e estruturação da empresa às regras das plataformas é algo obrigatório desde o início. A gama de regras que existem e devem ser fielmente respeitas para permitir a participação é grande, tanto de plataformas digitais quanto organizações internacionais que buscam regular de forma mais uniforme o esporte pelo mundo. Para além das normas características de um esporte competitivo, os riscos relacionados à lavagem de dinheiro aparecem como outra razão justificadora de um quadro autorregulatório tão intenso das empresas envolvidas.

É importante, nesse sentido, ficar atento às orientações não vinculativas de confederações e outras organizações internacionais e nacionais de ciberesportes. Isso, contudo, não é nenhuma novidade em relação ao mundo esportivo tradicional quando é lembrada a existência da *Lex Sportiva* em vários outros esportes, oriunda em boa parte de regulamentos de entidades não governamentais e de tribunais arbitrais desportivos (FILHO, 2006, p. 27–28).

Mesmo as regras positivadas brasileiras deixam isso claro. A Lei Pelé dá grande realce à incorporação dessas fontes não estatais, apontando já no art. 1º que o desporto brasileiro abrange práticas não formais. Mais ainda, no parágrafo primeiro desse artigo aponta que, além das normas nacionais e internacionais, a regulação da prática desportiva é dada "pelas regras de prática desportiva de cada modalidade, aceitas pelas respectivas entidades nacionais de administração do desporto". O Superior Tribunal de Justiça também já reconheceu a importância das regras das federações internacionais no desporto, inclusive para aqueles com

maior quantia de regulações estatais brasileiras, como é o futebol (BRASIL, 2013).

Por outro lado, nos *e-sports* de maneira geral não há entidades ou confederações com uma dominância tão grande quanto, a título de exemplo, a FIFA tem no futebol (ABANAZIR, 2019, p. 2). Uma rápida consulta nos mostra uma incerteza sobre qual será a associação, federação ou outro tipo de entidade mais influente no cenário global, ainda que algumas entidades estejam conseguindo até respaldo de seus governos nacionais ou de grandes empresas de tecnologia de seu país nessa disputa.

Pode-se citar, embora comumente não sejam conflitantes entre si e busquem propósitos específicos para se diferenciar e permitir uma convivência harmoniosa, a *International Esports Federation (IESF)*, a *Esports World Federation (EWSF)*, a *Global Esports Federation (GEF)* e a *World Esports Association (WESA)*. Uma busca no site dessas entidades mostra uma variedade de regulamentos e códigos de condutas próprios para seus membros.

O mesmo ocorre no Brasil, como se vê nos exemplos da Confederação Brasileira de *e-Sport* (CBeS), Confederação Brasileira de *Games e E-sports* (CBGE) ou da Confederação Brasileira de Esportes Eletrônicos (CBEE), valendo notar a maior dificuldade de consolidação até no fato de que uma ou outra dessas entidades tem sites de aparência simplória e nenhum parceiro de renome.

Esse cenário, felizmente, não se repete dessa forma no pôquer, até por ter também grande representação na parte presencial e envolver quantias monetárias elevadas há várias décadas. Há algumas organizações fortes consolidadas tanto a nível nacional quanto internacional, que conseguem se destacar e se tornar referências para busca de orientações.

Internacionalmente destaca-se a *International Federation of Match Poker (IFMP)*. Essa entidade conseguiu em 2010, apenas um ano após ser criada (e enquanto ainda era chamada de Federação Internacional do Pôquer – ou IFP, em inglês), ser aceita como membro provisório da Associação Internacional de Esportes da Mente (*IMSA - International Mind Sports Association*).

No Brasil existe a Confederação Brasileira de Texas Hold'em (CBTH), que, ganhando importância em um movimento similar ao que fez a IFMP, diligenciou em 2012 junto ao Ministério do Esporte para ser incluído na lista de organizações reconhecidas pelo governo. Isso, diferentemente do que se noticiou à época em diversos sites (HERMESMEYER, 2012), não era um reconhecimento como esporte, e sim uma análise essencialmente formal (FRANCESCHINI, 2012). No entanto, em novos esforços posteriores a CBTH obteve um compromisso em 2015 para que o Ministério regulamentasse o pôquer como esporte (KOJIKOVSKI; MARTINS, 2015), um procedimento que acabou ainda não se completando diante das turbulências no cenário político e econômico brasileiro desde então. A Confederação também acompanha e divulga o processo e as decisões judiciais que reconhecem o pôquer como um esporte da mente ou jogo de habilidade, e não um jogo azar (CBTH, 2019).

De qualquer forma, a grande diferença na importância da autorregulação para os esportes eletrônicos é o papel central assumido pelas *publishers*, ou seja, as empresas que divulgam os jogos, que não raramente são as mesmas que as produziram. Como elas são titulares dos códigos envolvidos nos jogos, elas são também capazes de fazer (e, em grande medida, impor) as regras não só internas, mas também externas – como as de participações em campeonatos. Afinal, sem a autorização dessas empresas o campeonato sequer pode ser organizado, especialmente por vedações oriundas dos direitos de propriedade intelectual (ABANAZIR, 2019, p. 6–8).

No pôquer jogado de forma online percebe-se esse papel pelas normas de plataformas com maior poder no mercado, como a conhecida *PokerStars*, que impõe diversos limites extralegais aos jogadores, como é possível ver nas limitadas possibilidades de saque do valor acumulado na conta do jogador, geralmente por carteiras digitais ou transferências para contas bancárias com deságios altíssimos[4]. Isso ocorre comumente por pressões de órgãos governamentais ou como uma estratégia para evitar a interferência e investigações de órgãos policiais e judiciais.

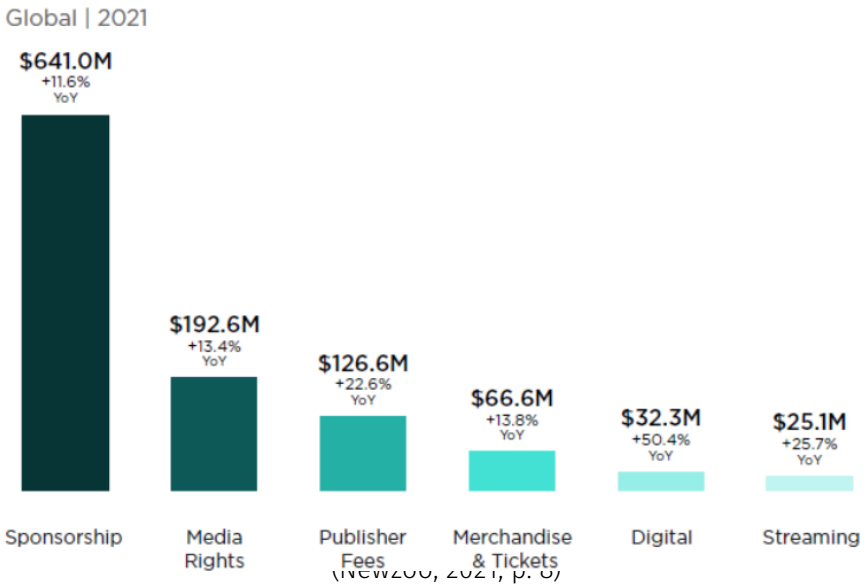
4. TÓPICOS ESPECÍFICOS DO PLANEJAMENTO: QUESTÕES DE PROPRIEDADE INTELECTUAL

Como é possível notar pelos parágrafos anteriores, os direitos intelectuais são um aspecto que precisa de particular atenção quando se fala de planejamento societário de *e-sports* (no mesmo sentido, SUMMERLY, 2020, p. 63). Aqui se juntam não só a importância geral que ativos imateriais têm para empresas (como marcas), mas também a importância dos direitos de imagem e de arena nos esportes em geral e, mais ainda, a importância dos direitos de propriedade intelectual nas empresas de jogos eletrônicos.

Quando alguém pensa em jogadores ou jogos com grande projeção, esses direitos são úteis principalmente para alguns objetivos, ainda que sem se resumir a eles, como (i) atrair dinheiro dos investidores; (ii) proporcionar receita com o licenciamento e ter moedas de troca em negociações; (iii) montar uma estrutura defensiva para poder utilizar sem obstáculos os sinais distintivos da empresa/time.

4 A seção "Política de Saques" do site do PokerStars.com detalha as formas de sacar o equivalente em dinheiro que está nas contas da plataforma, a exemplo das opções pelo NETELLER, Skrill, Muchbetter, ecoPayz, Paypal, Transferência Bancária direta, Visa, dentre outros.

Afinal, segundo o já mencionado relatório da Newzoo, a renda proveniente dos e-sports é em grande parte dependente de um bom manejo desses direitos de propriedade intelectual e dos bens que são objeto deles, aproveitando os grandes públicos do evento e capitalizando no patrocínio de investidores e rendas provenientes de publicidade de forma geral:



(Newzoo, 2021, p. 8)

Apesar do *e-sport* ser inegavelmente uma área ligada à tecnologia, os times geralmente não terão como foco o desenvolvimento de tecnologias em si. O que importa, em um primeiro momento, é o gerenciamento da imagem, direito de arena e sinais distintivos comerciais ligados ao time e aos jogadores, incluindo uma análise cuidadosa de disponibilidade prévia, visto que é comum o uso de certas expressões nos esportes eletrônicos, mesmo que em jogos diferentes.

Há um caso conhecido a nível internacional da *publisher Riot* (*League of Legends*), contra um time de múltiplos jogos de FPS,

chamado Riot Squad (CARPENTER, 2019). O caso ainda está para ser decidido, mas já expõe o risco de um time não ser suficientemente diligente nessa área, valendo a pena tomar precauções mesmo em casos nos quais o conflito não seja certo, pela marca ou sinal distintivo escolhido ter um caráter genérico.

A falta de planejamento prévio nesse campo pode causar efeitos desastrosos, especialmente se o que fazer em relação à cessão de direitos em situações de afastamento ou desligamento de sócios não for bem regulamentado. No Brasil há o exemplo da Ilha da Macacada *Gaming* que teve que se renomear para *Razer Pichau Gaming* no meio de um campeonato em razão de uma disputa judicial de direitos sobre o nome do time (THIAGO, 2018).

Por um lado, seria possível argumentar que essa não é uma situação tão urgente ou preocupante, afinal, ao se reconhecer os *e-sports* como verdadeiros esportes, observa-se a incidência da proteção do art. 87 da Lei Pelé, que determina ser automática e dispensar o registro para a proteção da "denominação e [d]os símbolos de entidade de administração do desporto ou prática desportiva, bem como o nome ou apelido desportivo do atleta profissional", inclusive para uso comercial.

Porém, para além da falta de segurança jurídica quanto ao reconhecimento desses jogos digitais como modalidade esportiva, ainda é incerto no ordenamento brasileiro a questão das disputas de direitos de propriedade intelectual registrados no INPI com os direitos de propriedade intelectual firmados na Lei Pelé, além do licenciamento feito a partir de marca registrada ser muito mais seguro, e ter oportunidades muito mais amplas de utilização em razão do respaldo art. 139 e 140 da Lei de Propriedade Industrial[5].

5 Art. 139. O titular de registro ou o depositante de pedido de registro poderá celebrar contrato de licença para uso da marca, sem prejuízo de seu direito de exercer controle efetivo sobre as especificações, natureza e qualidade dos

Nessa mesma seara, o planejamento estratégico da sociedade abarca pensar, já nos primeiros momentos, sobre os segredos de negócios. Questões como métodos e técnicas inovadoras de treinamento (ou até estratégias de jogo) devem ser protegidas desde os primeiros passos por meio de segredos industriais, elaborando-se contratos de confidencialidade e se estabelecendo procedimentos internos que configurem o esforço de sigilo, inclusive em atos constitutivos ou contratos de trabalho. A identificação de informações relevantes que podem ser protegidas como segredos de negócios nos esportes tradicionais, é um tema difícil que frequentemente é objeto de estudos, especialmente quando o treinamento envolve alta tecnologia (GROW; GROW, 2017; WERRA, 2010).

Pensando nas rendas provenientes do *streaming* ao vivo pelos jogadores, é importante prever desde os passos iniciais as instruções sobre as particularidades da aplicação das regras de direitos autorais para os membros do time, assim como o regime de responsabilização no caso de infração e divisão de lucros (ROBINSON, 2018). Da mesma forma, a estrutura societária deve pensar a atribuição originária e remuneração referente a outros tipos de propriedade intelectual caso o time tenha interesse em produzir material próprio para vender em lojas virtuais, o que é uma tendência das maiores empresas nesse setor.

Embora tudo isso pareçam preocupações que só fazem sentido à medida que a empresa de *e-sports* estiver crescendo exponencialmente, são na verdade questões que devem ser pensadas no momento de criação da empresa e fixação nos documentos essenciais.

---

respectivos produtos ou serviços. (...)
Art. 140. O contrato de licença deverá ser averbado no INPI para que produza efeitos em relação a terceiros.

Várias perguntas devem feitas e respondidas já nesse primeiro momento: A gestão dos direitos de imagens e dos sinais distintivos dos jogadores serão deles mesmos, ou gerenciados (e sob titularidade) da empresa? Está previsto no contrato social e/ou nos contratos de trabalho o que ocorre com os ativos intelectuais no caso do fim da relação entre o indivíduo e o time? A divisão dos valores resultantes de negociações desses bens também? Os direitos autorais do site da empresa estão sob titularidade dela mesmo, com expressa previsão no contrato feito com o programador e o designer? Os direitos sobre textos produzidos por colaboradores e publicados no site são da empresa ou deles mesmos? Todos os funcionários e jogadores estão cientes de quais são as informações sigilosas, e as medidas que devem tomar para mantê-las dessa forma?

Por fim, tanto no momento de planejamento quanto durante momentos importantes da empresa (fusões, aquisições, retiradas de sócios, dentre outros) é importante, para além de uma determinação prévia dos procedimentos necessários para possibilitar a continuidade do time, fazer auditorias dos ativos intelectuais da empresa, listando e juntando a documentação comprovativa sobre:

• Marcas de propriedade da empresa, registradas ou não, concedidas ou em processo de concessão, assim como os acordos/contratos ligados a elas;

• Marcas utilizadas pela empresa, mas que não são de sua titularidade, assim como os acordos/contratos ligados a elas;

• Nomes empresariais de propriedade da empresa, concedidas ou em processo de concessão, assim como os acordos/contratos ligados a elas, além de eventuais utilizações autorizadas de nomes empresariais de terceiros.

• Outros sinais distintivos, registrados ou não, assim como os acordos/contratos ligados a elas, além de eventuais utilizações autorizadas de nomes empresariais de terceiros.

• Direitos autorais sob titularidade da empresa, explicitando a data que o direito entrou em vigor, quem foram os criadores intelectuais e juntando os contratos de cessão/licenciamento relativos a eles;

• No caso de programas de computador, para os quais a atribuição originária à empresa é facilitada, devem ser elencados os contratos de prestação de serviços e de trabalho.

• No caso de programas de computador de titularidade de terceiros utilizados pela empresa, eles devem ser identificados e elencadas as licenças, mesmo que sejam só licenças de uso;

• No caso de direitos conexos, cópias dos contratos/acordos firmados com empresas terceiras que os administrem;

• Nomes de domínio utilizados pela empresa, mesmo que apenas para redirecionamento;

• Outros direitos de propriedade industrial voltados a produtos criados ou utilizados pela empresa (patentes, modelos de utilidade, desenhos industriais), concedidos ou em processo de concessão, assim como os acordos ligados a eles e a identificação dos inventores;

• Acordos/contratos relacionados a *know-how*, segredos de negócios e desenvolvimentos de novas tecnologias (em sentido amplo);

• Exemplo do contrato padrão de consultoria utilizado para contratar consultores externos envolvidos no desenvolvimento de métodos, produtos ou serviços;

• Qualquer outro acordo ou contrato relacionado ao *trade dress* da empresa;

• Contratos feitos com os advogados ou agentes de propriedade intelectual contratados pela empresa;

• Relatórios de avaliação de risco, se cabível.

Isso pode parecer já bastante complexo, mas vale lembrar que as questões relacionadas aos direitos de propriedade intelectual dentro de uma empresa são apenas algumas dentre as problemáticas que devem ser abarcadas em um planejamento societário cuidadoso. Não é a única, e comumente não será a mais importante, das preocupações que o jogador de e-sport deve ter, que também terá prioridades diferentes de acordo com a modalidade de *e-sport* praticada e com as pretensões comerciais de expansão ou diversificação de atividades da empresa.

Para o exemplo do pôquer, mais do que os direitos intelectuais, uma preocupação notável é a tributação incidente sobre sua atividade (MARQUES, 2012, p. 212–214). Afinal, como enquadrar os valores ganhos? Eles são realmente uma aposta? Se as plataformas online obrigam a retirada na forma de pessoa física, mesmo que se atue com um time, de uma forma altamente empresarializada, como evitar que a Receita ache que está ocorrendo uma simulação? Como a plataforma de pôquer online está localizada no exterior, as fichas na conta precisam ser declaradas? Como é a forma correta de trazer esse dinheiro para uma conta brasileira?

Mesmo quando as dúvidas parecem ter uma solução mais direta, com uma orientação relativamente clara de um órgão público, é preciso ter cuidado. Essa não é nem uma dificuldade apenas brasileira, ela se repete em diversos outros países do mundo (ALARIE, 2010; DUDA, 2010). Os órgãos públicos responsáveis pela arrecadação geralmente buscam, em suas orientações, maximizar os valores auferidos. Isso é perceptível, para citar casos concretos, nos entendimentos sobre recebimento de prêmios em concursos e competições esportivas. Entretanto, essas orientações não só podem como devem ser questionadas em situações em que elas visivelmente se encaixam mal.

Não faltam bons exemplos de situações em que isso ocorreu. Mais recentemente pode-se lembrar do entendimento da Receita Federal sobre a tributação de rendimentos recebidos do exterior por pessoa física decorrentes de ganhos em apostas online, na Resolução de Consulta Disit/SRRF03 nº 3007, de 04 de outubro de 2018, apontando para o caminho do carnê-leão no mês de recebimento, sem que fossem descontadas a dedução de perdas nas apostas realizadas. Embora isso seja um caminho razoável no caso de apostas tradicionais, pode até mesmo inviabilizar a atividade do jogador do pôquer, que estatisticamente perde grandes quantias com *buy-ins* para poder ter lucros.

Na mesma linha, a Receita Federal classicamente percebe com maus olhos o recebimento por pessoas jurídicas de valores provenientes de atividades tradicionalmente relacionadas às pessoas físicas, especialmente quando estes têm natureza intelectual (BRASIL, 2016).

Porém, assim como outros entendimentos firmados pela Receita na perspectiva de maximizar a arrecadação, tal posição é crescentemente afastada pelos Tribunais brasileiros. Um julgamento bastante recente do Supremo Tribunal Federal demonstra isso

de forma categórica, ao mudar radicalmente o paradigma vigente da impossibilidade de "pejotizar" atividades intelectuais, abrindo portas para novas estruturas empresariais capazes de diminuir a carga tributária de esportistas. Trata-se da Ação Direta de Constitucionalidade n. 66, no qual os ministros decidiram por oito votos a dois pela constitucionalidade do artigo 129 da Lei 11.196/05 (BRASIL, 2020). Na prática, isso tornou vinculante o entendimento de que prestar atividades intelectuais de natureza personalíssima e receber como pessoa jurídica não pode mais ser, por si só, tratado, pelo menos até então, como ilícito tributário pela Receita.

Em outras palavras, uma simples submissão cega às orientações genéricas da Receita pode não ser o melhor caminho quando há soluções lícitas passíveis de construção a partir da estrutura da empresa, de seus administradores e de seus funcionários. Ao identificar que as razões de tributação não refletem a realidade de como a atividade realmente se desenrola, é possível trabalhar de forma cuidadosa com o planejamento societário e montar uma estrutura bem embasada juridicamente, pensando sempre na possibilidade justificação das escolhas e construção de uma tese jurídica sólida perante um tribunal.

5. CONCLUSÃO

A profissionalização do *e-sports* implica também na profissionalização de sua gestão. Isso inclui, evidentemente, a participação de profissionais especializados não só na atividade desportiva eletrônica em si, mas também daqueles que cuidem da parte organizacional e burocrática, permitindo que o e-atleta possa se concentrar na partida. A gestão profissional, mesmo de times de menor porte, inclui não apenas uma equipe para cuidar do treinamento (físico, psicológico, etc.), mas também figuras geralmente vinculadas à imagem de grandes empresas – como gestor de marketing, advogado, contador e outros.

Iniciativas legislativas indicam uma preocupação do Estado em regular a questão, particularmente no ponto da tributação de receitas provenientes dessas modalidades esportivas até então inexistentes. Uma boa gestão e um planejamento societário adequado ajudam e evitar que essa regulamentação acabe se tornando prejudicial para o desenvolvimento da empresa, como evitando tributações a mais por entendimentos maximalistas da Receita Federal.

Para que esse resultado seja atingido, um dos pontos centrais é formular cuidadosamente a própria estrutura da empresa, para utilizar um cenário de regulamentação nebuloso em seu favor, em vez de deixar que ele se torne um obstáculo intransponível ou uma multa alta em alguns meses ou anos. Não se pode imaginar que uma gestão desordenada possa produzir bons frutos, ou que alicerces frágeis permitam a construção de uma estrutura robusta para o futuro. Assim como em outras empresas consideradas de áreas mais tradicionais, também é fundamental organizar a atividade voltada aos e-sports para que os resultados sejam otimizados.

Do ponto de vista regulatório é bom relembrar as críticas de que um modelo engessado, que almeje disciplinar detalhadamente o que se pode fazer e como isso deve ser feito, tende a nascer obsoleto. Ao invés de determinar o que o *e-sport* deveria ser, o Estado deveria se atentar em criar, por meio de princípios estimulantes, um cenário em que os envolvidos tenham segurança jurídica para desenvolver suas atividades regularmente e profissionalmente.

O pôquer, como exposto, é um ótimo exemplo para se analisar essa situação, porque regulamentações diversas pensadas em outros campos podem se aplicar a ele. Exemplos são as regras sobre jogo de azar, de apostas, regulamentações de esportes tradicionais ou mesmo de outros esportes eletrônicos, dentre

outros. Porém, o pôquer tem características próprias, que não são encontradas cumulativamente em nenhum dos outros quadros fáticos que poderiam ser estendidos a ele. Para citar algumas, ele já existia como um mercado forte mesmo antes da explosão da Internet, já foi criminalizado, envolve dinheiro para além das premiações finais em campeonatos, é jogado por um largo ecossistemas de plataformas diferentes (em vez de apenas uma *publisher* como ator central).

É enorme a potencialidade de combinar essas diferentes regras previamente existentes, assim como outras que estão se consolidando aos poucos, a fim de se chegar em um quadro regulatório realmente adequado ao pôquer, permitindo o estímulo à atividade e até mesmo uma cobrança tributária que não seja percebida como abusiva por estes esportistas intelectuais.

Em outras palavras, na falta desse quadro regulatório bem elaborado, cabe aos interessados achar formas de obter resultados similares por outros meios. O planejamento societário, para o qual não há fórmula mágica e um passo-a-passo fixo, é uma dentre as ferramentas possíveis para que as pessoas envolvidas com *e-sports* possam, a longo prazo, centrar suas energias na sua atividade profissional, em vez de gastar esse tempo valioso com problemas decorrentes da falta de zelo nos passos iniciais.

REFERÊNCIAS BIBLIOGRÁFICAS

ABANAZIR, Cem. ***Institutionalisation in E-Sports***. *Sport, Ethics and Philosophy*, v. 13, n. 2, p. 117–131, 3 abr. 2019.

ALARIE, Benjamin. ***Tax Law on Poker Winnings: Read It and Weep***. LawNow, v. 34, p. 34–36, 2010.

AZEVÊDO, Pedro Henrique. **O Esporte como Negócio: uma visão sobre a gestão do esporte nos dias atuais**. Revista EVS - Revista de Ciências Ambientais e Saúde, v. 36, n. 5, p. 929–939, 2009.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 3.450, de 28 de outubro de 2015. **Acrescenta o inciso V ao artigo 3º da Lei 9.615/1998, que "Institui normas gerais sobre desporto", para reconhecer o desporto virtual como prática esportiva".** Brasília: Câmara dos Deputados, 2013.Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2025514. Acesso em: 19 mai. 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 7.747, de 30 de maio de 2017a. **Institui o esporte virtual**. Brasília: Câmara dos Deputados, 2013. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2139618. Acesso em: 19 mai. 2021.

BRASIL. Receita Federal. **O fenômeno da "pejotização" e a motivação tributária**. Abril/2016. Brasília, DF, 2016. Disponível em: https://receita.economia.gov.br/dados/receitadata/estudos-e-tributarios-e-aduaneiros/estudos-e-estatisticas/estudos-diversos/o-fenomeno-da-pejotizacao-e-a-motivacao-tributaria.pdf. Acesso em: 16 mai. 2021.

BRASIL. Senado Federal. Proposta de Projeto de Lei do Senado nº 383, de 10 de outubro de 2017b. **Dispõe sobre a regulamentação da prática esportiva eletrônica**. Brasília, DF: Senado Federal, 2017. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/131177. Acesso em: 19 mai. 2021.

BRASIL. Superior Tribunal de Justiça (STJ), **ROMS n.º 15.449-MG**, 2ª Turma, Rel. Min. Eliana Calmon, j. 14.04.2003.

BRASIL. Supremo Tribunal Federal (STF), **ADC 66**. Rel. Min. Carmen Lucia, j. 21.12.2020. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5794122. Acesso em: 19 mai. 2021.

BRASIL. Superior Tribunal de Justiça (STJ), **Recurso Especial N. 1.296.944 – RJ**, 4ª Turma. Rel. Min. Luis Felipe Salomão, j. 7.5.2013.

BRASIL. Tribunal de Justiça de Santa Catarina (TJ/SC), **Mandado de Segurança n. 2010.047810-1**. Rel. Des. Sérgio Roberto Baasch Luz. j. 27.10.2011.

CAMBRIDGE DICTIONARY. **Definição de e-sports**. Disponível em https://dictionary.cambridge.org/pt/dicionario/ingles/e-sports. Acesso em: 19 mai. 2021.

CARPENTER, Nicole. ***Riot Games files lawsuit against esports organization over 'Riot' trademark***. POLYGON. 10/10/2019. Disponível em https://www.polygon.com/2019/10/10/20908027/riot-games-copyright-trademark-lawsuit-riot-squad. Acesso em: 19 mai. 2021.

CARVALHO, Mário Tavernard Martins de. **Planejamento Sucessório no Âmbito da Empresa Família**. In: COELHO, Fabio Ulchoa; FÉRES, Marcelo Andrade (Eds.). Empresa Familiar. São Paulo: Saraiva, 2014.

CASTRO, Luis Roberto Martins. **Conceito e Evolução Sociológica do Esporte**. In: Enciclopédia de Gestão, Marketing e Direito Desportivo. Porto Alegre: INEJE, 2017.

CBTH – Confederação Brasileira de Texas Hold'em. **CBTH celebra decisão judicial favorável ao poker no Rio de Janeiro**. CBTH. 07/2019. Disponível em https://www.cbth.org.br/. Acesso em: 19 mai. 2021.

DUDA-HYZ, Michalina. ***Taxation of Poker Winnings in Polish Tax Law***. Rev. Comp. L., v. 14, p. 127–144, 2010.

GROW, Lara; GROW, Nathaniel. ***Protecting Big Data in the Big Leagues: Trade Secrets in Professional Sports***. Washington and Lee Law Review, v. 74, n. 3, p. 1567-1622, 2017.

FILHO, Álvaro Melo. **Direito desportivo: aspectos teóricos e práticos**. São Paulo: IOB Thompson, 2006.

FRANCESCHINI, Gustavo. **Pôquer comemora "aval" do governo e agora quer regulamentação da atividade no país**. UOL. 03/02/2012. Disponível em: https://www.uol.com.br/esporte/ultimas-noticias/2012/02/03/poquer-comemora-aval-do-governo-e-agora-quer-regulamentacao-da-atividade-no-pais.htm. Acesso em: 19 maio 2021.

HERMESMEYER, Luiz Fernando. **Ministério dos Esportes Reconhece Oficialmente a Confederação Brasileira de *Texas Hold'em*. *PokerNews***. 27/01/2012. Disponível em: https://br.pokernews.com/noticias/2012/01/ministerio-dos-esportes-reconhece-oficialmente-a-cbth-4308.htm. Acesso em: 12 jun. 2021.

KOJIKOVSKI, Gian; MARTINS, Raphael. **Ministério do Esporte vai regulamentar o pôquer no Brasil**. Exame. 02/08/2017. Disponível em: https://exame.com/brasil/ministerio-do-esporte-vai-regulamentar-o-poquer-no-brasil. Acesso em: 21 julho 2021.

LUBET, Steven. ***The Game Is Lawyers' Poker***. *Litigation*, v. 32, n. 1, p. 59–70, 28 jul. 2005.

MARQUES, Leonardo Araujo. **Aspectos legais e tributários do poker e dos demais esportes da mente: a necessidade de uma regulamentação específica**. Revista da EMERJ, Rio de Janeiro, v. 59, p. 199–216, 2012.

MIGUEL, Ricardo Affonso Georges. **O enquadramento jurídico do esporte eletrônico**. 2018. 126 p. Dissertação (Mestrado em Direito) - Universidade Estácio de Sá, Rio de Janeiro, 2018.

NESSON, Charles; WOODS, Andrew. ***Commentary on the Law of Poker***. *Richmond Journal of Global Law and Business*, v. 8, 2008.

NEWZOO. **Newzoo's Global Esports & Live Streaming Market Report 2021**. Shanghai. Disponível em: https://resources.newzoo.com/hubfs/Reports/2021_Free_Global_Esports_and_Streaming_Market_Report_EN.pdf. Acesso em: 21 jul. 2021.

OLIVEIRA, Jair de; TERENCE, Ana Cláudia Fernandes; ESCRIVÃO FILHO, Edmundo. **Planejamento estratégico e operacional na pequena empresa: impactos da formalização no desempenho e diferenças setoriais**. RGO - Revista de Gestão Organizacional, p. 119–133, 2010.

THIAGO. **IDM Jogará Como *Razer Pichau Gaming (RPG)* Na Fase De Escalada Do CBLoL**. Pichau Arena. 10/08/2018. Disponível em https://www.pichauarena.com.br/pichau-arena/idm-jogara-co-

mo-rpg/. Acesso em: 19 mai. 2021.

REALE JR., Miguel. **Parecer elaborado após consulta da CBTH**. fls. 122-152. 07.04.2010. In: BRASIL. Tribunal de Justiça de Santa Catarina (TJSC), MS n. 2010.047810-1, Grupo de Câmaras de Direito Público, Rel. Des. Sérgio Roberto Baasch Luz, j. 26/10/2011.

ROBINSON, Nicholas. ***From Arcades to Online: Updating Copyright to Accommodate Video Game Streaming***. North Carolina Journal of Law & Technology, v. 20, no. 2, p. 286-330, dec. 2018.

SEBRAE. **As Pequenas Empresas do Simples Nacional**. 2011. Disponível em https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/As_pequenas_empresas_SN.pdf. Acesso em: 21 mai. 2021.

STEFANI, Ray. ***E-sports, mind sports and the Olympics: What is a sport, anyway? Significance***. 28/03/2017. Disponível em: https://www.significancemagazine.com/sports/539-e-sports-mind-sports-and-the-olympics-what-is-a-sport-anyway. Acesso em: 18 mai. 2021.

SUITS, Bernard. ***The elements of sports***. In: MORGAN, William (Ed.). Ethics in sport. Champaign: Human Kinectics, p. 9–19, 2007.

SUMMERLEY, Rory. ***The Development of Sports: A Comparative Analysis of the Early Institutionalization of Traditional Sports and E-Sports***. Games and Culture, v. 15, n. 1, p. 51–72, 2020.

WERRA, Jacques de. ***How to Protect Trade Secrets in High-Tech Sports? An Intellectual Property Analysis based on the Experiences at the America's Cup and in the Formula One Championship***. *European Intellectual Property Review*, v. 32, n. 4, p. 155-164, 2010.

BANIMENTOS E ARREPENDIMENTOS EM GAMES E COMPETIÇÕES "VAC (VALVE ANTI-CHEAT) BAN"

BANNING AND REGRETS IN GAMES AND COMPETITIONS''VAC (VALVE ANTI-CHEAT) BAN''

Camila Israel Rosa
Head of Legal - Detona Gaming. Pós-graduada em Direito Digital e Compliance pela Damásio IBMEC. Cursando especialização em Proteção de Dados Pessoais.
camila@camilarosa.adv.br

Mariane Siqueira Moreira
Advogada no Balconi Moreti-Advocacia da Inovação. Pós-graduada em Direito Tributário - IBET. LLM em Direito Empresarial - FGV. Mediadora judicial em formação (CEJUSC). Cursando Mediação e Arbitragem Avançadas – SFERA. Membro da Comissão de Inovação e Gestão da OAB/PR e Secretária da Comissão de Inovação e Gestão da OAB-Londrina.
marianesiqueira.balconimoreti@gmail.com

RESUMO:
O cenário de esports vem ganhando relevância mundial e, com seu crescimento, aumentam também as tentativas de trapaça e outras situações que necessitam regulação. Uma das soluções contra trapaça, apresentada pela desenvolvedora de jogos Valve, foi o VAC Ban *(Valve Anti-Cheat Ban)*, que será o principal objeto de estudo deste artigo. Trata-se de banimento polêmico, aplicado pela desenvolvedora aos usuários que trapaceiam dentro dos seus jogos. Até pouco tempo, esse banimento tinha caráter arbitrário, aplicado por tempo indeterminado, não permitindo ao jogador banido qualquer defesa ou proporcionalidade na penalidade. Diante das controvérsias que envolvem esse assunto, é necessário um estudo detalhado, para melhor compreensão dos

banimentos e suas limitações, seja na sua prática recreativa ou em competições, especialmente no que se refere ao *VAC Ban*. Serão abordados neste artigo os conceitos das palavras *cheat*, *hack* e *VAC Ban*, bem como será analisada essa modalidade de punição sob diversos aspectos. Ainda, serão citados alguns exemplos de jogadores que sofreram o banimento VAC, demonstrando o impacto causado pela punição na vida e na carreira desses atletas. Por fim, haverá um comparativo à legislação brasileira, buscando fazer uma analogia com o código penal e com a legislação específica desportiva, no que se refere à prática de doping esportivo ou outras espécies de trapaça dentro dos jogos.

Palavras-Chave: Banimento. Arrependimento. VAC Ban. *Esports*. *Games*.

ABSTRACT:
The esports scenario has been gaining relevance worldwide and, with its growth, attempts at cheating and other situations that need regulation also increase. One of the solutions against cheating, presented by game developer Valve, was the VAC Ban 2 (Valve Anti-Cheat Ban), which will be the main object of study in this article. This is a controversial ban, applied by the developer to users who cheat within their games. Until recently, this ban had an arbitrary character, applied indefinitely, not allowing the banned player any defense or proportionality in the penalty. In view of the controversies involving this matter, a detailed study is needed, in order to better understand the bans and their limitations, whether in their recreational practice or in competitions,

especially with regard to the VAC Ban. In this article, the concepts of the words cheat, hack and VAC Ban will be addressed, as well as this type of punishment will be analyzed under several aspects. Also, some examples of players who suffered the VAC ban will be mentioned, demonstrating the impact caused by the punishment on their lives and careers. Finally, there will be a comparison with Brazilian legislation, seeking to make an analogy with the penal code and with specific sports legislation, with regard to the practice of sports doping or other types of cheating within games.

Keywords Ban: *Repentance. VAC Ban. Sports. Games.*

1. INTRODUÇÃO

Os banimentos nos *esports* ganharam destaque nos últimos anos, principal-mente devido ao número de atletas profissionais de esportes eletrônicos que tiveram sua carreira afetada e prejudicada de alguma maneira pelo uso, ainda que anterior à sua profissionalização, de *softwares* utilizados com a finalidade de trapacear dentro dos jogos, prática que é comumente conhecida como *cheat*.

Não é incomum realizar uma busca na internet e se deparar com diversas notícias sobre o assunto, sendo que a frequência com que surge alguma notícia de um atleta com uma conta banida só aumenta.

O *cheat* ou *hack* também se refere às modificações realizadas nos arquivos base dos jogos através de *softwares* desenvolvidos por terceiros.

Com a profissionalização dos *games*, passando os jogos a terem caráter competitivo e seus jogadores serem equiparados a atletas, existe o nascimento de uma nova relação jurídica.

Assim, se faz necessária a adequação das normas jurídicas ao caso concreto, até que esse novo segmento seja regulado e possua legislação específica. Porém, muitas dúvidas surgem nesse momento, uma vez que esse cenário é bastante inovador e traz situações nunca experimentadas antes.

Um dos desafios é em relação à globalização dos esportes eletrônicos e o impacto que esse fato possui quanto à legislação aplicável.

É muito comum que a desenvolvedora do jogo seja de um país (seguindo a legislação do mesmo), a equipe de esportes eletrônicos seja de outro e, ainda, que essa equipe tenha jogadores de outras nacionalidades. Isso sem mencionar quando essas equipes participam de campeonatos internacionais.

Outro ponto bastante complexo é a aplicação de uma penalidade que satisfaça todos os envolvidos, portanto, uma boa fundamentação se faz necessária na aplicação da pena.

Afinal, quem sofre a penalidade sente-se, normalmente, injustiçado, enquanto aquele que foi prejudicado pela trapaça sempre vai pensar que a punição não foi suficiente para o prejuízo suportado.

Por outro lado, ainda temos as equipes e as organizações que, na maioria dos casos, desconhecem a trapaça que foi praticada por um único membro da equipe, porém, acabam arcando também com as consequências dessa prática.

Inúmeros são os pontos de vista, opiniões e posicionamentos, muitas vezes, vindos de pessoas que não possuem uma visão holística do negócio, cada qual de-fendendo seus interesses.

Por isso é preciso ter cautela e realizar uma análise bastante imparcial de todos os aspectos, na tentativa de chegar ao máximo de razoabilidade e proporcionalidade possível.

Este artigo busca a abordagem de diversas questões referentes aos banimentos em competições de esportes eletrônicos, de forma que seja possível a compreen-são da aplicação dessa punição e sua análise sob a ótica das normas e princípios jurídicos.

O artigo trará, em primeiro lugar, o conceito de VAC Ban, que é uma das modalidades de banimento mais conhecidas, dentro dos esportes eletrônicos.

Em seguida, este artigo trará uma análise do banimento, de forma a examinar a aplicação da penalidade por parte da desenvolvedora de jogos Valve.

Após ampliar a compreensão a respeito da punição aplicada pela Valve, alguns casos com grande repercussão midiática serão apresentados.

Assim, ao final, após as devidas conceituações, esclarecimentos e apresentação dos casos, será traçado um comparativo com a legislação brasileira, possibilitando uma reflexão sobre o tema.

2. CONCEITO DE VAC BAN

Em um primeiro momento, para garantir ampla compreensão e discutir o tema proposto neste trabalho, faz-se necessário esclarecer alguns conceitos sobre terminologias comumente utilizadas no mercado de esportes eletrônicos.

O primeiro destes conceitos é o VAC Ban que é um dos mais famosos sistemas *"anti-cheat"*, ou antitrapaça, onde VAC significa *Valve Anti-Cheat* e *Ban* é a abreviação de banimento (KOVACS, 2020).

O segundo conceito é sobre a Valve e se refere à Valve Corporation, que é uma conhecida desenvolvedora de jogos eletrônicos e de distribuição digital. A empresa foi fundada em 1996 por dois ex-funcionários da Microsoft, e possui sede na cidade de Bellevue, estado de Washington (VALVE, sem data).

Alguns dos jogos desenvolvidos pela *Valve* são bastante conhecidos e relevantes no cenário de *games*, como *Half-Life, Counter-Strike, Portal, Day of Defeat, Team Fortress, Left 4 Dead e Dota 2* (VALVE, sem data).

Importante ressaltar que uma das criações mais famosas da empresa, e bastante utilizada pela comunidade *gamer*, é a Steam, que é uma plataforma de distribuição de jogos digitais para computadores. Esta plataforma foi criada em 2003 para servir como um canal de distribuição de conteúdo digital, antes mesmo que as lojas de aplicativos existissem.

Desde então, seu crescimento e expansão a transformaram em uma plataforma para milhares de criadores e editores fornecerem conteúdo e estabelecerem relacionamentos diretos com seus clientes.

A Comunidade Steam permite que milhões de jogadores façam o mesmo, compartilhando entretenimento e ideias. Além disso é muito utilizada por eles para fazerem amigos (VALVE, sem data).

Quando se trata de plataforma de distribuição de jogos eletrônicos para computadores, a Steam é a plataforma mais bem-sucedida do mundo, contando com mais de 35.000.000 (trinta e cinco milhões) de usuários ativos e uma enorme quantidade de *games* digitais em seu catálogo (CANALTECH, sem data).

O *VAC Ban* é, portanto, um sistema de banimento automatizado, que foi projetado pela Valve, considerando o grande número de usuários de sua plataforma e dos seus jogos, para detectar os *cheats* e banir o usuário, automaticamente, sempre que identificar que o computador utilizado por aquele jogador possui *cheats* identificáveis instalados, proporcionando, dessa forma, um ambiente mais seguro e uma experiência mais agradável para os seus usuários (STEAM, sem data).

Assim, o jogador que for banido pelo sistema *VAC Ban* ficará proibido de voltar a jogar o jogo no qual foi banido em servidores *VAC-Secured* (servidores prote-gidos e considerados seguros pela Valve, normalmente são servidores oficiais da empresa).

Importa salientar que o sistema VAC detecta *cheats*, sendo que qualquer modificação de terceiros em um jogo, projetado para dar a um jogador uma vantagem sobre outro, é classificada como uma fraude ou *hack* e irá desencadear um *VAC Ban*. Isso inclui modificações nos principais arquivos executáveis do jogo e nas bibliotecas de vínculo dinâmico (*dynamic link library*, ou DLL) (WIKIPÉDIA, sem data).

Esse tipo de banimento, por ser automatizado, não pode ser aplicado por pessoas, como é o caso dos administradores do servidor, que podem escolher banir jo-gadores específicos.

Alguns programas de bate-papo, configurações de *hardware* do sistema, ou drivers de sistema atualizados, como drivers de placa de vídeo, não são passíveis de causar banimento VAC.

A Valve afirma em sua página oficial que o usuário não será banido pelo sistema VAC a menos que faça login em um servidor *VAC secured* com um *cheat* instalado em seu computador (VALVE, sem data).

Por isso é tão importante que o usuário não forneça os dados de sua conta para terceiros, não faça login com sua conta Steam em computadores desconhecidos, como é o caso das *LAN houses*, e também não compartilhe sua biblioteca de jogos com terceiros.

O sistema *Valve Anti-Cheat*, apesar de ser mais conhecido por sua repercussão dentro do cenário de *Counter-Strike* (CS:GO), também é utilizado para outros jogos desenvolvidos pela Valve, como por exemplo: *DOTA 2, Team Fortress 2, Day Z, Rust, Left 4 Dead 2, Dying Light e ARK: Survival Evolved*.

Dessa forma, muitas pessoas associam erroneamente o *VAC Ban* apenas ao jogo *Counter-Strike*, devido à fama e relevância que essa ferramenta possui nessa modalidade de jogo, principalmente quando buscamos por notícias relacionadas ao assunto. Entretanto, o banimento deve ser associado à empresa Valve e a todos os jogos acima mencionados.

3. ANÁLISE DO BANIMENTO (PUNIÇÕES)

Feitas estas considerações introdutórias sobre conceitos importantes e a contextualização do cenário, a problemática a seguir abordada se refere às peculiaridades e aspectos da aplicação do banimento a jogadores de esportes eletrônicos, tema este em alta nas notícias e veículos informativos que acompanham este mercado.

Para tanto, será realizada a análise apenas do banimento realizado pela Valve pois cada desenvolvedora tem regras próprias de verificação de utilização de *softwares* de trapaça e procedimentos de aplicação de punições.

A própria Valve afirma, expressamente, em seu site, que os banimentos de VAC são permanentes, não negociáveis e que não podem ser removidos pelo Suporte Steam (STEAM, sem data).

A empresa também explica que não é possível apelar de um banimento VAC, ou seja, essa proibição não pode ser contestada. Segundo a empresa, se um banimento VAC for emitido incorretamente, ele será removido automaticamente após investigação (STEAM, sem data).

O VAC Ban possui alguns pontos polêmicos, como, no caso da sua conta ser utilizada por terceiros. Segundo a desenvolvedora, independentemente de quem estava utilizando a conta no momento da infração, os banimentos são permanentes e não serão removidos. A Valve alega a necessidade de manter uma política de tolerância zero para trapaças, a fim de promover um jogo justo que agrade a todos os jogadores.

Após um banimento VAC, o jogador perde todos os itens e jogos que possui, uma vez que estes não podem ser movidos de uma conta banida do VAC para uma conta diferente.

Entretanto, novos jogos ainda podem ser comprados e registrados em uma conta banida e a conta ainda pode receber itens, mas não pode enviá-los, o que pode acarretar enorme prejuízo financeiro ao usuário que teve sua conta banida.

O VAC Ban está associado ao número de telefone cadastrado pelo jogador. Assim, os banimentos são aplicados a todas as contas que compartilham um número de telefone no momento da infração.

Mesmo as contas que compartilham o número de telefone, e que não possuem o jogo para o qual o VAC foi banido, ainda receberão um VAC Ban e não pode-rão adquirir o jogo no futuro.

Salienta-se que ainda que o jogador trocasse de número telefônico, de com-putador, e conta Steam, ele poderia até conseguir jogar para se divertir, participando de jogos de um jogador, jogos de LAN locais e multijogador em servidores de jogos não protegidos por VAC, mas não seria possível sua participação em torneios oficiais da Valve.

Essa regra foi modificada recentemente, principalmente pela repercussão do caso V$M (Vinícius Santos Moreira), o qual abordaremos adiante.

Com a mudança da regra, o *VAC Ban* só poderá impedir a participação de um jogador em torneio oficial, caso o banimento tenha sido recebido a menos de cinco anos ou se aconteceu após a primeira participação do atleta em um campeonato da Valve, ou seja, o banimento não é mais por prazo indeterminado, agora ele

tem um limite estabelecido de 5 (cinco) anos, contados da data da infração que o gerou (desde que o atleta não tenha, ainda, participado de campeonato oficial da Valve) (VALVE, sem data).

Os outros efeitos do *VAC Ban* não foram modificados, sendo a elegibilidade em torneios oficiais a única alteração sofrida, assim como não houve nenhuma modificação nos demais motivos para um jogador não poder participar de um campeonato da Valve.
A Valve prevê, em seu Acordo de Assinatura da Steam:

> A Valve poderá terminar a sua Conta ou uma Assinatura específica por qual-quer conduta ou atividade que ela considere ilegal, que constitua um Método de Trapaça, ou que de outra forma afete negativamente a satisfação com o Steam dos outros Assinantes. Você reconhece que a Valve não é obrigada a avisá-lo previamente do término das sua(s) Assinatura(s) e/ou Conta (STEAM,2021).

Ou seja, de forma unilateral, a Valve pode encerrar a conta do usuário por qualquer conduta ou atividade que, no seu exclusivo entendimento, seja considerada ilegal, constitua trapaça ou afete negativamente a Steam, sem qualquer aviso prévio ao usuário.

4. CASOS

Alguns casos ganharam maior repercussão e relevância, sendo amplamente divulgados pela mídia, o que resultou, inclusive, em algumas alterações nas regras trazidas pela Valve, como citamos anteriormente.

4.1. HOVIK " KQLY " TOVMASSIAN

Ex-atleta de esportes eletrônicos, hoje profissional aposentado de *Counter-Strike: Global Offensive* e *Counter-Strike: Source*, o francês Hovik " KQLY " Tovmas-sian sofreu um VAC Ban em novembro de 2014.

Na época, ele era o *AWPer* (posição em que o jogador utiliza a arma AWP) secundário na equipe da *Titan esports*, onde era colega de equipe dos jogadores kennyS, Maniac, apEX e Ex6TenZ.

Com a notícia do banimento, a *Titan esports* suspendeu o atleta, que fez uma declaração oficial sobre o assunto no dia seguinte, admitindo que a punição seria "justificada" (LIQUIPEDIA, s/ data).

Como consequência do banimento, KQLY não poderia participar de qualquer torneio patrocinado pela Valve. Assim, inevitavelmente, o atleta foi expulso da equipe após algum tempo.

No ano de 2018, o ex-atleta ainda fundou a organização francesa eFrog, mas deixou a equipe no ano seguinte, ocasião em que se aposentou das competições e se mudou para Los Angeles, onde passou a conduzir uma empresa de aluguel de carros de luxo (LIQUIPEDIA, sem data).

Os banimentos VAC, na ocasião, eram por tempo indeterminado, o que acabava fazendo com que os atletas banidos mudassem de modalidade, partindo para jogos de outras desenvolvedoras, ou então se aposentassem.

Em abril de 2021, a Valve modificou as regras, limitando a cinco anos, conta-dos a partir data da infração, o período de banimento (GLOBO ESPORTE, 2021).

Figura 1

Hovik "KQLY" Tovmassian

KQLY atuou pela Titan, mas ficou marcado no cenário pelo banimento recebido — Foto: Divulgação

O jogador francês Hovik "KQLY" Tovmassian ficou conhecido por um dos headshots mais incríveis do mapa Dust2: o atleta pulou, deu um único tiro e acertou o oponente dentro do bombsite A. Mas, além do caso de sucesso, KQLY também ficou famoso por ser banido pouco antes da disputa da DreamHack Winter 2014. O jogador foi afastado do time Titan e mesmo assim a equipe foi desqualificada do torneio.

Fonte: Luiz Felipe Lima, para o site TechTudo, em 18/07/2018 08h00

4.2. ELIAS "JAMPPI"

Outro caso com grande repercussão foi do jogador Elias "Jamppi". O finlandês chegou a abandonar o cenário competitivo de CS:GO, após uma longa batalha com a Valve (BENVEGNÙ, 2020).

Ele recebeu o *VAC Ban* em 2015 e chegou a ingressar na justiça contra a desenvolvedora, numa tentativa de remover o banimento. O tribunal decidiu a favor da empresa, e Jamppi optou por fazer uma transição de carreira para o Valorant, da desenvolvedora *Riot Games*, que é outra modalidade de jogo FPS (*first-person shooter*), ou seja, jogo em que a visão do personagem é em primeira pessoa (é a mesma do jogador) (GLOBO ESPORTE, 2021).

4.3. BANIMENTOS NO CIRCUITO BRASILEIRO DE CS:GO

Recentemente, em abril de 2021, apenas alguns dias após o comunicado de mudança das regras de banimento, o Circuito Brasileiro de CS:GO ("CBCS") recebeu uma série de denúncias de contas banidas sobre seis jogadores que estavam inscritos e participando do torneio, o que ocasionou a saída voluntária de algumas das equipes desse campeonato, a fim de evitar maiores transtornos (GLOBO ESPORTE, 2021).

Houve bastante polêmica, principalmente quanto ao fato de um possível banimento das equipes e dos demais jogadores dos times cujo jogador que possui conta banida esteja vinculado.

A polêmica se deu, principalmente, pelo fato de que não é possível às equipes constatarem, no ato da contratação do atleta, se este possui ou não uma conta gravada com o VAC Ban, uma vez que somente através de denúncia de determinada conta é possível averiguar se existe alguma relação entre a mesma e o atleta acusado.

Assim, houve um questionamento em relação à eventual punição das equipes e dos demais jogadores, que também não possuem nenhuma ligação ao banimento da conta de parceiro de sua equipe.

O fato ocorrido no CBCS (Circuito Brasileiro de CS:GO) gerou bastante reper-cussão e forçou um posicionamento da Valve, que é conhecida por sua postura de tolerância zero para condutas trapaceiras e de pouca comunicação com a comunidade.

Um fato como esse gera prejuízo não apenas ao atleta, mas à organização como um todo, aos companheiros de equipe, ao campeonato e, inclusive, à própria desenvolvedora.

Enxergamos uma linha bastante tênue entre coibir condutas de trapaça e prejudicar o cenário de esportes eletrônicos, de forma até a favorecer a migração para outras modalidades de jogos, de outras desenvolvedoras.

Para entendermos melhor o caso, a edição de 2021 do CBCS faz parte do RMR (*Regional Major Rankings*), que é um sistema de pontos que define quais as equipes vão se classificar para o próximo Major de CS:GO, que ocorrerá no final deste ano, em Estocolmo (LIQUIPEDIA, sem data).

A competição, que faz parte do circuito oficial da Valve, teve início em 22 de abril de 2021, ou seja, a mudança nas regras, feita pela empresa, já havia sido anun-ciada.

Antes do primeiro dia do CBCS, após uma denúncia de VAC Ban em uma conta antiga do atleta Mateus “cidZzZ”, a equipe *Bears e-sports* anunciou que estaria se retirando do campeonato (GLOBO ESPORTE, 2021).

A notícia teve grande impacto no cenário, mas foi apenas a primeira, de uma série de denúncias que vieram a seguir. Apenas um dia após, em 24 de abril de 2021, a *Detona Gaming* tomou conhecimento de uma denúncia sobre uma conta com VAC Ban de um de seus atletas, Kaue "kauez", cujo banimento teria sido ocasionado pelo uso de *"skin changer"* (GLOBO ESPORTE, 2021).

O *cheat* do tipo *skin* changer realiza alterações meramente cosméticas nos itens internos do jogo, quais sejam, as cores aplicadas às armas escolhidas pelo usu-ário, de forma a alterar a aparência destes itens apenas para o próprio usuário. É importante sua distinção dos cheats considerados prejudiciais à competição, por aumentarem o desempenho do jogador, tais quais o *wall hack* e *aim bot*.

Apesar de não gerar aparente prejuízo à competição, tal *software* também configura trapaça, uma vez que uma das fontes de receita da Valve é a venda de *skins*, portanto seu uso causa prejuízos financeiros diretos à empresa.

Entendemos necessária a distinção dos softwares apenas para fins de distinguir os prejuízos e, assim, o grau de punibilidade e a proporcionalidade na aplicação da pena pelo seu uso.

Na mesma data do recebimento da denúncia, a *Detona Gaming* também optou por se retirar do campeonato (GLOBO ESPORTE, 2021).

A próxima equipe a se retirar do torneio foi a Vivo Keyd, que também recebeu denúncia de banimento de um de seus atletas, o Kayke "Kye". Mais uma vez a denúncia foi sobre uma conta antiga do jogador (GLOBO ESPORTE, 2021).

Apenas dois dias após o ocorrido, foi a vez da equipe Isurus receber informações sobre conta antiga com VAC Ban de seu jogador André "*drop*". Na ocasião, a equipe optou pela substituição do atleta por outro, Rodrigo "pino" (GLOBO ESPORTE, 2021).

Entretanto, pouco tempo após a substituição, a equipe tomou a decisão de se retirar do campeonato, assim como as demais (GLOBO ESPORTE, 2021).

Antes da quarta rodada da competição, foi a vez da equipe Jaguares comunicar sua saída do torneio para averiguar um caso de VAC Ban relacionado ao seu jogador Emerson "Desh" (GLOBO ESPORTE, 2021).

A equipe *Imperial E-sports*, embora não estivesse participando do CBCS, pois estava no México se preparando para o RMR norte-americano, também foi alvo de denúncias na mesma época. A denúncia recebida foi sobre uma conta com VAC Ban de seu jogador Guilherme "piriajr", e a equipe optou por substituir o mesmo pelo atleta Fernando "fer" (GLOBO ESPORTE, 2021).

A Valve se posicionou sobre apenas dois jogadores da lista acima, que con-seguiram provar que não eram os donos das contas banidas pelo VAC Ban. Entretanto, do ponto de vista jurídico, analisaremos a tomada de decisão da empresa, fazendo um comparativo com a legislação brasileira.

5. COMPARATIVO COM LEGISLAÇÃO BRASILEIRA

Após a abordagem dos conceitos introdutórios e exposição de alguns casos emblemáticos que demonstram a aplicação de VAC Ban a jogadores em que se de-tectou a utilização de softwares de trapaça, bem como os procedimentos trazidos pela Valve com relação a essa apuração, será realizado a seguir um comparativo com a legislação brasileira, de forma a dar uma compreensão mais ampla e permitir uma maior reflexão sobre o assunto.
No Brasil, quando uma pessoa comete um crime, ela é considerada inocente até que se prove o contrário. Trata-se do princípio constitucional da presunção de inocência, previsto no artigo V, LVII, da Constituição Federal (BRASIL, 1998):

> 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 proprie-dade, nos termos seguintes: LVII - ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória.

Ainda, o princípio in dubio pro reo, que também trata da presunção de inocência, prevê que, em caso de dúvidas, o réu/acusado será favorecido. No mesmo artigo 5ºda CF, temos em seu inciso XXXIX que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (BRASIL, 1998).

A partir dessas premissas, é viável presumir que para haver condenação e cumprimento de determinada pena, deve primeiro existir legislação que tipifique de-terminada conduta como ilícita, bem como a cominação legal da pena para tal conduta.

É preciso haver clareza e transparência quanto ao que é proibido e qual será a penalidade aplicada no caso de prática proibida. Porém, não é suficiente a mera imposição de uma penalidade.

Na dosimetria da pena, o juiz deve atender ao sistema trifásico estabelecido no artigo 58 do Código Penal, atendendo a três fases: fixação da pena base; análise das circunstâncias atenuantes e agravantes; análise das causas de diminuição e de aumento (BRASIL, 1940).

Assim, o magistrado deve atender à culpabilidade, aos antecedentes, à conduta social, à personalidade do agente, aos motivos, às circunstâncias e consequên-cias do crime, bem como ao comportamento da vítima, para só então estabelecer, conforme seja necessário e suficiente para reprovação e prevenção do crime, a pena-lidade. Tudo conforme prevê o artigo 59 do Código Penal (BRASIL, 1940).

Em seguida, após a fixação da pena base, serão consideradas as circunstâncias atenuantes e agravantes; por último, as causas de diminuição e de aumento da pena, consoante o artigo 68 do Código Penal (BRASIL, 1940).

Por isso também é importante que sejam levados em consideração sempre os princípios da proporcionalidade e razoabilidade, elementares no direito, muito embora sejam princípios não escritos, e sua observância independa de explicitação em texto constitucional, por pertencerem à natureza e essência do Estado de Direito.

Dessa forma, a dosimetria da pena serviria como critério utilizado apenas para orientação e uniformização das penalidades aplicadas.

Assim como o uso de *doping* que aumenta o desempenho físico do atleta durante as competições esportivas, não deve ser comparado a um crime hediondo contra a vida, se faz necessária a distinção e graduação nas penalidades impostas aos atletas de

esportes eletrônicos, de acordo com a conduta apresentada.

Analisando o *VAC Ban*, e considerando que até pouco tempo essa modalidade de banimento penalizava o usuário banindo-o por tempo indefinido, nota-se que tal punição vai em desencontro à Constituição Federal e à legislação penal vigente no Brasil.

Fazendo uma analogia, é possível chegar ao entendimento de que o uso de *softwares* não autorizados que aumentam o desempenho do atleta dentro do jogo, pode ser comparado ao uso de doping no esporte convencional, uma vez que ambos se tratam de práticas não autorizadas com a finalidade de aumentar o desempenho do atleta no desenvolvimento da atividade esportiva.

De acordo com o Código Mundial Antidoping, o indivíduo que violar as regras antidoping poderá ter a desqualificação de todos os seus resultados individuais obtidos no evento, com todas as consequências cabíveis, como confisco de medalhas, pontos e premiações (BRASIL, 2021).

Sua punição, entretanto, levará em consideração vários fatores, como por exemplo, a severidade da violação da regra. Antes de ser imposto um período de inelegibilidade, o atleta deverá ter a oportunidade de estabelecer as bases para eliminação ou redução dessa sanção.

Durante a Conferência Mundial sobre Doping nos Esportes, realizada em Lausanne em fevereiro de 1999, foi estabelecido, por consenso, inelegibilidade de dois anos para a primeira violação séria de regra antidoping, seguido do banimento perpé-tuo para uma segunda violação (AMBITO JURÍDICO, 2017).

Além desses fatores, quando o atleta estabelecer que o uso da substância não pretendia incrementar seu desempenho espor-

tivo, a punição passa a ser de advertência e repreensão para a primeira violação, dois anos de inelegibilidade para a segunda violação e inelegibilidade perpétua para uma terceira violação.

É possível observar no Código Mundial Antidoping que inúmeros fatores influenciam na aplicação das sanções. Desde o tipo de substância utilizada, até a recusa em fazer o teste, bem como a quantidade de vezes em que o atleta fez uso da subs-tância. Tudo vai influenciar na aplicação da pena.

Ainda dentro Código Mundial Antidoping, é importante destacar que, além dos fatores mencionados, a conduta da pessoa que fornece a substância para o atleta também pode ser punida.

Sobre as consequências para as equipes, se mais de um membro da equipe for pego cometendo violação de regra antidoping durante o mesmo evento, a equipe poderá estar sujeita à desqualificação ou outra ação disciplinar.

Ainda, o Código prevê a possibilidade de que as decisões sejam objeto de recurso, devendo respeitar alguns princípios como: audiência pontual; corpo de auditores justo, imparcial e independente; o direito do atleta ser representado por consultor; e uma decisão pontual, por escrito, e bem fundamentada.

Entretanto, a aplicabilidade de analogia ao doping requer a devida diferenciação quando se trata do uso de *softwares* da espécie *skin changer*, que modificam a parte estética do jogo, permitindo que o jogador visualize as *skins* (espécie de avatar, que modifica o design das armas, dentro do jogo) sem adquiri-las.

Isso porque, essa prática, com certeza causa prejuízo financeiro à desenvolvedora do jogo, uma vez que essa lucra com a atividade de venda das skins aos usu-ários do jogo. Entretanto, não há que

se falar em aumento do desempenho do jogador, posto se tratar de alteração meramente estética/cosmética.

Fazendo novamente uma analogia, tal prática se assemelha ao crime de pirataria, previsto no artigo 184 do Código Penal que dispõe que "violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa" (BRASIL, 1940). Assim, os banimentos dentro dos esports poderiam ter diferentes graus de classificação e punibilidade, de forma a adequar as sanções às condutas praticadas, de acordo com a espécie de software utilizado, a ocasião, a idade do agente, a quan-tidade de vezes em que praticou a conduta, a finalidade da prática, dentre outros fatores relevantes para a aplicação da pena.

Ainda, apesar de não ser uma prática no mercado, como verificamos nos casos trazidos, antes da aplicação de qualquer sanção, é importante garantir ao acusado o devido processo (legal ou administrativo), contraditório e ampla defesa, bem como o direito de recorrer da decisão condenatória.

6. CONCLUSÃO

Os *esports* vêm ganhando cada vez mais relevância no cenário nacional e internacional, e sua expansão demanda uma série de ajustes e regulamentações para que a comunidade cresça de forma saudável.

Existe o entendimento de que, uma vez que o usuário concorda com os termos de uso do jogo, não há que se falar na alegação de desconhecimento das regras ou penas mais brandas.

Por outro lado, há o entendimento de que muitos dos usuários começam a jogar quando ainda são crianças, por lazer, ocasião em que não cogitam a hipótese de jogar profissionalmente, e não

possuem maturidade ou discernimento para pensar nas consequências reais de um ato tido por brincadeira.

Considerando todo o estudo realizado neste artigo, desde as conceituações dos neologismos utilizados no segmento, passando pela punição propriamente dita, análise dos casos e analogia com a legislação brasileira e princípios de Direito, bem como o crescimento exponencial dos esportes eletrônicos no país e no mundo, sua conclusão permite o entendimento de que seria possível a existência de uma regulamentação mais detalhada e clara sobre as punições em eventuais casos de infração.

Para os banimentos, que são o maior grau de punição para o atleta de esportes eletrônicos, a cautela deve ser elevada a seu nível máximo, pois trata-se de uma punição severa e, muitas vezes, por tempo indeterminado, o que pode destruir uma carreira profissional.

Ainda, em se tratando de um cenário predominantemente adolescente, repleto de rivalidades e disputas de ego, comuns dessa fase, pode ser perigosa uma sanção tão severa sem a comprovação efetiva da conduta e autoria, uma vez que é perfeita-mente possível que uma conta seja forjada e atribuída ao atleta, ou até mesmo uma conta pertencente ao mesmo, mas indevidamente utilizada por terceiro.

Ademais, a graduação da pena não é sinônimo de penas mais brandas ou qualquer tipo de tolerância às condutas ilícitas, pelo contrário, o que se espera é que traga maior equidade e justiça às partes envolvidas.

REFERÊNCIAS BIBLIOGRÁFICAS

Acordo de Assinatura do Steam. Steam. Disponível em: https://store.steampowe-red.com/subscriber_agreement/?snr=1_44_44_#4. Acesso em: 06 jun. 2021.

Equipe Âmbito Jurídico. **A lei antidoping e os direitos fundamentais do atleta**. Âmbito Jurídico. 01/02/2017. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/a-lei-antidoping-e-os-direitos-fundamentais-do-atleta/amp/. Acesso em: 04 jun. 2021.

At Vave we make games, Steam, and Hardware. Valve. Disponível em: https://www.valvesoftware.com/pt-br/about. Acesso em: 14 jun. 2021.

BENVEGNÚ, Lucas. **Valve aponta que VAC Ban não impede Jamppi de seguir carreira profissional. Jogador da ENCE busca na justiça o revogamento do VAC Ban**. DRAFT5. 20/08/2020. Disponível em: https://draft5.gg/noticia/valve-aponta-que-vac-ban-nao-impede-jamppi-de-seguir-carreira-profissional. Acesso em: 04 mai. 2021.

BRASIL. **Constituição Da República Federativa Do Brasil De 1988**. Brasília, DF, 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constitui-cao/constituicao.htm. Acesso em: 15 jun. 2021.

CBCS Elite: Bears abandona disputa por VAC ban de cidZzZ. Equipe tomou conhe-cimento de uma conta antiga do jogador banida, o que proíbe a participação dele em campeonatos caso a ocorrência aconteceu há menos de cinco anos. Globo Esporte. 23 abr. 2021. Disponível em: https://ge.globo.com/esports/csgo/noticia/cbcs-elite-bears-abandona-disputa-por-vac-ban-de-cid-

zzz.ghtml. Acesso em: 04 jun. 2021.

CBCS Elite: DETONA abandona disputa por suposto VAC ban de kauez. Equipe é a segunda a deixar CBCS *Elite League Season 1;* adversários recebem vitória por W.O. Globo Esporte. 24 abr. 2021. Disponível em: https://ge.globo.com/es-ports/csgo/noticia/cbcs--elite-detona-abandona-disputa-por-suposto-vac-ban-de-kauez.ghtml. Acesso em: 05 jun. 2021.

CS:GO: kauez anuncia saída da DETONA por conta de VAC ban. Jogador teve a punição confirmada pela Valve e não poderá atuar em competições oficiais pelos próximos anos. Globo Esporte. 17 jun. 2021. Disponível em: https://ge.globo.com/esports/csgo/noticia/csgo-kauez-anuncia-saida-da-detona-por-conta-de-vac-ban.ghtml. Acesso em: 02 mai. 2021.

CBCS Elite: Isurus substitui jogador por suposto VAC ban. Organização troca André "drop" por analista Rodrigo "pino" até fim das investigações. Globo Esporte. 28 abr. 2021. Disponível em: https://ge.globo.com/esports/csgo/noticia/cbcs-elite-isurus--substitui-jogador-por-suposto-vac-ban.ghtml. Acesso em: 05 jun. 2021.

CBCS Elite: Isurus deixa torneio após confirmação de VAC Ban. André "drop" teve seu banimento confirmado pela FURIA, e a organização argentina optou por desistir do campeonato. Globo Esporte. 28 abr. 2021. Disponível em: https://ge.globo.com/esports/csgo/noticia/cbcs-elite-isurus-deixa-torneio-apos-confir-macao-de-vac-ban.ghtml. Acesso em: 03 jun. 2021.

CBCS Elite: Jaguares abandona campeonato após VAC ban. Organização é a quinta a abandonar a competição, que sofre com os casos de VAC bans em contas antigas de jogadores. Globo Esporte. 28 abr. 2021. Disponível em: https://ge.globo.com/

esports/csgo/noticia/cbcs-elite-jaguares-abandona-campeonato-apos-vac-ban.ghtml. Acesso em: 02 jun. 2021.

CBCS Elite: Vivo Keyd abandona após denúncia de VAC ban. Guerreiros se retiram da primeira etapa do Circuito Brasileiro de Counter-Strike por suposto banimento de conta antiga de Kye. É a terceira desistência dessa natureza em quatro dias. Globo Esporte. 26 abr. 2021. Disponível em: https://ge.globo.com/esports/csgo/noti-cia/cbcs-elite-vivo-keyd-abandona-apos-denuncia-de-vac-ban-kye.ghtml. Acesso e: 02 jun. 2021.

DLL. Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/DLL. Acesso em: 20 jun. 2021.

Código Mundial Antidopagem. Governo Do Brasil. Disponível em: https://www.gov.br/abcd/pt-br/composicao/regras-antidopagem-legislacao-1/codi-gos/copy_of_codigos/codigo-mundial-antidopagem-2021.pdf/view. Acesso em: 09 jun. 2021.

BRASIL. **Decreto-Lei 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Ja-neiro, 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/cci-vil_03/decreto-lei/del2848compilado.htm. Acesso em: 05 jun. 2021.

HOJAIJ, Matheus. **Banimento de "vsm" é retirado pela Valve e ele pode voltar a competir no mundo dos games: Com a atualização do termo de elegibilidade dos jo-gadores, aqueles que estavam banidos há cinco anos podem retornar às competi-ções**. BolaVIP. 15 abr. 2021. Disponível em: https://br.bolavip.com/noticias/Banimento-de-vsm-e-retirado-pela-Valve-e-ele-pode-voltar-a-competir-no-mundo-dos-ga-mes-20210415-0069.html. Acesso em: 03 mai. 2021.

KOVACS, Leandro. **Como funciona o *Valve Anti-Cheat [VAC System].* Pelo fim dos cheaters!** Saiba como funciona o Valve Anti-Cheat, programa oficial de caça os tra-paceiros no CS:GO. Tecnoblog. Disponível em: https://tecnoblog.net/351695/como-funciona-o-valve-anti-cheat-vac-system/. Acesso em: 02 jun. 2021.

KQLY. Liquipedia. Disponível em: https://liquipedia.net/counterstrike/KQLY. Acesso em: 13 jun. 2021.

O escândalo de VAC bans no CS:GO brasileiro. Globo Esporte. 30 abr. 2021. Dis-ponível em: https://globoesporte.globo.com/esports/stories/2021/04/30/o-escandalo-de-vac-bans-no-csgo-brasileiro.ghtml. Acesso em: 05 mai. 2021.

Regional Major Rankings 2021: Europe. *Liquipedia Counter-Strike.* Disponível em: https://liquipedia.net/counterstrike/Regional_Major_Rankings/2021/Europe. Acesso em: 04 jun. 2021.

Remover o banimento do VSM da Valve. ***Chance Org***. Disponível em: https://www.change.org/p/valve-remover-o-banimento-do-vsm. Acesso em: 02 jun. 2021.

Steam Support. I've been VAC banned. **Steam**. Disponível em: https://support.ste-ampowered.com/kb_article.php?ref=4044-qdhj-5691#reason. Acesso em: 12 jun. 2021.

VAC Ban no CS:GO: entenda o que é e relembre maiores casos. Cenário brasileiro passou por onda de denúncias, levando a três desistências do CBCS Elite. Globo Esporte. 28 abr. 2021. Disponível em: https://ge.globo.com/esports/csgo/noticia/vac-ban-no-csgo-entenda-o-que-e-e-relembre-maiores-casos.ghtml. Acesso em: 20 mai. 2021.

Valve. **Canaltech**. Disponível em: https://canaltech.com.br/empresa/valve/. Acesso em: 13 jun. 2021.

CONTRATOS DE E-SPORTS: CLÁUSULA "ANTI-CHEAT"

E-SPORTS CONTRACTS: "ANTI-CHEAT" CLAUSE

Camila Israel Rosa
Head of Legal - Detona Gaming. Pós-graduada em Direito Digital e Compliance pela Damásio IBMEC. Participante do Grupo de Estudos, Trabalho, Direito e Esports da Universidade Federal de Minas Gerais. Cursando especialização em Proteção de Dados Pessoais.
camila@camilarosa.adv.br

Mariane Siqueira Moreira
Advogada no Balconi Moreti-Advocacia da Inovação. Pós-graduada em Direito Tributário - IBET. LLM em Direito Empresarial - FGV. Mediadora judicial em formação (CEJUSC). Cursando Mediação e Arbitragem Avançadas – SFERA. Membro da Comissão de Inovação e Gestão da OAB/PR e Secretária da Comissão de Inovação e Gestão da OAB-Londrina.
marianesiqueira.balconimoreti@gmail.com

RESUMO:

Os *softwares* de trapaça, também conhecidos como *cheats* e o banimento de atletas por conta deste ato estão sendo pauta de diversas notícias no mundo dos esportes eletrônicos. Ocorre que a utilização destes *softwares* gera implicações em diversos atores do mercado, sendo estes, as desenvolvedoras, os jogadores, as organizadoras e equipes. Por este motivo faz-se necessário analisar o conceito de trapaça nos e-sports e como vêm sendo aplicadas as sanções de banimento referentes a verificação destes atos. Importante ressaltar que cada desenvolvedora tem termos próprios que regulamentam a apuração e punição referentes ao

cheat. No caso deste trabalho foi analisado apenas o sistema VAC *(Valve Anti-Cheat System)* que opera dentro da plataforma Steam do desenvolvedor. Assim, importante é a análise dos termos de Suporte Steam (da Valve), em especial as disposições sobre o banimento, tais como os motivos e o software utilizado pelo jogador e a possibilidade de apelação do banimento. Por isso, a pesquisa apresentou três cases e analisou quais as implicações que tiveram para os atores acima citados. Merece destaque às consequências com relação às organizações e empresas de e-sports e verificamos que a gestão e mitigação de riscos pode ser feita a partir de algumas condutas adotadas por estas, tais como políticas internas de compliance, implementação de manuais de conduta, bem como a inserção da aqui chamada clausula "anti--cheat" nos contratos com os jogadores.

Palavras-Chave: *E-Sports*. Banimento. *Cheat*. Cláusula *"Anti-Cheat"*.

ABSTRACT:
Cheating softwares, also known as cheats and the banning of athletes for this act is being the subject of several news in the world of electronic sports. It so happens that the use of these softwares generates implications for several market players, such as developers, players, organizers and teams. For this reason, it is necessary to analyze the concept of cheats in e-sports and how the banning sanctions regarding the verification of these acts have been applied. Importantly, each developer has its own terms that regulate the verification and punishment related to cheats.

In the case of this article, it will be analyzed only the VAC system (Valve Anti-Cheat System) that operates within the developer's Steam platform. Thus, it will be also addressed the review the Steam Support terms (from Valve), in particular the banning provisions, such as the reasons and software used by the player and the possibility of appealing the ban. Therefore, it is brought three cases and analyzed the implications they had for the actors mentioned above. Furthermore, it is highlighted the consequences in relation to e-sports organizations and companies and verified that the management and mitigation of risks can be done from some conducts adopted by them, such as internal compliance policies, implementation of conduct manuals, as well as the insertion of the here called "anti-cheat" clause in the contracts with the players.

Keywords: *E-Sports. Banishment. Cheat. "Anti-Cheat" Clause.*

1. INTRODUÇÃO

O *cheat*, ou seja, a trapaça é um tema fortemente debatido e divulgado atualmente no mercado de *e-sports* no contexto nacional e internacional. No segmento de esportes eletrônicos a trapaça é verificada por meio da utilização de *softwares*, estes desenvolvidos de forma específica para determinados jogos e buscando melhorar o desempenho e evolução dos jogadores dentro dos torneios.

Visualiza-se que este é um problema que vem sendo enfrentado mundialmente e que, com a evolução da tecnologia, vem surgindo diversos tipos de *softwares* de trapaça e suas repercussões são verificadas nas competições, nas políticas das organizações, desenvolvedoras e suas consequências afetam diversos atores. Por este motivo a importância do estudo proposto neste trabalho.

Desta forma, a proposta é estudar a utilização de cláusulas *anti-cheat* pelas organizações de *e-sports* como forma de mitigação de sua responsabilidade frente a utilização destes softwares pelos jogadores. Neste sentido, o primeiro capítulo tratará sobre o cenário atual deste mercado. Apesar dos esportes eletrônicos estarem crescendo constantemente e serem um mercado que está aportando muitos investimentos, são poucas pessoas que conhecem o cenário e suas peculiaridades. Isto se dá porque este mercado se desenvolveu fortemente nos últimos anos, ante o surgimento da internet e o desenvolvimento de novos games, fazendo com que a profissionalização do mercado seja completamente nova.

O segundo capítulo tratará sobre o conceito de *cheat* e os procedimentos de apuração. Para a melhor compreensão, realizaremos um paralelo com o *doping*, este conceito já muito discutido e

mencionado no mercado do esporte tradicional.

Este tópico, abordará as legislações especificas do *doping*, demonstrando regras, legislações e práticas de marcado já bem consolidadas. No entanto, com relação a trapaça nos esportes eletrônicos (*cheat*) teremos que evoluir muito socialmente para que em algum momento possamos ter uma maior previsibilidade das condutas, e sanções aplicáveis e práticas mercadológicas.

Importante ressaltar que com a crescente utilização e desenvolvimento de *softwares* de trapaça, os atores deste mercado tais como desenvolvedoras, organizadores de campeonatos e as próprias equipes tiveram que criar mecanismos que coibissem a utilização desses instrumentos.

Por este motivo, para coibir suas utilizações, as desenvolvedoras criaram sistemas (*softwares*) que pudessem detectar e verificar automaticamente se o computador do jogador está operando com algum cheat (*software* de trapaça) que seja identificado por meio de sua base de dados.

Existem diversos sistemas nesse sentido, contudo, para fins deste artigo analisaremos apenas o sistema VAC (*Valve Anti-Cheat System*) que opera dentro da plataforma Steam do desenvolvedor. Assim, faz-se necessária a análise dos termos de Suporte Steam (da Valve), em especial as disposições sobre o banimento, tais como os motivos e o *software* utilizado pelo jogador e a possibilidade de apelação do banimento.

O terceiro capítulo iniciará trazendo três cases de jogadores que tiveram suas contas banidas após ser detectado pelo sistema VAC que utilizaram softwares de trapaça, sendo estes, o Nikhil “forsaken”, o VSM e o Kauez. Todos os cases implicaram em banimentos, contudo, as condutas realizadas pelos jogadores tiveram

contextos e situações diferenciadas.

Ainda nesse capítulo, a partir dos *cases* expostos, far-se-á análises sobre as consequências da utilização de *softwares* de trapaça e seu eventual banimento para alguns atores do mercado de esportes eletrônicos, sendo estes os jogadores, a desenvolvedora e as organizações (equipes). Essa análise será importante para a verificação de que o banimento implica em diversas consequências diretas e indiretas, umas mais facilmente identificáveis que outras.

Por fim, o último capitulo abordará a mitigação de riscos por parte das organizações de equipes, mencionando todas as ações que podem ser implementadas, dando o foco a inserção de cláusulas *anti-cheat* nos contratos com seus jogadores.

Assim sendo, este trabalho abordará a problemática exposta onde podemos verificar que os efeitos da utilização de *softwares* de trapaça e suas consequências vão muito além do que imaginamos, em especial para as organizações equipes.

2. CENÁRIO ATUAL

O mercado de *e-sports* vem crescendo consideravelmente nos últimos anos. Com a transformação digital dos negócios e da sociedade surgiram novas formas de entretenimento e novos modelos de esportes, os chamados esportes eletrônicos (*e-sports*).

Assim como o mercado de esportes tradicional, os *e-sports* têm diversas regras, tanto com relação a operacionalidade dos jogos, quanto a conduta dos seus jogadores, que devem ser seguidas e respeitadas. Um dos grandes debates que está em alta na atualidade é a utilização de modalidades de trapaça pelos jogadores, os chamados *cheat*.

Isso porque a utilização de *hacks* e *cheats* (*softwares* para trapacear em campeonatos) são uma causa de banimentos dos atletas em campeonatos de *e-sports*, tendo repercussões atuais, em especial em torneios de *CS:GO* e *League of Legends-LoL*.

Alguns pontos que merecem ser analisados separadamente para compreendermos todo este contexto são as legislações e regulamentações dos campeonatos, as punições dadas aos atletas e as punições aplicadas as suas equipes.

Pelo fato deste mercado ser completamente novo, verificamos a ausência de normas que tratem de procedimentos para apuração e aplicação de sanções ao atleta e a equipe, o que torna temerária sua aplicabilidade, a depender do campeonato em que foi verificada a utilização do *cheat*.

Por este motivo torna-se cada vez mais relevante entender estas implicações e buscarmos construir normas, regulamentações e práticas de mercado que melhor se adequem e dialoguem com a realidade social.

3. CONCEITO DE CHEAT E PROCEDIMENTOS DE APURAÇÃO

Para melhor elucidar o entendimento sobre o que é o *cheat*, termo este tão mencionado ultimamente nas notícias referentes ao mundo dos *e-sports*, deve-se fazer um paralelo com o mercado dos esportes tradicional.

Primeiramente, faz-se necessário mencionar que *cheat* está relacionado a trapaça durante as competições. Devido à ausência de normas específicas e regulamentações padrões sobre trapaça durante os torneios de esportes eletrônicos, iniciaremos entendendo o conceito de trapaça nos esportes tradicionais, ou seja,

o *doping*.

3.1. PARALELO COM O DOPING

Ao analisar o conceito de doping, também não se verifica na doutrina e nas legislações uma unanimidade sua definição, contudo, entende-se majoritariamente que se antes ou durante as competições houver uma verificação do uso de substâncias que alterem a performance do atleta e essa substância conste na lista de substâncias dopantes, estaremos diante de um caso de *doping*.

Devido a prática dos esportes tradicionais ser muito antiga, já houve diversas situações que fizeram com que estas discussões fossem levadas à sociedade e, consequentemente, fosse inserida uma regulação no ordenamento jurídico e fizesse com que o mercado estabelecesse boas práticas. Por este motivo, quanto ao doping temos no Brasil legislações específicas que trazem as regulamentações.

Todas estas disposições estão presentes na Lei nº 13.322 (BRASIL, 2016) que alterou a Lei nº 9.615 (BRASIL, 1998), lei que instituiu as normas gerais sobre desporto, para acrescentar as normas referentes ao doping. Nesta legislação, verificamos que foi aprovado o Código Brasileiro Antidopagem – CBA e suas alterações (BRASIL, 2021), onde foram estabelecidas as regras antidopagem e suas sanções, os critérios para dosimetria destas sanções e o procedimento a ser seguido para processamento e julgamento das violações das regras antidopagem.

Analisando o Código Brasileiro Antidopagem, faz-se necessário fazer alguns apontamentos específicos para que, posteriormente, possamos realizar um paralelo com as regulamentações referentes aos *e-sports*.

Deve-se destacar que este código traz disposições específicas sobre as res-ponsabilidades do atleta, responsabilidades do pessoal de apoio do atleta, ações de prevenção à dopagem, estabelece as competências da Autoridade Brasileira de Controle de Dopagem (ABCD); traz disposições sobre a Justiça Desportiva Antidopagem (JAD), em especial sobre a estrutura e a jurisdição; dispõe sobre as violações às regras antidopagem e infrações conexas; dispõe sobre o procedimento de controle de dopagem, em especial sobre coleta e análise de amostras e gestão de resultados e traz disposições sobre o procedimento de julgamento de violação às regras antidopagem.

Assim, pode-se concluir que, quanto ao *doping,* os atletas e organizações têm uma previsibilidade quanto as substâncias proibidas, procedimento de apuração e sanções especificas, o que traz um respeito a direitos e garantias fundamentais, em especial os previstos no artigo 5º, incisos LIII e LV da Constituição Federal (BRASIL, 1998) que garantem o processamento e sentenciamento por uma autoridade competente, bem como o contraditório e ampla defesa no processo administrativo.

3.2. SOBRE O CHEAT

Feitas estas considerações, o próximo passo é a análise dos *e-sports*. Como já mencionado, por ser um mercado relativamente novo, não há legislações especificas que regulamentem a trapaça em competições e suas consequências. Neste mercado, por se tratar de esportes dentro do ambiente online, a forma de trapaça é por meio de *softwares* utilizados para obter a vitória de um campeonato, estes denomina-dos de *cheat* (palavra vinda da língua inglesa que significa enganação).

Na prática, os atletas utilizam *softwares* que dão esta vantagem competitiva, podendo também ser utilizados teclados ou mouses

que permitam a instalação de códigos.

Tal conduta é reprimida pela comunidade dos esportes eletrônicos justamente por ser considerada uma afronta ao espírito de respeito e competitividade que permeia estes campeonatos. Assim como em outros tipos de esportes, as trapaças sempre são vistas como condutas indesejadas.

Para coibir e verificar que estão sendo utilizados mecanismos ilegais como estes, foram desenvolvidos sistemas como o VAC (*Valve Anti-Cheat System*) que opera dentro da plataforma Steam do desenvolvedor. Este *software* tem por finalidade a verificação automática do computador que o jogador está utilizando, se há algum cheat identificável em sua base de dados. Importante frisar que este sistema VAC é apenas um dos *softwares* criados para detecção de trapaças criados pelas desenvolvedoras dos jogos.

Uma questão a ser destacada é que, na maioria dos casos, a verificação de cheat, ou seja, a apuração de um resultado positivo com a utilização destes *softwares*, gera uma punição. Na maioria dos casos a sanção aplicável é o banimento perma-nente e não negociável ao jogador, podendo também gerar repercussões para as organizações de *e-sports*.

Ocorre que ao contrário do mercado de esportes tradicionais, ante a ausência de regulamentações específicas, acabamos verificando punições realizadas de forma arbitrária nos *e-sports*, ou seja, sem a apuração por meio de um processo administra-tivo com respeito a todas as garantias e direitos fundamentais.

Tais punições imediatas acabam tendo diversas repercussões, sendo estas: o banimento do jogador que foi pego utilizando um *software* de trapaça (*cheat*), em alguns casos a perda de todos os itens e jogos que possui, pois é impossibilitado que este mova

seus bens para outra conta que possuir.

Contudo, o problema não são tão somente as punições, mas a ausência de normas claras quanto a sua aplicação. O primeiro ponto é que este mercado vem há muito tempo encontrando e expondo trapaceiros, porém não com regras claras. Isto porque, apesar de muitos editores de jogos escreverem um conjunto de regras, elas não são padronizadas quanto ao procedimento de apuração e a sanção. Outro ponto é que alguns jogos têm suas regras oficialmente ocultas ao público e seus processos de arbitragem são completamente sigilosos. Por fim, muitas das empresas não se manifestam detalhadamente sobre as peculiaridades que levaram algum jogador ao banimento.

A título exemplificativo, no suporte página da Steam, nas disposições sobre o banimento através do *software VAC*, há previsão especifica da ausência de informação quanto ao motivo e o programa ou *software* que causou o banimento do jogador e a apelação do banimento, vejamos:

> Você pode me dizer qual programa ou *software* causou meu banimento do VAC? Não. Nós não divulgamos os *cheats* que foram detectados enquanto conectado a um servidor protegido por VAC que resultou em um banimento do VAC. Temos registros detalhados para cada proibição VAC, no entanto, divulgar essas informações só beneficiaria os desenvolvedores de *cheats*. A equipe VAC regularmente investiga alegações de proibições falsas de VAC para aumentar a eficácia do *Valve Anti-Cheat*. Posso apelar do meu banimento do VAC? Não. As proibições de VAC não podem ser contestadas. Se um banimento VAC for emitido incorretamente, ele será automaticamente removido após investigação, mas o Suporte Steam não remove manualmente os banimentos VAC aplicados a contas por qualquer motivo (STEAM, 2021) (tradução nossa).[1]

1 No original: *Can you tell me what program or software caused my VAC ban? No. We do not disclose the cheats that were detected while connected to a VAC-secured server that resulted in a VAC ban. We have detailed records for*

Tais pontos só reforçam a ausência de contraditório e ampla defesa dentro deste processo de apuração de trapaças. Esta é uma questão que ainda deve ser palco para muitas discussões nesse cenário nos próximos anos.

Além disso, em um mercado que move milhões, o banimento do jogador interfere totalmente na organização do time para um campeonato, muitas vezes ensejando a saída da equipe e, por consequência, problemas com patrocinadores e com a credibilidade da organização e do jogador frente ao mercado.

4. CONSEQUÊNCIA DA TRAPAÇA - CASOS

Para entender as consequências da utilização do *cheat* deve-se analisar alguns cases de jogadores que foram pegos utilizando estes *softwares* e que tiveram diversas implicações, em especial, a suspensão ou o banimento imediato das competições.

Importante ressaltar que os três *cases* que serão analisados são de jogadores do CS-GO. Isto quer dizer que a análise foi feita a partir das consequências da trapaça, ou seja, da verificação de utilização do *cheat* apenas nesses torneios. Assim sendo, o recorte analisado foi apenas para a desenvolvedora destes jogos, podendo ter outros tipos de punições a depender do jogo analisado.

Outro ponto a ser verificado é que cada um dos *cases* aconteceu em um contexto diferente e ensejaram punições severas tanto

each VAC ban, however, releasing this information would only benefit cheat developers. The VAC team regularly investigates claims of false VAC bans to increase the effectiveness of Valve Anti-Cheat. Can I appeal my VAC ban? No. VAC bans cannot be appealed. If a VAC ban is issued incorrectly it will be automatically removed after investigation, but Steam Support does not manually remove VAC bans applied to accounts for any reason.

para o jogador quanto para a equipe.

4.1. COUNTER-STRIKE - NIKHIL "FORSAKEN"

O primeiro case que analisado é do jogo *Counter-Strike: Global Offensive (CS:GO)* em que o jogador Nikhil "*forsaken*" da OpTic India foi pego utilizando o *cheating* em seu usuário principal durante as etapas finais da Zowie eXTREMESLAND 2018 – Ásia (GUERRA, 2021).

Figura 1 – Jogador Nikhil"forsaken" no campeonato

Fonte: GLOBO ESPORTE, 24/04/2021 (oto de Yujen Chen).

Este caso foi importante para a análise das punições referentes a trapaça e foi verificada a utilização de *cheat* durante este evento presencial. Importante ressaltar que a punição neste caso foi aplicada ao time todo, onde a OpTic India (filial indiana da

OpTic Gaming, organização americana de esportes eletrônicos) com a imediata desclassificação do campeonato e a suspensão de investimentos.

Segundo notícias do Globo *E-sports*, o jogador também teve como punição o banimento do CS:GO profissional pelo prazo de cinco anos. Assim sendo, verifica-se que a utilização de *softwares* de trapaça, neste caso, gerou prejuízos, tanto ao jogador, quanto a sua equipe (GUERRA, 2021).

4.2. V$M – DETONA GAMING

Outro *case* importante trazido é o do jogador *V$M da Detona Gaming*. O jogador foi denunciado por um antigo VAC Ban e a Valve confirmou a suspeita, tirando o jogador dos campeonatos promovidos pela desenvolvedora por tempo indefinido (GLOBO ESPORTE, 14/04/2021).

Neste caso, o jogador, que antes integrava a equipe da *Detona Gaming*, havia sido punido quando criança pela *VAC Ban*. Sendo assim, o jogador, por ter recebido o *VAC Ban* (banimento dado pelo sistema *anti-cheat* da Valve) não podia disputar qualquer evento que tivesse o apoio dessa desenvolvedora.

Enquanto estava banido ele pode participar de outro campeonato *ESL Pro League* (da ESL – organizadora de outro campeonato), pois houve uma permissão de participação por desta organizadora (MARQUES, 2018).

Contudo, dos campeonatos organizados pela empresa Valve, o jogador estaria impedido de participar em virtude da punição aplicada. Por este motivo, a *Detona Gaming* (equipe que o jogador fazia parte) optou por não participar de torneios promovidos

pela referida desenvolvedora.

Esta opção de não participar dos campeonatos promovidos pela desenvolvedora foi realizada por conta de o jogador fazer parte da equipe, assim, apesar de poderem continuar participando, optaram por não colocar outro jogador no local.

Segundo relatos da advogada da *Detona Gaming*, Camila Israel Rosa, a equipe teve diversos prejuízos devido à punição, como por exemplo, o prejuízo reputacional da empresa que acabou ficando má vista frente ao mercado. Além disso, sofreu prejuízos na medida em que investiu tempo, dinheiro e *know how* no treinamento deste jogador que acabou perdendo valor de mercado frente a este banimento.

Enquanto estava banido, seus fãs e a comunidade do CS-GO criaram uma hashtag (*#freeVSM*) para que a desenvolvedora retirasse o banimento do jogador e este pudesse retornar aos campeonatos.

Neste ano de 2021, o jogador foi autorizado a voltar a integrar as competições de CS:GO. O caso foi importante porque ensejou uma alteração nos termos de elegibilidade da Valve para jogadores (GLOBO ESPORTE, 15/04/2021).

Nos termos antigos da Valve, qualquer punição a um jogador ensejava o banimento imediato, contudo, pelas novas regras, publicadas neste ano de 2021, a Valve em sua nota explica que os termos não haviam recebido atualizações desde que o jogo foi lançado e por este motivo um *VAC ban* só vai desqualificar um jogador de um evento se ele foi recebido a menos de cinco anos ou se aconteceu após a primeira participação do atleta em um campeonato da desenvolvedora (GLOBO ESPORTE, 28/04/2021).

Este *case* é importante porque até então a desenvolvedora não havia modificado nenhuma regra de seus termos, principalmente com relação ao banimento. Tal posição demonstra que as desenvolvedoras, em especial a Valve, estão se atentando aos movimentos do mercado (como por exemplo o #freeVSM) e como são as reações frente aos banimentos.

4.3. KAUEZ – DETONA GAMING

O terceiro case analisado é o do jogador Kauez, também pertencente à equipe da *Detona Gaming* na época. O jogador teve sua conta denunciada.

Após Vac ban, teve uma penalidade de banimento. Ressalte-se que o cheat (*software*) utilizado foi do tipo *skin changer*, que realiza alterações meramente cosméticas nos itens internos do jogo, quais sejam, as cores aplicadas às armas escolhidas pelo usuário, de forma a alterar a aparência destes itens apenas para o próprio usuário. Ocorre que normalmente estes itens customizados são vendidos pela desenvolvedora e estes *softwares* de trapaça permitem que os jogadores utilizem sem adquirir os produtos em sites oficiais (LIMA, 2018).

Figura 2: Utilização do cheat skin changer

Fonte: TECH TUDO (Foto: Reprodução Cheatz0ne/Counter-Strike: Global Offensive)

Importante frisar que na época do banimento de Kauez, ele estava participando do CBCS e a *Detona Gaming*, sua equipe, por medo de sofrer uma penalidade, optou por retirar-se na metade do campeonato (GLOBO ESPORTE, 24/04/2021).

4.4. CONSEQUÊNCIAS DA TRAPAÇA PARA OS DIFERENTES ATORES

Após a exposição destes três *cases*, pode-se verificar que as consequências da utilização de um cheat e o eventual banimento repercutem em diversos atores, tais como o jogador, a equipe e a própria desenvolvedora.

Primeiramente, realiza-se uma análise das repercussões de um banimento para o jogador. Observando os *cases* acima, os três jogadores (Nikhil “forsaken”, VSM e Kauez) ficaram impedidos de disputar torneios vinculados a desenvolvedora. Isto fez com que

estes jogadores acabassem perdendo valor de mercado.

Considerando que o valor de mercado desses jogadores é mensurado mediante a combinação de diversos dados, tais como salários atuais e futuros, duração do contrato e quantidade de transações semelhantes em várias regiões (RENNER, 2020), bem como seu desempenho dentro dos campeonatos e reputação, a partir do momento em que é verificada a utilização de um *cheat* e o banimento deste jogador, este valor de mercado é totalmente prejudicado.

Isto porque com o banimento este jogador fica impedido, no caso do *VAC ban*, de disputar torneios que tenham relação com a desenvolvedora, o que limita o campo de atuação deste jogador afetando diretamente no seu valor de mercado e sua carreira dentro do mercado de *e-sports*.

Importa mencionar novamente que no suporte página da Steam, por exemplo, nas disposições sobre o banimento do VAC, as disposições são claras no sentido de não disponibilizarem ao jogador informações a respeito do programa ou *software* que causou o banimento. Também não há possibilidade de apelação do banimento do VAC.

Tais informações foram trazidas apenas para deixar uma provocação acerca de custo benefício. Será que realmente vale a pena o jogador utilizar um *software* de trapaça (*cheat*)? Considerando todas essas repercussões vale a pena uma reflexão neste sentido.

Outros atores que sofrem consequências com o *cheat* e o banimento são as organizações ou equipes. Para entender este cenário se faz necessário um paralelo com os esportes tradicionais.

No futebol existem organizações provedoras, que criam especificamente jogadores de academia/base, ou mesmo equipes inteiras, e geram receita por meio de suas transferências (RENNER, 2020) e também existe a figura das equipes que competem nos torneios e ligas.

Ainda que a equipe não seja penalizada diretamente, ela sofrerá consequências indiretas. Deve-se compreender que o nome de um jogador está totalmente atrelado ao nome da equipe e, por este motivo, quando da verificação da utilização de um *cheat* e sua punição, não é apenas a reputação do jogador que está em jogo, mas essa conduta afeta diretamente a reputação da equipe que ele está inserido. Por este motivo uma das consequências verificadas pode ser a perda de patrocínios.

Outro ponto é que muitas equipes investem no desenvolvimento de habilidades dos jogadores, disponibilizando acompanhamento psicológico, equipe técnica e até mesmo *gaming houses*[2]. Todos estes investimentos são feitos para que o jogador melhore seu desempenho, seu valor de mercado e traga mais prêmios para a equipe. Por este motivo, a equipe tem prejuízos indiretos com o banimento de um jogador.

A título exemplificativo, vale analisar a Detona Gaming. No tópico anterior foram trazidos dois cases de jogadores pertencentes a sua base, o VSM e o Kauez. No primeiro deles, quando foi aplicado o *VAC Ban*, por um cheat usado quando o jogador era criança, a Detona Gaming optou por não participar de torneios promovidos pela desenvolvedora. No segundo, o jogador foi pego utilizando o *cheat* durante o campeonato e a equipe optou por abandona-lo.

2 As gaming houses são instalações que acomodam jogadores profissionais de esportes eletrônicos. Os *pro-players* utilizam essas casas (ou apartamentos) para treinar e morar.

Neste exemplo, pode-se perceber que uma equipe deixar de participar de um torneio próximo ou abandonar um em andamento gera prejuízos, pois, além do jogador penalizado, temos outros jogadores integrantes da equipe e o desempenho de um jogador afeta diretamente no sucesso da equipe dentro do torneio.

Por fim, importa trazer mais um ponto apenas para reflexão: será que este banimento reiterado, ou seja, o banimento de diversos jogadores, pode acabar desestimulando algumas equipes a participarem de determinados jogos ou migrarem para outros? Está aqui mais uma reflexão que deve começar a ser realizada para que futuramente tenhamos respostas e melhores práticas de mercado.

Uma reflexão sobre a rigidez das políticas de banimento das desenvolvedoras é válida já que percebemos pelos seus termos, em especial nas disposições sobre o banimento do VAC, que não disponibilizam ao jogador informações a respeito do programa ou *software* que causou o banimento. Também não há possibilidade de apelação do banimento do VAC.

5. CLÁUSULA "ANTI-CHEAT"

Após a análise de algumas consequências do banimento com relação a alguns atores do mercado de *e-sports*, dar-se-á ênfase as equipes. No tópico anterior foi verificado que as equipes sofrem diversas consequências e prejuízos indiretos com a utilização de *software* de trapaça por um de seus integrantes.

Primeiramente vale ressaltar que normalmente quando um jogador é contratado, em seu contrato é inserida uma cláusula indenizatória que representa uma multa que a equipe ganhará na transferência do jogador (ganha um valor pecuniário na venda deste jogador). Esta representa uma forma de receita das equi-

pes com relação ao jogador integrante. Contudo, conforme já foi mencionado, se este jogador é pego usando um cheat ele perde valor de mercado, não pode participar de campeonatos e perde premiações.

Por este motivo, algumas equipes começaram a buscar meios de se blindar de modo que consigam minimizar os efeitos negativos quando isto acontecer.

Já que não há um modo das equipes se prevenirem e identificarem a conta banida previamente, nem meios razoáveis de descobrir se o jogador utiliza *softwares* de trapaça (jogador costuma utilizar seus periféricos – mouse, teclado, fone de ouvido), um dos meios da empresa se proteger e reforçar sua política contra o uso destes meios é a inserção de cláusula *anti-cheat* em seus contratos (CBES, sem data).

A possibilidade de inserção dessa cláusula tem fundamento em um princípio clássico do direito contratual, o princípio da autonomia da vontade. Por este princípio, que se vincula à liberdade das partes, estas têm a liberdade de contratar ou de não contratar, a liberdade de escolher o parceiro contratual e a liberdade de determinar o conteúdo e a forma do contrato (KLOH, MACHADO, SEABRA, VIOLA, 2020).

Essa cláusula busca limitar a responsabilidade pelas organizações de *e-sports* frente a utilização de softwares de trapaça pelos jogadores integrantes de suas equipes. É importante que a redação desta cláusula seja clara e objetiva, de modo que as partes compreendam o que está sendo inserido. Está cláusula poderia ser construída sob os seguintes termos:

> O CONTRATADO se obriga a abster-se de portar ou utilizar qualquer sof-tware não autorizado, em especial, aqueles com a finalidade de melhorar o desempenho dentro do jogo ("*Cheat*"), e declara expres-

> samente que nunca utilizou nenhum *software* dessa categoria, responsabilizando-se por eventual prejuízo que venha a ser causado à CONTRATANTE em decorrência do seu uso, além de indenização por perdas e danos.

Pode-se verificar então, que a cláusula dispõe sobre a limitação de responsabilidade pela contratante (organização) frente a utilização de *software (cheat)* pelo jogador. Essa prática é necessária pois é extremamente difícil que a organização consiga averiguar se o jogador utilizou softwares de trapaça e, por este motivo, faz-se necessária sua expressa declaração a respeito disso.

Outro ponto é a previsão de indenização por perdas e danos frente aos prejuízos causados a organização. Isto faz com que a organização consiga mitigar os riscos trazidos pela informação falsa declarada pelo jogador de sua equipe.

Assim sendo, verificamos que está cláusula é construída observando disposições do nosso Código Civil, em especial os artigos 186, 187, 402, 927 (BRASIL, 2002) que dispõe sobre responsabilidade civil, obrigação de indenizar e perdas e danos.

Deve-se ressaltar que esses softwares de trapaça evoluem com o passar dos anos, contudo, apesar de todas as tentativas de se tornar imperceptível, pode ser identificado no cotidiano de treinamento da equipe. Esse ponto também reforça a importância da implementação de regras rígidas de compliance permitindo que, os coachs, responsáveis pela equipe, corpo técnico e até mesmo os companheiros de equipe possam verificar indícios de práticas de trapaça por membros da equipe.

Tal prática é utilizada no mercado, contudo a mera inserção de cláusulas *anti-cheat* nos contratos com os jogadores não é suficiente para acabar com este problema. Tem-se que adotar outras medidas para que a coibição seja reforçada, internalizada

e entendida.

Por isso, o posicionamento da empresa contrário a utilização de cheat é reforçado com a elaboração de políticas anti-trapaça, políticas internas de compliance, implementação de manuais de conduta, orientação frequente mediante workshops internos sobre os riscos e novas formas de cheating que estão presentes no mercado na modalidade de jogo que a equipe participa, métodos periódicos de avaliação dos perfis dos jogadores para identificação de indícios, investimentos em ferramentas eletrônicas nas gaming houses que dificultem a utilização destes softwares de trapaça, análise individual dos perfis dos pro players antes de competições, entre outras medidas que possam ser adotadas.

Todas essas regras e procedimentos são construídos para mitigar a utilização destes artifícios e aumentar a vigilância restrita sobre os perfis dos *pro-players* que a equipe mantém um contrato.

Esta mitigação de riscos e danos é importante pois, em eventual apuração de utilização de software de trapaça por um integrante da equipe, esta pode demonstrar que utilizou todos os meios possíveis para que essas práticas fossem reprimidas internamente. Tal conduta por parte da equipe mitiga, principalmente, os danos reputacionais.

6. CONCLUSÃO

Após todas as considerações trazidas neste trabalho, conclui-se que muitos dos danos e implicações trazidos pela utilização de *softwares* de trapaça no mercado de esportes eletrônicos são desconhecidos por grande parte da sociedade e, por este motivo, faz-se necessário refletir e analisar quais são as práticas e condutas que melhor se adequam para reprimir tais danos.

Este mercado vem crescendo consideravelmente e com a evolução tecnológica da sociedade vem surgindo diversos outros games e, consequentemente, são desenvolvidos *softwares* de trapaça para burlar regras e melhorar o desempenho dos jogadores, entretanto, para que essa prática seja cada vez mais reprimida no mercado, todos os atores devem implementar soluções que as coíbam.

Quando a observação é feita sob a ótica das organizações e equipes percebe-se serem necessárias a tomada de algumas medidas especificas para que sejam eximidas de responsabilidades e mitiguem os danos referentes ao uso de cheats por seus jogadores.

Tais medidas podem ser materializadas na criação de políticas anti-trapaça, políticas internas de compliance, implementação de manuais de conduta, bem como a inserção da aqui chamada clausula *"anti-cheat"* nos contratos com os jogadores.

Verifica-se ao longo deste trabalho que a inserção dessa cláusula é extremamente importante, pois, com ela, o jogador declara expressamente que não utilizou *softwares* de trapaça e que em caso de descumprimento, ou seja, no caso deste jogador ter passado uma informação falsa, este deverá indenizar a equipe por perdas e danos.

Este ponto é extremamente relevante pois, conforme mencionado, a equipe investe muito no desenvolvimento do jogador, seja com apoio técnico, *gaming houses*, horas de treinamento, etc. Com a inserção desta cláusula os prejuízos financeiros podem ser mitigados quando da verificação de *cheat* e eventual banimento.

Quanto aos prejuízos reputacionais, estes podem ser mitigados com a aplicação dos outros mecanismos citados, como compliance, treinamentos e explicações aos atletas sobre os cheats que estão no mercado, redação e explicação e manuais e políticas da organização. Isto se dá porque com eventual escândalo a equipe pode provar que tomou todas as medidas que estiveram em seu alcance.

Desta forma, todo esse arcabouço de soluções, ou seja, a cláusula *anti-cheat* cumulada com as outras medidas expostas, faz com que a organização tenha uma melhor gestão de riscos frente a utilização de *softwares* de trapaça e consequente banimento de seus atletas.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Código Brasileiro Antidopagem 2021**. Disponível em: https://www.gov.br/abcd/pt-br/composicao/regras-antidopagem--legislacao-1/codi-gos/copy_of_codigos/codigo-brasileiro-anti-dopagem-aprovado-cne.pdf. Acesso em: 15 jun. 2021.

BRASIL. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988**. Brasília, DF, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/cci-vil_03/constituicao/constituicao.htm. Acesso em: 15 jun. 2021.

BRASIL. **Lei 9.615, de 24 de março de 1998**. Institui normas gerais sobre des-porto e dá outras providências. Brasília, DF, 24 de março de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9615consol.htm. Acesso em: 15 jun. 2021.

BRASIL. **Lei 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF, 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/cci-vil_03/leis/2002/l10406compilada.htm. Acesso em: 2 jun. 2021.

BRASIL. **Lei 13.322, de 28 de julho de 2016**. Altera as Leis n. 9.615, de 24 de março de 1998, que institui normas gerais sobre des-porto, para dispor sobre o controle de dopagem, 12.780, de 9 de janeiro de 2013, que dispõe sobre medidas tributárias referentes à realização, no Brasil, dos Jogos Olímpicos de 2016 e dos Jogos Paralímpicos de 2016, 10.973, de 2 de dezembro de 2004, e 8.010, de 29 de março de 1990; e dá outras providências. Brasília, DF, 28 de julho de 2016. Disponível em: http://www.planalto.gov.br/cci-vil_03/_ato2015-2018/2016/lei/L13322.htm. Acesso em: 15 jun. 2021.

CBCS Elite: DETONA abandona disputa por suposto *VAC ban* de kauez. Equipe é a segunda a deixar CBCS Elite League Season 1;

adversários recebem vitória por W.O. Globo Esporte. 24/04/2021. Disponível em: https://ge.globo.com/es-ports/csgo/noticia/cbcs--elite-detona-abandona-disputa-por-suposto-vac-ban-de-kauez.ghtml. Acesso em: 02 jun. 2021.

Eu fui banido do VAC. Suporte STEAM. 24/04/2021 . Disponível em: https://sup-port.steampowered.com/kb_article.php?ref=4044-q-dhj-5691#reason. Acesso em: 20 jun. 2021.

***Free vsm*: Valve retira *ban* e jogador pode voltar a torneios: Empresa atualizou os termos de elegibilidade para jogadores e passou a permitir que atletas banidos há mais de cinco anos, como é o caso do jogador, atuem em campeonatos oficiais**. Globo Esporte. 15/04/2021. Disponível em: https://ge.globo.com/esports/csgo/noti-cia/freevsm-vsm-e-desbanido-e-pode-jogar--campeonatos-da-valve.ghtml. Acesso em: 14 jun. 2021.

GUERRA, Felipe. **Aimbot no CS:GO: o que é o *hack*, riscos e punições do *cheat*: Trapaça facilita a vida dos usuários, que conseguem abater os oponentes sem qualquer esforço**. Globo Esporte. 24/04/2021. Disponível em: https://ge.globo.com/es-ports/csgo/noticia/aimbot-no-csgo-o-que-e-o-hack-riscos-e-punicoes-do--cheat.ghtml. Acesso em: 20 jun. 2021.

KLOH, Gustavo; MACHADO, André Roberto; SEABRA, André; VIOLA, Rafael. **Fundamentos do Direito Contratual**. Apostila FGV Direito Rio LLM em Direito Civil e Processual Civil. Rio de Janeiro: Editora FGV, 2020.

LIMA, Luiz Felipe. ***Skin changer* dá *ban* no CS:GO; entenda punição do *VAC*: *Skin changer* também é muito comum em jogos como LoL e Fortnite**. TECH TUDO. 21/09/2018. Disponível em: https://www.techtudo.com.br/noticias/2018/09/skin-chan-ger-da-ban--no-csgo-entenda-punicao-do-vac-esports.ghtml. Acesso em: 06

jun. 2021.

MARQUES, Roque. **Valve aplica banimento em v$m; ESL isenta jogador**. ESPN. 05/11/2018. Disponível em: https://www.espn.com.br/esports/ar-tigo/_/id/4948323/valve-aplica-banimento-em-vm--esl-isenta-jogador. Acesso em: 22 mai. 2021.

O caso de *cheat "forsaken"* e a necessidade de estrutura de compliance *cheating* nos *eSports*. CBES. Disponível em: http://cbesports.com.br/artigos/o-caso-de-cheat-forsaken-e-a-necessidade-de-estrutura-de-compliance-cheating-nos-esports/. Acesso em: 02 jun. 2021.

RENNER, Vinicius. **Como o mercado de transferências de jogadores de Esports se difere dos esportes tradicionais?** B2Game. 07/01/2020. Disponível em: https://b2game.com.br/jogadores-de--esports/. Acesso em: 02 jun. 2021.

Steam Support. ***I've been VAC banned***. STEAM. Disponível em: https://support.ste-ampowered.com/kb_article.php?ref=4044-qdhj-5691#reason. Acesso em: 12 jun. 2021.

***VAC Ban* no CS:GO: entenda o que é e relembre maiores casos: Cenário brasileiro passou por onda de denúncias, levando a três desistências do CBCS Elite**. Globo Esporte. 28/04/2021. Disponível em: https://ge.globo.com/esports/csgo/noticia/vac-ban-no-csgo--entenda-o-que-e-e-relembre-maiores-casos.ghtml. Acesso em: 20 jun. 2021.

DIREITOS DO TITULAR NA LGPD: REFLEXÕES SOBRE OS DIREITOS DE ACESSO E PORTABILIDADE E A SUA RELAÇÃO COM O OPEN BANKING

DATA SUBJECT'S RIGHTS IN THE BRAZILIAN DATA PROTECTION ACT: REFLECTIONS ON ACCESS AND PORTABILITY RIGHTS AND THEIR RELATIONSHIP WITH OPEN BANKING

Carlos de Paula Soares Filho
Advogado, Mestrando em Gestão da Informação pela Universidade Federal do Paraná Especialista em Direito Civil e Processo Civil pela Estácio de Sá Cursando pós-graduação em Direito Contemporâneo pela FESP-PR Graduado pela UNIOPET
soaresfilho@ufpr.br

Dafini Boldrini
Advogada, pós-graduada em Compliance e Governança Jurídica pela FAE *Business School*, Especialista em LGPD pela NextLaw Academy, membro do Instituto Nacional de Proteção de Dados Graduada pela Unicuritiba
daniboldrini@gmail.com

Giovanni Vernillo
Advogado, Pós-Graduando em Advocacia Empresarial pela EBRADI Graduado pela Universidade Positivo
g.vernillo@outlook.com

Julio Herman Faria
Advogado, MBA em grau de especialização em Direito Bancário pela FGV/SP Especialista em Direito Administrativo pelo Instituto de Direito Romeu Felipe Bacellar Pós-graduado em Direito Digital e Compliance pelo Instituto Damásio - IBMEC SP
Graduado em Direito pela PUC PR
aju61325@terra.com.br

RESUMO:
O presente artigo tem por objetivo levantar, de forma breve, o debate sobre cada um dos temas sugeridos - direito do titular ao acesso de seus dados pessoais, portabilidade e sua relação com o *open banking* - por meio de breves introduções sobre cada um dos temas e conceituação a partir de perspectivas mais sólidas sobre a Proteção de Dados ao redor do mundo. Sobre cada um dos temas é possível extrair problemáticas identificadas no bojo do cenário brasileiro especialmente no que tange à aplicação LGPD no ano de 2021 e suas futuras aplicações, bem como adentrar os conceitos básicos sobre cada tópico, abrindo-se, ainda, espaço para ao debate a respeito dos temas e possíveis soluções para os problemas identificados. O estudo se desenvolveu a partir de pesquisa bibliográfica doutrinária e legislativa nos âmbitos nacional e internacional, bem como por direito comparado.

Palavras Chaves: Direitos do Titular dos Dados. Acesso aos Dados. Portabilidade. *Open Banking*.

Portabilidade; 3.2. O Processo De Transferência Dos Dados; 3.3 Responsabilidades De Controladores Advindas Com A Portabilidade; 4. *Open Banking*: Aspectos Gerais E Conceitos; 4.1 Do Consentimento Explícito Do Consumidor; 4.2. Diferenças Entre Portabilidade De Dados E *Open Banking*; 4.3. Implementação Do Sistema *Open Banking*; 5. Considerações Finais; Referências Bibliográficas.

ABSTRACT:
This article has the goal of briefly introducing the debate about each one of the suggested themes (the data subject rights to access their personal data, portability and relation to open banking) trough brief introductions about each of the themes and the conceptualization from more solidified perspectives about Data Protection from all around the world, utilizing doctrinal and legislative bibliography research, nationally and worldwide, and the comparative law methodology. About each of the themes, it is also possible to extract problematics identified in the brazilian GDPL in the year of 2021 and its anticipated application.

Keywords: *Data Subject Rights. Access to Personal Data. Portability. Open Banking.*

Summary: *1. Introduction; 2. Data Subjects Right To Access Their Personal Data; 2.1. Brief Considerations; 2.2. Dialogues Between Legal Sources; 2.3. The Right To Access As A Guarantee Of The Other Forecast Rights On The Gdpl; 2.4. Field Research About The Data Subject Right To Access Personal Data; 3. Right Of Portability And Its Application On Europe And Brazil; 3.1. Conceptualization Of The Right Of Portability; 3.2. The Process Of Data Transference; 3.3. Responsibilities Of The Controllers Resulting From The Portability; 4. Open Banking: General Aspects And Concepts; 4.1. The Explicit Consentiment From The Data Subject; 4.2. Differences Between Data Portability And Open Banking; 4.3. Implementation Of An Open Banking System; 5. Final Considerations; References.*

1. INTRODUÇÃO

Três anos após a aprovação da Lei Geral de Proteção de Dados - LGPD - o cenário que circunda a proteção de dados no país ainda segue rodeado de incertezas, tanto nos aspectos práticos da aplicação da lei, quanto no sentido do debate e conceituação de termos e direitos ainda em discussão no ambiente de proteção, cujas definições se demonstram cada vez mais imprescindíveis para o estabelecimento de um ambiente juridicamente seguro para o controlador, o operador e, principalmente, para o titular de dados.

Torna-se possível comprovar este quadro de incertezas diante dos atrasos nas agendas estabelecidas pela Autoridade Nacional de Proteção de Dados - ANPD - bem como, por exemplo, pela análise de que, somente em julho de 2021, através da Portaria nº 16, a autoridade estabeleceu oficialmente os procedimentos para a elaboração da agenda regulatória e de atos normativos por ela editados.

Neste cenário, a prática e o debate têm se revelado mais do que relevantes, absolutamente necessários onde, precedendo as primeiras sanções oficiais, conceitos teóricos e práticos ainda se revelam carentes do debate e até mesmo de definições iniciais satisfatórias à análise necessária. Neste sentido, este trabalho possui por objetivo o debate de temas ainda sensíveis no campo de estudo dos Direitos do Titular, identificados pela análise dos pesquisadores como temas ainda pouco explorados e/ou cujo impacto do estudo e análise se revelam como fundamentais à academia de forma urgente, especialmente na fase inicial de aplicação da lei e de suas sanções, bem como das devidas e necessárias regulações por parte das autoridades competentes, com a perspectiva de que o debate contribua com a elucidação dos temas e conceitos propostos.

2. DIREITO DO TITULAR AO ACESSO DE SEUS DADOS PESSOAIS

2.1. BREVES CONSIDERAÇÕES

A Lei Geral de Proteção de Dados – LGPD - tem como um de seus objetivos a proteção do direito fundamental de privacidade. Direito esse que teve como marco jurídico inicial o artigo *"The Right To Privacy"*, de Samuel Warren e Louis Brandeis, publicado na *Harvard Law Review* em 1890 (WARREN; BRANDEIS, 2021, p. 193-220). Os autores trataram a privacidade como uma liberdade individual negativa do indivíduo de ser deixado a sós, em paz. Os avanços sociais e tecnológicos[1] resultaram na necessidade de garantir ao indivíduo uma liberdade positiva de autodeterminação informativa, na qual o titular detém o controle sobre a divulgação e utilização de seus dados pessoais. De acordo com Stefano Rodotá o bem jurídico tutelado na privacidade gira em torno da informação e do sigilo, enquanto no direito à proteção de dados abarca a informação, circulação e o respectivo controle (RODOTÁ, 2009, p. 287-290). Para exercer mencionado controle é necessária a criação de mecanismos que permitam ao titular o conhecimento sobre as atividades de tratamento envolvendo seus dados pessoais. Mecanismos esses efetivados através dos direitos do titular de dados, que envolvem sua participação nas decisões sobre o conteúdo, registro, divulgação e utilização de suas informações.

Uma das formas de fazer valer essa participação é através do acesso, princípio (art. 6, IV, da LGPD) e direito (art. 18, II, da LGPD) que garante aos titulares uma "consulta facilitada e gratuita sobre

1 Aqui cabe lembrar a definição do filósofo Norberto Bobbio de que os direitos são produtos históricos, nascem de necessidades e dos interesses em jogo, da alteração das classes no poder, bem como das transformações técnicas, sociais e econômicas (BOBBIO,1992, p. 15.).

a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais".

A edição da LGPD foi inspirada pelo Regulamento Geral de Proteção de Dados da União Europeia (RGPD-UE), e a natureza do direito ao acesso é a mesma na legislação brasileira e europeia, ambas dispõem que ele é efetivado quando são criados meios do indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de que forma ela é utilizada.

Segundo a Convenção nº 108 do Conselho Europeu, de 1981, o livre acesso é salvaguarda do titular de dados. No capítulo 2, art. 8º, está previsto que qualquer indivíduo tem o direito de: a) ter conhecimento da existência do banco de dados e seu objetivo; b) obter em intervalo de tempo razoável e sem despesas confirmação sobre quais dados estão armazenados; c) obter a retificação de informações incorretas e exclusão daquelas obsoletas ou tratadas em desconformidade com a Lei. A questão foi ratificada depois na Diretiva 95/46 e no RGPD-UE. No Brasil, em que pese a LGPD estar em vigor apenas desde 2020, a problemática acerca da falta de conhecimento pelo titular já era tema de decisões judiciais no Brasil em 1995, na decisão do Ministro Ruy Rosado de Aguiar:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de

> delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. (STJ. Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119)

Percebe-se que apesar de só recentemente a matéria ter ganho força legal específica, a proteção de dados já era uma preocupação, bem como o direito ao acesso já estava regulamentado por outras fontes, como na Constituição Federal e no Código de Defesa do Consumidor.

2.2. DIÁLOGO ENTRE AS FONTES JURÍDICAS

A Constituição Federal de 1988 foi pioneira mundial ao contemplar o *Habeas Data*, posteriormente regulamentado pela Lei 9507/1997, que se trata do instituto que permite ao cidadão acessar e retificar seus dados que estejam em posse de órgãos governamentais e de caráter público. Entretanto, essa ação que precisa ser interposta por advogado não cumpre com o requisito de acesso facilitado previsto na LGPD.

Já o CDC possui uma seção específica para os Bancos de Dados e Cadastros dos Consumidores, determinando o acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Ainda, estabelece pena de detenção de seis meses a um ano ou multa para quem "impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros" (BRASIL, Lei 8.078, 1990, art. 72).Além do Habeas Data e do CDC, o Código Civil, o Marco Civil da Internet, a Lei do Cadastro Positivo, a Lei de Acesso

à Informação e outras leis são exemplos de que a pauta da proteção de dados já estava em discussão antes da edição da LGPD. Apesar da relevância dos mencionados diplomas, era extremamente necessária a edição de uma norma própria para garantir o acesso facilitado e igualar o Brasil aos países mais desenvolvidos no que diz respeito à proteção de dados, pauta constante na Organização para Cooperação e Desenvolvimento Econômico (OCDE).

2.3. O DIREITO AO ACESSO COMO GARANTIDOR DOS DEMAIS DIREITOS PREVISTOS NA LGPD

Os direitos dos titulares de dados são posições jurídicas individuais que servem para que as exigências jurídicas de proteção de dados sejam implementadas e o titular mantenha o controle sobre os dados e as decisões neles baseadas (DOHMANN, 2021, p. 109). O capítulo III da LGPD é dedicado aos direitos do titular e deve servir como norteador para os agentes de tratamento no momento da implementação de políticas de proteção de dados, que devem sempre garantir os direitos daquele que está no centro do palco, o titular.

O art. 18, da LGPD determina que os direitos poderão ser exercidos a qualquer momento mediante requisição e traz em seus nove incisos um rol exemplificativo dos direitos do titular. Compreende-se que o rol não seja taxativo, pois como mencionam Bruno Gressler Wontroba e Paola Gabriel Ábila sempre que o exercício de um direito, ainda que não previsto expressamente na LGPD, "for necessário para proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, ele deve ser reconhecido e juridicamente amparado" (ÁBILA; WONTROBA, 2021). Percebe-se que o direito ao acesso é requisito para a efetivação dos demais, uma vez que sem ter acesso não é possível realizar a correção, anoni-

mização, exclusão e portabilidade, por exemplo. Por ser garantidor dos demais direitos, no decorrer da LGPD, o direito ao acesso é mais regulamentado. No art. 19, restou definida a forma como o acesso deve ser providenciado, são duas as opções que o controlador possui: i. formulário simplificado, imediatamente; ou ii. declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

Há ainda, a determinação ao controlador de que os dados pessoais sejam armazenados de forma a favorecer o exercício do direito ao acesso e que o mesmo deverá ser gratuito (§1º).

2.4. PESQUISA DE CAMPO SOBRE O EXERCÍCIO DO DIREITO AO ACESSO

Em uma breve pesquisa de campo, buscou-se entender como os controladores estão reagindo aos pedidos de acesso dos titulares de dados e quais são as principais lacunas desse exercício.

A primeira conclusão é em relação ao prazo de quinze dias, previsto no art. 19, II, da LGPD. Não há previsão sobre a contagem em dias úteis ou corridos, bem como sobre suspensão quando solicitado ao titular verificação sobre sua identidade. Verificou-se que nos casos em que não foram enviados documentos para comprovação de identidade do solicitante, não houve retorno dos controladores dentro do prazo legal.

A verificação de identidade é a segunda problemática encontrada no que tange o exercício do acesso aos dados. Os resultados mais efetivos aconteceram nos casos em que o controlador já disponibilizava ao usuário aplicativo ou área do usuário para ações rela-

tivas à sua atividade. Nesses casos, em que existe login mediante usuário e senha, há autenticidade e apenas foi criada uma área específica para requisições do titular de dados pessoais.

Entretanto, nem todos os controladores possuem meios tecnológicos como esses e utilizam meios menos seguros, como solicitações por e-mail diretamente ao encarregado em que a verificação aconteceu mediante confirmação dos dados ou até mesmo mediante formulário de solicitação e envio de documentos comprobatórios.

As instituições financeiras, em razão da regulamentação setorial, fazem parte do setor com maior facilidade em atender aos pedidos de acesso. Entretanto, mesmo nesses casos, não houve parâmetros sobre o conteúdo dos relatórios. Enquanto algumas enviaram relatórios completos com definição de bases legais e finalidades, outras se limitaram a informar quais dados são tratados, de forma genérica.

Conclui-se que apesar do previsto no art. 19, da LGPD, há necessidade de regulamentação sobre o procedimento de acesso aos dados pessoais. Na agenda da Autoridade Nacional de Proteção de Dados, ANPD, está prevista para o primeiro semestre de 2022 a regulamentação do tema: Direitos dos titulares de dados pessoais.

3. DIREITO DE PORTABILIDADE E A APLICAÇÃO NA EUROPA E NO BRASIL

3.1. CONCEITUAÇÃO DO DIREITO DE PORTABILIDADE

Sendo titular de dados pessoais, um consumidor pode desejar aproveitar-se dos direitos de portabilidade que a lei lhe confere e, assim, tanto para a facilitação do processo de compra como para melhorar a sua experiência notadamente no novo universo online das relações de consumo. O detentor dos dados pessoais, ou seja, o controlador, deve atender às solicitações do titular na forma da lei. Porém o exercício desse direito ainda carece de regulamentação e reveste-se de preocupações adicionais conforme se verá.

3.1.1. NATUREZA, CONCEITO E BENEFÍCIOS

O direito à portabilidade de dados está assegurado no Artigo 20 da GDPR e, em nossa Lei Geral de Proteção de Dados (LGPD), surge no Artigo 18, inciso V, com a seguinte redação: "portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial" (BRASIL, LEI 13.709, 2018). No sentido da legislação, a portabilidade é o ato de obter, após expressa solicitação do titular a um controlador, o fornecimento dos respectivos dados pessoais com a intenção de transferi-los, ou seja, reutilizá-los, em um novo controlador (ou controlador recebedor).

A portabilidade é, em essência, um instituto de natureza especial, pois se verifica a intersecção entre o regime jurídico da proteção de dados, direito concorrencial e a defesa do consumidor. Possui uma natureza e uma finalidade (BERGENSTEIN, 2020, p. 2). Para Laís Bergstein:

> O direito à portabilidade dos dados pessoais, entendido como o direito do titular dos dados a transmitir ou receber dados pessoais que lhe digam respeito, tem uma dupla dimensão: primeiro, assegura ao titular dos dados pessoais a possibilidade de obter uma cópia dos seus dados em um formato adequado (acessar); segundo, obriga o titular à entrega dessas informações a outro fornecedor de produtos ou serviços, observados os segredos comercial e industrial (transmitir). (BERGSTEIN, 2019, p. 11).

Desse modo, o direito à portabilidade permite o exercício do direito à autodeterminação informacional, buscando a promoção da concorrência em mercados dominados por monopólios, assim como reduz ou previne o risco de aprisionamento (*lock-in*) do titular dos dados, enquanto consumidor, a um fornecedor (controlador) (BERGENSTEIN, 2020, p. 3) . Para além da questão acerca do *lock-in*, o *European Data Protection Bureau* (EDPB) entende que a portabilidade tem o condão de impulsionar novas oportunidades de inovação no mundo digital, através do compartilhamento seguro e confiável dos dados, por expressa solicitação dos titulares, e com o controle do processo pelos mesmos titulares. Com isso, espera-se novos serviços e melhor experiência dos usuários (WP 29, 2017, p. 5).Chris Skinner afirma que, apesar de um cenário de incertezas e receios quanto a abertura e compartilhamento de dados, no contexto do setor financeiro, o uso compartilhado de dados, por meio das APIs, podem representar uma espécie de ganha-ganha tanto para os incumbentes financeiros, como para os seus concorrentes diretos, as *Fintechs* (SKINNER, 2020, p. 113). Neste arranjo, quem sai beneficiado é o consumidor de produtos financeiros, principalmente a partir do *Open Banking*.

3.1.2. ESCOPO DOS DADOS PESSOAIS PORTÁVEIS

A nossa LGPD, conforme a redação dada ao inciso V, do artigo 18, conjugada com o próprio *caput* do artigo 18 é mais abrangente quanto ao escopo dos dados pessoais sujeitos à portabilidade. De fato, o artigo 18 assegura o exercício de direitos pelo titular diante do controlador inerentes aos dados pessoais "por ele tratados". Além disso, o inciso remete à regulamentação pela ANPD das questões relativas à portabilidade. Comparativamente à GDPR, o nosso regulamento é mais amplo, ao passo que na Europa seria mais restrito (WP29, 2017, p. 5).Entretanto, em ambas as legislações existe a ressalva de proteção de segredos comerciais ou industriais, informações protegidas por legislações específicas, além, por óbvio, de dados pessoais concernentes a terceiros e as que possam afetar os direitos e liberdades individuais (GDPR, art. 20 (4)). Tais aspectos atraem o dever de cuidado dos controladores no processamento das solicitações do titular.

Conforme o artigo 20 da GDPR, integram o escopo de dados portáveis aqueles que digam respeito ao titular e que tenham sido fornecidos por ele a um responsável pelo tratamento. E, ainda, que assim tenha sido com embasamento em consentimento, contrato ou aferidos por processos automatizados. Pelo menos em nível legislativo a LGPD não impõe restrições, ressalvados os segredos industriais ou comerciais, restando aguardar a regulamentação para avaliar o escopo final dos dados portáveis no país. Um outro ponto relevante em nossa Lei, é o contido no § 7º, do artigo 18, que exclui do escopo os dados que, porventura, já tenham sido anonimizados pelo controlador. Considerando que o processo de anonimização, se corretamente realizado, é irreversível, não haveria lógica em não explicitar formalmente essa exceção.

Nas reflexões do EDPB fica em aberto a questão dos dados pessoais decorrentes de contratos de trabalho. É que parte da doutrina

entende que os dados dos empregados podem ser tratados à égide do legítimo interesse. Deste modo, pelo regulamento europeu, tais informações não entrariam no escopo da portabilidade (EDPB, 2017, p. 8-9). Concluindo, como o regulamento europeu se refere a dados processados por meios automatizados, há o consenso de que cópias em papel de arquivos não estão no escopo da portabilidade. É um direito tipicamente da era digital, para funcionamento e exercício em ambientes online (EDPB, 2017, p. 9).

3.2. O PROCESSO DE TRANSFERÊNCIA DOS DADOS

Preliminarmente, cabe ponderar sobre a natureza do processo de transferência de dados em face do que disciplina a LGPD. Por ser um processo, reveste-se de uma sequência de atividades que adquire o contorno de ações encadeadas de tratamento de dados pessoais, perfazendo todo um ciclo, que vai do acesso ao armazenamento, ou, até mesmo à própria eliminação ou descarte. Além desse aspecto, o processo pode envolver não somente o controlador atual e o controlador destinatário, mas terceiros habilitados ao processamento tecnológico das atividades. É o que este tópico procura elucidar em vista das práticas e exemplos internacionais.

3.2.1. ASPECTOS NORMATIVOS, TÉCNICOS, DE PADRONIZAÇÃO E DE SEGURANÇA

O processo de transferência de dados, em razão da portabilidade, é também uma espécie de atividade de tratamento enquadrada no artigo 5º, inciso X, da LGPD, ou seja "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". Assim, caracteriza-se tratamento quando o controlador, ao atender à solicita-

ção, transmitir ou transferir dados pessoais, e quando o controlador receptor ou novo controlador, receber, armazenar ou arquivar tais dados.

Então, por força destas disposições, os cuidados com a segurança e integridade dos dados pessoais, previstos no artigo 6º, inciso VII, se impõe para ambos os controladores envolvidos no processo[2]. Segundo a Comissão Europeia (EDPB) alguns aspectos técnicos precisam estar presentes. O controlador deve transmitir os dados pessoais em formato interoperável, não existindo a obrigatoriedade para o novo controlador manter o mesmo formato para os dados recebidos. Somente o processamento da transferência terá que respeitar a compatibilidade (EDPB, 2017, p. 16) . A transmissão deve ocorrer na hipótese de a comunicação entre os dois sistemas for possível, de forma segura, com o uso de criptografia e sob autenticação das partes. Não sendo factível, por razões técnicas, o fato deve ser explicitado ao titular solicitante com os devidos motivos (EDPB, 2017, p.16). Os dados poderão ser transferidos diretamente, de uma só vez, toda a base de dados do titular, ou, parcialmente, por partes de um arquivo global maior. De outro lado, existe a alternativa do emprego de ferramenta automatizada para extração dos dados relevantes e subsequente entrega ao titular em meio (ou mídia) digital (EDPB, 2017, p. 16).
Recomenda-se o uso de mensagens seguras, servidores SFTP[3],

2 LGPD, Art. 6º (...) - VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

3 *SFTP – Secure File Transfer Protocol*. Como usar o SFTP para transferir arquivos com segurança com um servidor remoto. Justin Ellingwood. Maio, 2015. Disponível em: Ver mais em: https://www.digitalocean.com/community/tutorials/como-utilizar-o-sftp-para-transferir-arquivos-com-seguranca-com--um-servidor-remoto-pt. Acesso em 17 jun 2021. (Rever normas ABNT para esse tipo de referência. Adequar ao longo de todo o artigo e ao final no item Referências)

Web API[4] segura ou, finalmente, *Web Portal*[5] seguro. Utilizando-se tais ferramentas, os titulares podem ser habilitados a acessar os próprios dados, em ambiente seguro, com autenticação e uso de *tokens*, facilitando o processamento pelos controladores de suas solicitações (EDPB, 2017, p. 16).

Pesquisas feitas por Emmanuel Syrmoudis et ali, revelaram que a portabilidade direta entre os incumbentes e os pequenos provedores de serviços, não tem sido objeto de grande interesse, ainda, por parte dos consumidores (SYRMOUDIS, 2021, p. 14).

Existem opções tecnológicas em amplo uso no mercado que possibilitam a portabilidade de dados pela via indireta, notadamente os procedimentos de identificação e autenticação de titulares em várias plataformas de serviços. Essa opção vem sendo aproveitada pelos incumbentes, tais como Facebook, Google e Apple, que utilizam o protocolo de autenticação *OAuth*[6] ou (*One-way data Exchange by design*[7]). Em cerca de 45% dos serviços online pesquisados o OAuth vem sendo empregado (SYRMOUDIS, 2021, p.

4 Uma *Web API* é uma interface de programação de aplicações utilizada em servidores ou em navegadores para recuperação apenas dados necessários de um banco de dados. Disponível em: https://pt.wikipedia.org/wiki/Web_API. Acesso em 17 jun 2021.

5 Um *web portal* é uma plataforma baseada na web que coleta informações de diferentes fontes em uma interface de usuário única e concede aos usuários as informações mais relevantes de acordo com seu contexto. Disponível em: https://www.liferay.com/pt/resources/l/web-portal. Acesso em 17 jun 2021.

6 O *OAuth* é um padrão aberto para autorização utilizado para que usuários da internet possam fazer logon em outras plataformas, utilizando-se de suas contas já existentes em Google, Facebook, Microsoft, Twitter etc., sem ter que expor as suas senhas. Disponível em: https://pt.wikipedia.org/wiki/OAuth. Acesso em 17 jun 2021.

7 Troca de dados unilateral por design. Trata-se de protocolo de transferência padronizada de dados.

14). Considerando os princípios e fundamentos da legislação de proteção de dados e a necessidade de que o titular precisa estar no controle do seu tratamento, defende-se o emprego de Sistemas de Gerenciamento de Informações Pessoais (PIMS[8]).

Estes sistemas funcionam como um controlador de dados separado, com trocas diretas de dados entre controladores externos. São diferentes, portanto, de uma *Web API*, visto que esta é utilizada por terceiros (*third parties*) (KRAMER, 2020, p. 9). A premissa central do PIMS é ofertar ao usuário uma espécie de dashboard centralizado, integrando-o a vários serviços por ele utilizados, com funcionalidades-chave como: a) gestão da identidade; b) gestão de permissões; e c) transferência de dados (Idem, ibidem). O ponto crucial no processamento das solicitações de portabilidade, portanto, é a garantia de adoção de mecanismos e soluções seguros para a proteção dos dados pessoais que estão sendo portados - GDPR, art. 5 (I) (f) e LGPD, art. 6, VII e art. 44, I e III - logo, o compliance com os dispositivos legais e regulamentares sobre este tema.

3.2.2. O DEVER DE NÃO IMPOR OBSTÁCULOS À PORTABILIDADE

Como a portabilidade é um dos direitos expressamente assegurados aos titulares, a GDPR vedou a cobrança de tarifas ou taxas, em geral, para o atendimento das solicitações (GDPR, art. 12). Nesse aspecto, a LGPD remete o exercício de direitos, especialmente o da portabilidade, à posterior regulamentação pela autoridade nacional (LGPD, art. 18, V). O regulamento europeu somente admite a cobrança, excepcionalmente, diante de solicitações infundadas, abusivas ou repetitivas, o que deve ser demonstrado pelo controlado (EDPB, 2017, p. 15).

8 *PIMS – Personal Information Management Systems.*

Para além da questão da cobrança pelos serviços, que seria uma forma de custeio do processo de automatização da portabilidade, a regulamentação europeia é bastante incisiva quanto a não imposição de obstáculos ou embaraços ao atendimento das solicitações dos titulares. Assim, os dados pessoais devem ser transmitidos ao novo controlador sem nenhum tipo de obstáculo legal, técnico ou financeiro. Isto é, taxas, falta de interoperabilidade ou uso de formatos não compatíveis, APIs não apropriadas, demora excessiva ou complexidade em recuperar internamente os arquivos concernentes ao titular, dificuldade deliberada em disponibilizar os dados pessoais requeridos, imposição de excessiva padronização setorial ou, ainda, demandas de acreditação ou certificação não razoáveis ou desnecessárias (EDPB, 2017, p. 15). E tal cuidado faz todo o sentido, já que um dos objetivos da portabilidade é exatamente o fomento à concorrência, refletindo em maiores benefícios aos titulares. Se o fator custos de mudança representam uma das barreiras de entrada em mercados concentrados ou monopolizados, nos mercados marcadamente digitais[9] a tendência é que tais custos de transação sejam menores, e a portabilidade sem obstáculos promete um novo patamar de competitividade nesses negócios (EDPB, 2017, p. 56).

3.3. RESPONSABILIDADES DE CONTROLADORES ADVINDAS COM A PORTABILIDADE

Como princípio basilar da proteção dos dados pessoais contra riscos de violação da privacidade, e mitigação de prejuízos morais ou materiais que incidentes de segurança possam ocasionar, cumpre analisar a responsabilização dos controladores no processo de atendimento às solicitações de portabilidade dos dados feitas

9 Diante da dinâmica dos modelos de negócio digitais, a portabilidade neste aspecto requer que os dados voluntariamente fornecidos pelos titulares, bem como os dados observados, sejam prontamente disponibilizados em formato estruturado, simples, padronizado e legível por máquinas (WP 242, p. 56).

pelo titular. O fato de ser um atendimento de requisição de iniciativa do titular não exonera os controladores e terceiros envolvidos dos cuidados recomendados e da devida responsabilização.

3.3.1. A RESPONSABILIDADE DO CONTROLADOR, DO NOVO CONTROLADOR E O MOMENTO EM QUE CESSA A RESPONSABILIDADE

Como visto, é necessária a proteção dos dados pessoais durante o processo de transferência do controlador para o novo controlador, pois a transmissão é uma das espécies que caracterizam o tratamento, ainda que a providência tenha sido por solicitação expressa do titular (HERINGER; VIOLA, 2020, p. 7) . Logo, a garantia de medidas seguras é dever de quem transmite e de quem recebe tais dados. Logo, Mario Viola e Leonardo Heringer entendem que, por ser uma atividade levada a cabo por expressa solicitação do titular, e não em razão de seu consentimento, o controlador assume o papel de operador de dados, incumbindo-lhe certificar-se de que os dados foram corretamente entregues ao verdadeiro destinatário, assegurada previamente a autenticidade da identidade do titular dos dados (HERINGER; VIOLA, 2020, p. 8).

Atendidos a esses requisitos, a responsabilidade do controlador se encerra, estando presente somente durante o processamento da portabilidade e vai até a sua conclusão. Existem ressalvas, por exemplo, quando por força de aspectos legais ou regulamentares os dados pessoais devam ser mantidos ou mesmo tratados na origem, não exonerando, portanto, o antigo controlador das responsabilidades, visto que não deixa de continuar sendo um controlador (HERINGER; VIOLA, 2020, p.9). Neste ponto, o Comitê Europeu entende que o processo de portabilidade não impõe a obrigação do controlador de reter por um período muito maior do que o necessário os dados pessoais portados. Por exemplo, para atender futuras solicitações de “nova portabilidade”. Tampouco,

o controlador precisa verificar se os dados pessoais estão com a qualidade desejada para promover a transmissão (EDPB, 2017, p.6). O Comitê Europeu, ainda, assentou que a responsabilidade do controlador é a de verificar se o novo controlador age realmente em nome do titular, mediante a adoção de processo de autenticação. Todavia, o controlador, ao atender à solicitação do titular, não detém a responsabilidade de confirmar se o novo controlador, destinatário, está aderente às leis e padrões de segurança, uma vez que a escolha do ente receptor é livre do titular dos dados (EDPB, 2017, p. 6). O novo controlador é responsável por assegurar que os dados recebidos são relevantes e não excessivos, isto é, de acordo com a nova finalidade consentida pelo titular para o seu uso. Em razão do princípio da minimização, deve ser observado, então, o propósito do tratamento (EDPB, 2017, p. 6). Concluída a portabilidade, a organização receptora se transforma em controladora dos dados pessoais, incidindo as disposições do art. 5, da GDPR, com todos os reflexos e obrigações decorrentes, como a transparência, limitação da coleta, qualidade, integridade, confidencialidade, limitação do arquivamento ou conservação e, ainda, *accountability* (EDPB, 2017, p. 6).

De outro lado, todos os controladores devem estar preparados para facilitar o exercício do direito, sem obstáculos, como já assinalado, porém podem escolher se aceitam ou não os dados pessoais de um titular dessa forma. Conquanto seja obrigação ao controlador promover a portabilidade, a pedido do titular, para o novo controlador a modalidade é facultativa, segundo o Conselho Europeu (EDPB, 2017, p. 7) . Assim como na LGPD (art. 18, § 4º, II[10]), a GDPR (art. 12 (3)) estabelece o prazo máximo de um mês, e, excepcionalmente para os casos complexos, o máximo

10 LGPD. Art. 18, "§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: (...) II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência".

de três meses, para que o controlador atenda à solicitação. Ou, não sendo possível, deverá justificar fundamentadamente (GDPR, art. 12 (4)), até o máximo de um mês, indicando as razões para não atender (EDPB, 2017, p. 14-15). A definição do prazo, no caso da portabilidade, ficou a cargo de regulamentação posterior pela ANPD. As legislações não contemplam a opção de não responder ao titular. Ou o controlador atende, ou justifica, sempre no prazo dado pela legislação ou regulamento. Este dever decorre do princípio da transparência. Finalmente, aguarda-se que bem assim das sanções eventualmente aplicáveis em decorrência do descumprimento pelos agentes de tratamento do disposto na lei e nos regulamentos (artigo 53[11], da LGPD).

4. OPEN BANKING: ASPECTOS GERAIS E CONCEITO

Atualmente, os dados podem ser considerados o novo petróleo na era digital, dando origem às empresas gigantes como foram as *Standard Oil* no início do século XX (*THE ECONOMIST*, 2017, tradução livre). Essa transformação e atribuição monetária vinculada ao compartilhamento de dados é fomentada principalmente pelo uso de aplicativos instalados em aparelhos de telefonia móvel.

Em território brasileiro, o IBGE estima que aproximadamente 80% dos brasileiros tenham aparelho celular e que 98% destes o utilizem para acessar a Internet, em comparação a algo em torno de 50,7% dos brasileiros que utilizam o computador e 12% que usam o tablet para acessar a rede. Os dados são referentes à Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua de 2018 do Instituto Brasileiro de Geografia e Estatística (IBGE, 2020).

11 LGPD: 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.

Estes números refletem uma sociedade altamente conectada. Autores como Chaves (1996, p. 97) alertavam sobre uma potencial mudança da transferência unilateral da informação numa modalidade interativa. Neste sentido, a informática, ou tratamento eletrônico e digital, vem agilizando a coleta de dados, sua manipulação e armazenamento em parâmetros quase que ilimitados de possibilidades.

O *Open Banking*, ou sistema financeiro aberto, é um desdobramento deste novo ecossistema informacional vinculado ao uso da internet e plataformas digitais, se tornando uma ferramenta de inovação na prestação de serviços financeiros pelo meio eletrônico.

Esse sistema é utilizado no Reino Unido desde 2018. Seu conceito está atrelado a uma política de compartilhamento de dados abertos que permitem a circulação de informações entre diferentes instituições e em território nacional está estritamente conectado aos Direitos do Titulares, expressos no art.18, da Lei Geral de Proteção de Dados (LGPD). Sobre o sistema *Open Banking*, Carrete e Tavares (2019, p.24) afirmam:

> É um sistema bancário aberto e colaborativo, onde os dados pertencem aos clientes – donos da conta bancária –, que têm a prerrogativa de poder compartilhá-los com instituições bancárias ou não bancárias. O sistema pressupõe que os dados bancários dos clientes serão compartilhados com terceiros.
> No *open banking* o cliente poderá integrar várias contas bancárias, de diversos bancos, em um mesmo cartão. Nesse sistema, os bancos perdem a exclusividade de informações como saldo na conta-corrente e nas aplicações ou endividamento. Por outro lado, os bancos oferecem seus produtos, sejam de investimento ou financiamento, e abrem acesso às suas *application programming interfaces (APIs)* – interfaces de programação de aplicativos, para que clientes (pessoas físicas e jurídicas) possam acessar. A ideia é ampliar o acesso aos produtos e serviços do mercado financeiro e, com isso, obter melhores taxas.

Para fins de contextualização, o *Open Banking* dita como os fluxos de dados ocorrerão nas interfaces de programação de aplicativos (APIs). Essas APIs funcionam como um garçom em um restaurante. As *fintechs* (clientes) selecionam os tipos de dados que possuem interesse no cardápio (documentação) e informam ao garçom (API). O pedido é entregue para o cozinheiro (Banco). O cozinheiro preparará a comida (dados solicitados). Assim que pronto, o garçom trará a comida para os clientes (PRATINI, 2019, tradução livre). O objetivo principal é beneficiar os consumidores de serviços financeiros pelo uso da tecnologia de código aberto.

4.1. DO CONSENTIMENTO EXPLÍCITO DO CONSUMIDOR

No Brasil, a regulamentação do *Open Banking* é recente e data de 2020, consolidando-se pela Resolução Conjunta nº1/2020 do Banco Central do Brasil (BCB) com o Conselho Monetário Nacional (CMN), e percebe-se que mesmo a LGPD possibilitando hipóteses de tratamento de dados que dispensam o consentimento do titular, isto não ocorre no sistema *Open banking*.

Vislumbra-se na resolução, que, em se tratando deste sistema, o consentimento do titular se torna o principal alicerce para se legitimar a prestação do serviço, conforme se extrai do seu art.8º "a solicitação de compartilhamento de dados de cadastro e de transações e de serviços (...) compreende as etapas do consentimento, autenticação e confirmação".

Ressalta-se que a resolução, também estipula o procedimento adotado para a coleta do consentimento do titular em seu art.10, §1º, devendo:

> I - ser solicitado por meio de linguagem clara, objetiva e adequada;
> II - referir-se a finalidades determinadas;
> III - ter prazo de validade compatível com as finalidades de que trata o inciso II, limitado a doze meses;

> IV - discriminar a instituição transmissora de dados ou detentora de conta, conforme o caso;
> V - discriminar os dados ou serviços que serão objeto de compartilhamento, observada a faculdade de agrupamento de que trata o art. 11;
> VI - incluir a identificação do cliente;
> e VII - ser obtido após a data de entrada em vigor desta Resolução Conjunta, com observância dos prazos estabelecidos no art. 55.

Assim, resta mais do que comprovada pela Resolução a importância atribuída ao consentimento do titular para que se efetue a prestação do serviço, sob pena de responsabilidade. Salienta-se que a autorização para o compartilhamento de dados do cliente possui três etapas: Consentimento; Autenticação e Confirmação. Segundo o BCB (2020) "Essas etapas devem ser realizadas exclusivamente por canais eletrônicos e devem ser efetuadas com segurança, agilidade, precisão e conveniência, de forma sucessiva e ininterrupta, com duração compatível com seus objetivos e nível de complexidade".

Ainda sobre o compartilhamento Claudia (2020) explica que:

> O compartilhamento deve ser expressamente autorizado pelo cliente e tem prazo de um ano, mas pode ser encerrado a qualquer momento pelos canais de cada instituição financeira. Só podem participar do *open banking* instituições reguladas, autorizadas e supervisionadas pelo BC, estando sujeitas às sanções administrativas por eventual quebra de sigilo bancário.

Ressalta-se, com o apontamento, duas limitadoras da efetivação do compartilhamento de dados abertos: a autonomia na vontade do cliente que a qualquer momento pode solicitar o imediato cancelamento da prestação do serviço, e o caráter temporal da prestação que deve ter prazo de um ano.

4.2. DIFERENÇAS ENTRE PORTABILIDADE DE DADOS E OPEN BANKING

Ainda que o sistema aberto financeiro possa ser considerado uma extensão da portabilidade de dados, ambos possuem diferenças, pois, segundo Viola e Thomazelli (2021, p.5), "na portabilidade dos dados, pretende-se que o titular dos dados possa levar os seus dados pessoais para um novo fornecedor, ainda que não seja fornecedor de serviços que atue na mesma área do fornecedor que disponibilizará os dados para serem portados", extinguindo assim o vínculo anterior.

Enquanto no *Open Banking* não há a transferência integral dos dados do consumidor para o novo prestador de serviços, apenas é possibilitado o acesso aos dados para ser efetuada a operação desejada pelo cliente, assim não há a extinção do vínculo anterior. Ambos possibilitam a promoção da competitividade, pois o consumidor não se vê preso a um único fornecedor.

Delineada a diferença, é importante pontuar os principais objetivos do sistema aberto de dados, expressos na Resolução Conjunta nº1, no seu art. 3º: "I- incentivar a inovação; II – promover a concorrência; III - aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro; e IV - promover a cidadania financeira". Nota-se que esse sistema é pensado no intuito de garantir a cidadania financeira, realizando a proteção dos dados e promovendo a autodeterminação informativa.

Sobre os objetivos, o Diretor de Regulação do Banco Central do Brasil, em sede do voto 44/2020, relata que (BRASIL, 2020):

> (...)Tais ações [*open banking*] geralmente têm por objetivo aumentar a competitividade nos mercados financeiros, incentivar a inovação financeira, racionalizar os processos de instituições reguladas, possibilitar parcerias comerciais entre instituições financeiras e insti-

> tuições não financeiras, e, também, em diversos casos, empoderar o consumidor financeiro. Importante ressaltar que o consumidor é reconhecido como o titular dos seus dados pessoais; no caso do Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei nº 13.709, de 14 de agosto de 2018, reforçará e sistematizará, a partir de sua entrada em vigor, a tutela desses dados. Com o *Open Banking*, o consumidor financeiro pode consentir com o compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas de instituições financeiras e de pagamento, caso vislumbre algum benefício com esse compartilhamento, a exemplo do acesso a serviços financeiros adequados ao seu perfil.

Esse cuidado com o empoderamento do consumidor financeiro, citado pelo Diretor de Regulação do Banco Central do Brasil, não se dá por mera casualidade, pois a LGPD assegura como fundamento, justamente, o princípio da autodeterminação informativa.

Salienta-se que mesmo não sendo uma novidade trazida pela LGPD, a autodeterminação informativa no atual contexto se faz extremamente importante ao consumidor, pois o conhecimento consciente do tratamento de dados utilizado se tornou necessário, não só para proteger à privacidade e à intimidade, mas para os atos da vida civil, como aponta a Unesco:

> Atualmente, todos os cidadãos precisam conhecer as funções, os papéis, os direitos e as obrigações das instituições de informação e mídia nas sociedades do conhecimento; e também precisam conhecer as oportunidades e as dificuldades envolvidas, além da possibilidade de abuso imposto por instituições e indivíduos nas comunidades ou em grupos específicos, como jovens, idosos, mulheres, homens ou qualquer indivíduo em geral. (UNESCO, 2016, p. 26).

4.2.1. INTEROPERABILIDADE DOS SISTEMAS

Outro ponto que norteia as discussões centrais sobre o sistema *Open Bankig*, é a interoperabilidade dos sistemas, que é um requisito para a efetivação do compartilhamento de dados abertos. A interoperabilidade nada mais é do que a disponibilização dos dados em formatos padronizados, representados em meio digital, processáveis em máquina, em formato livre de restrição quanto à sua utilização e está regulamentada nos arts. 23 e 44 da Resolução Conjunta nº1/2020. Sobre a interoperabilidade, Viola e Thomazelli (2021, p.10) observam que:

> A interoperabilidade entre os sistemas dos participantes do *Open Banking*, por meio da padronização de interfaces e de dados, bem como do estabelecimento de princípios e regras de governança entre os participantes, permitirá não somente a transmissão efetiva dos dados, mediante o consentimento do cliente, como também o uso ou reuso dessas informações pela instituição receptora, seja para fins de portabilidade desses dados ou para o compartilhamento de produtos e serviços.

A interoperabilidade entre os sistemas é fundamental para que se consolide o compartilhamento de dados abertos, tornando-se a primeira fase para a implementação do sistema *Open Banking*, prevista até 01/02/2021, e será tratada a seguir.

4.3 IMPLEMENTAÇÃO DO SISTEMA OPEN BANKING

O sistema *Open Banking*, nasce com a promessa de representar uma nova era no âmbito das prestações dos serviços financeiros, fomentando de forma significativa a transformação digital nas agências bancárias, Mignot (2021) ressalta que:

> O *Open Banking* tem tudo para representar uma nova era para o segmento bancário e financeiro, impulsionando de vez a transformação digital. Isso porque, de forma prática, a abertura do sistema bancário

> permitirá o compartilhamento de dados dos usuários entre as instituições financeiras, liberando assim a troca de informações essenciais para a oferta de serviços e produtos dos mais variados tipos.

A aposta nesta transformação é tão séria, que na Resolução Conjunta nº1/2020, o BCB com o CMN, em seu art. 6º impõe a adesão de forma obrigatória pelas instituições enquadradas nos segmentos 1 (S1) e 2 (S2). Estes seguimentos são conceituados pela Resolução nº4.553/2017 do BCB, e são compostos:

> § 1º O S1 é composto pelos bancos múltiplos, bancos comerciais, bancos de investimento, bancos de câmbio e caixas econômicas que:
> I - tenham porte igual ou superior a 10% (dez por cento) do Produto Interno Bruto (PIB); ou
> II - exerçam atividade internacional relevante, independentemente do porte da instituição.
> § 2º O S2 é composto:
> I - pelos bancos múltiplos, bancos comerciais, bancos de investimento, bancos de câmbio e caixas econômicas, de porte inferior a 10% (dez por cento) e igual ou superior a 1% (um por cento) do PIB; e
> II - pelas demais instituições de porte igual ou superior a 1% (um por cento) do PIB. (BRASIL, 2017).

Com a obrigatoriedade, grandes instituições como o Banco Bradesco, Banco do Brasil, Banco Itaú e Banco Santander[12] aderirão ao *Open Banking*, e consequentemente promoverão a sua popularização (OPEN, 2021). Em relação aos outros segmentos e demais instituições a adesão se realiza de forma voluntária, todavia a tendência é acompanharem o mercado financeiro. O BC, dentro de suas atribuições legais, regulamentou, por meio da Circular nº4.032/2020, como será disposta a estrutura inicial responsável pela governança do processo de implementação do *Open*

12 Cinco maiores bancos do Brasil conforme UOL em notícia publicada em 04/06/2020: https://economia.uol.com.br/noticias/redacao/2020/06/04/5-maiores-bancos-concentram-mais-de-80-dos-depositos-e-emprestimos--diz-bc.htm. Acesso em: 24 abr. 2021.

Banking no País. A circular estipula, em seu art 2°, três níveis da estrutura inicial, divididas por um Conselho Deliberativo estratégico, um Secretariado administrativo e Grupos Técnicos.

Para a implementação deverá ser observada a resolução conjunta nº1/2020 do BCB, que, em seu art. 55, dispõe sobre o processo de implementação deste novo sistema, especificando quatro diferentes fases com datas pré-definidas. Salienta-se que este cronograma foi alterado posteriormente, em 27/11/2020, pela resolução conjunta nº2/2020 passando a vigorar com as seguintes alterações:

> Art. 55. Esta Resolução Conjunta entra em vigor em 1º de junho de 2020, com observância dos seguintes prazos:
> I - até 1º de fevereiro de 2021, para a implementação do disposto nos incisos III e VI do art. 44, bem como dos requisitos necessários para o compartilhamento de dados sobre canais de atendimento e produtos e serviços de que trata o art. 5º, inciso I, alíneas "a" e "b", itens 1 a 5;
> II - até 15 de julho de 2021, para a implementação do disposto no inciso IV do art. 44, bem como dos requisitos necessários para o compartilhamento de dados de cadastro e de transações de que trata o art. 5º, inciso I, alíneas "c" e "d", itens 1 a 5;
> III - até 30 de agosto de 2021, para a implementação dos requisitos necessários para o compartilhamento de serviços de que trata o art. 5º, inciso II; e
> IV - até 15 de dezembro de 2021, para a implementação dos requisitos necessários para o compartilhamento de:
> a) dados sobre produtos e serviços de que trata o art. 5º, inciso I, alínea "b", itens 6 a 10; e
> b) dados de transações de que trata o art. 5º, inciso I, alínea "d", itens 6 a 11." (NR). (BRASIL, 2020).

Sobre as fases o Diretor de Regulação do Banco Central do Brasil esclarece que serão organizadas da seguinte forma:

> I - Fase I do *Open Banking*: compartilhamento de dados relacionados com canais de atendimento e com produtos e serviços disponíveis

> para a contratação relacionados com contas de depósito à vista ou de poupança, contas de pagamento ou operações de crédito;
> II - Fase II: compartilhamento de: a) informações de cadastro de clientes e de representantes, feitas algumas exceções, a exemplo dos dados classificados como dado pessoal sensível pela legislação em vigor, com vistas a evitar tratamento discriminatório de clientes; e b) dados de transações dos clientes acerca dos produtos e serviços relacionados na Fase I que forem contratados ou distribuídos pela instituição transmissora de dados, especificamente o histórico de transações realizadas nos últimos doze meses e os contratos vigentes nesse mesmo período, no caso de operações de crédito;
> III - Fase III: compartilhamento dos serviços de iniciação de transação de pagamento e de encaminhamento de proposta de crédito; e
> IV - Fase IV: expansão do escopo de dados, com vistas a abranger os dados de produtos e serviços de operações de câmbio, serviços de credenciamento em arranjos de pagamento, investimentos, seguros e previdência complementar aberta, bem como os dados de transação de clientes a respeito desses produtos e serviços e também sobre contas-salários. (BRASIL, 2020)

Ainda, sobre a segunda fase de implementação do *Open Banking*, o BC, em 16/04/2021, modificou as regras estipuladas na resolução conjunta n° 1/2020. A alteração complementou e estabeleceu requisitos técnicos e procedimentos operacionais, o objetivo foi reforçar o direito à proteção de dados dos clientes por meio da resolução BCB nº 86/2021.

Uma das principais medidas que a nova resolução estabelece é a instituição do manual de experiência do cliente, que segundo Claudia (2020) "(...) O novo manual se junta a outros quatro já previstos na regulamentação, são eles: Escopo de Dados e Serviços; APIs; Serviços Prestados pela Estrutura de Governança; e Segurança, que também estão sendo atualizados e consolidados".

Essas alterações possuem o sentido de melhorar a experiência do consumidor com o serviço, aprimorar a regulamentação anterior, reforçar a proteção dos dados, e assegurar direitos ao con-

sumidor. Sobre as alterações destaca-se:

> Que as instituições participantes no quadro de banco aberto para fins de compartilhamento de dados devem informar a data e hora da última atualização dos dados compartilhados, bem como a data e a hora em que ocorreu o compartilhamento de dados;
> - Para efeitos de partilha de dados relacionados com contas conjuntas de pessoas singulares, a instituição que transmite os dados deve: garantir que a instituição que recebe os dados tenha acesso aos dados cadastrais apenas do titular da conta responsável pelo consentimento, não sendo permitido o compartilhamento dos dados cadastrais de outros titulares da conta; compartilhar dados transacionais da conta conjunta por meio do consentimento do titular dos dados, que pode ter acesso às informações da conta transacional; e exigir a confirmação de todos os titulares de contas para acesso às informações transacionais; e
> - A criação do manual de experiência do cliente de banco aberto que deve: delinear os princípios para orientar a experiência do cliente no processo de solicitação de compartilhamento de dados e serviços; fornecer os requisitos do guia de experiência do cliente, incluindo o seu conteúdo e esquema, com vista a harmonizar as etapas de consentimento, autenticação e confirmação entre as instituições participantes no *open banking*; e
> - Disponibilizar uma versão atualizada às instituições participantes e ao público em geral por meio do portal de banco aberto no Brasil. (DATAGUIDANCE, 2021, tradução livre).

Outros requisitos técnicos e procedimentais, importantes, que devem ser observados pelas organizações financeiras, são: a proibição de compartilhamento de dados cadastrais de outros titulares da conta, devendo ser observado o consentimento destes; a admissão, sem prejuízo da regulamentação a respeito do tempo de resposta, de que os dados compartilhados pela instituição transmissora tenham a defasagem máxima em relação à disponibilização em seus canais eletrônicos de até cinco minutos, no que se refere a dados de saldo e transações realizadas em conta de depósitos ou de pagamento e de até uma hora para

outros casos. Percebe-se que os requisitos técnicos estipulados possuem caráter preventivo sobre os riscos do negócio e também melhoram a prestação da efetividade do serviço.

4.3.1 PRINCIPAIS DESAFIOS

Muitos são os desafios trazidos para as instituições financeiras com o advento da implementação do *Open Banking*, pois é necessária a implementação de padrões tecnológicos para a prestação do serviço e a tomada de decisões preventivas para prevenir futuras irregularidades jurídicas. Sobre os desafios existentes Viola e Thomazelli (2021, p.11) alertam que:

> A implementação de um sistema de *Open Banking* interoperável trará, por um lado, desafios significativos para as instituições, que terão que estabelecer interfaces no ecossistema e padronizar a formatação de dados. Isso implicará, em muitas vezes, na organização interna de sistemas legados, além de implementação de mudanças na forma de gestão das informações, sem falar na necessidade de estabelecer princípios, regras e governança que permitam a gestão contínua do *Open Banking*.

Inevitavelmente, o compartilhamento aberto de dados trará uma reestruturação na organização, na parte tecnológica, no sentindo de padronizar os sistemas, conforme é previsto na Resolução Conjunta nº 1. A padronização dos sistemas, também chamada de interoperabilidade é importante no âmbito das tecnologias IoT para promover a comunicação fluída e uniforme destas instituições, Matos (2020, p.15) observa que "(...) é difícil encontrar um padrão amplamente estabelecido em ambientes de sistema IoT. Portanto, a interoperabilidade acaba sendo um desafio na portabilidade de dados (...)".

Além da padronização, chamam a atenção as questões da segurança e privacidade dos dados tratados, pois são inúmeros os

casos em que dados são utilizados de forma inadequada ou vazados, gerando danos para os seus titulares, para Matos (2020, p.15):

> Por trabalhar com dados pessoais dos usuários, os quais são considerados dados sensíveis, o tópico de segurança e privacidade é um dos principais desafios no desenvolvimento e aplicabilidade de ambientes com sistemas IoT. Além disso, a portabilidade pode adicionar um risco a mais na segurança dos dados, uma vez que os mesmos terão de trafegar pela rede entre a plataforma de origem e a plataforma de destino.

Portanto, é evidente a preocupação no dever de proporcionar um sistema padronizado, com uma circulação de dados fluida, bem como com recursos tecnológicos que reduzam a chance de vazamento de dados, sob a pena de reparação na esfera administrativa e a descredibilidade do serviço na esfera comercial.

5. CONSIDERAÇÕES FINAIS

Concluídos os debates propostos, as considerações que se cumprem realizar seguem no sentido apontado e fundamentador do trabalho: a ANPD, bem como todo o ambiente legal da proteção de dados no Brasil está longe de satisfazer as necessidades de definição de conceitos, técnicas e *standards* mínimos de prática necessários à garantia de um cenário juridicamente seguro para todas as partes envolvidas, diante do que se torna inconcebível não externar as preocupações identificadas pelo debate e estudo proposto, demonstrando-se clara a necessidade de exigir das autoridades competentes uma rápida e eficiente colaboração com a comunidade jurídico-acadêmica visando a supressão das deficiências indicadas.

Ao tempo e no decorrer da produção das pesquisas e do trabalho, identificaram-se que temas como a portabilidade e o o*pen banking*, em que pese há muito e amplamente debatidos e supe-

rados no cenário internacional, careciam até mesmo de definições claras quando importadas para o ambiente de regulação e proteção de dados no Brasil, por vezes sendo alvo de confusão, inclusive entre si, tanto no campo teórico de definição quanto na prática, na aplicação por controladores e operadores experientes e até bem assessorados.

Ainda, no que diz respeito aos Direitos do Titular de acesso aos seus Dados, cumpre destacar o resultado da pesquisa de campo realizada ao longo do trabalho, através da qual identificou-se que as confusões não se dão somente com relação aos conceitos, teorias e terminologias, mas também no campo prático, uma vez que identificada imensa dificuldade dos controladores em adequar, facilitar e promover o acesso do Titular aos seus Dados Pessoais, algo que, supostamente, deveria ser básico.

O campo de estudo dos Direitos do Titular revela-se, assim, ainda muito fértil ao debate tanto na variedade de temas quanto na possibilidade de aprofundamento de temas já estabelecidos. Entretanto, é necessário apontar a necessidade urgente de que as autoridades trabalhem no estabelecimento de bases, regulações, definições, limites e procedimentos claros de modo a uniformizar os critérios de legalidade e licitude no tratamento de dados e conceder aos controladores, operadores e titulares, segurança jurídica nestes tratamentos que, conforme demonstrado no desenvolvimento, em regra, no âmbito pessoal da titularidade dos dados e até mesmo no âmbito comercial, tendem a ser benéficos a todas as partes, desde que devidamente guarnecidos.

5. CONSIDERAÇÕES FINAIS

Concluídos os debates propostos, as considerações que se cumprem realizar seguem no sentido apontado e fundamentador do trabalho: a ANPD, bem como todo o ambiente legal da proteção de dados no Brasil está longe de satisfazer as necessidades de definição de conceitos, técnicas e standards mínimos de prática necessários à garantia de um cenário juridicamente seguro para todas as partes envolvidas, diante do que se torna inconcebível não externar as preocupações identificadas pelo debate e estudo proposto, demonstrando-se clara a necessidade de exigir das autoridades competentes uma rápida e eficiente colaboração com a comunidade jurídico-acadêmica visando a supressão das deficiências indicadas.

Ao tempo e no decorrer da produção das pesquisas e do trabalho, identificaram-se que temas como a portabilidade e o *open banking*, em que pese há muito e amplamente debatidos e superados no cenário internacional, careciam até mesmo de definições claras quando importadas para o ambiente de regulação e proteção de dados no Brasil, por vezes sendo alvo de confusão, inclusive entre si, tanto no campo teórico de definição quanto na prática, na aplicação por controladores e operadores experientes e até bem assessorados.

Ainda, no que diz respeito aos Direitos do Titular de acesso aos seus Dados, cumpre destacar o resultado da pesquisa de campo realizada ao longo do trabalho, através da qual identificou-se que as confusões não se dão somente com relação aos conceitos, teorias e terminologias, mas também no campo prático, uma vez que identificada imensa dificuldade dos controladores em adequar, facilitar e promover o acesso do Titular aos seus Dados Pessoais, algo que, supostamente, deveria ser básico.

O campo de estudo dos Direitos do Titular revela-se, assim, ainda muito fértil ao debate tanto na variedade de temas quanto na possibilidade de aprofundamento de temas já estabelecidos. Entretanto, é necessário apontar a necessidade urgente de que as autoridades trabalhem no estabelecimento de bases, regulações, definições, limites e procedimentos claros de modo a uniformizar os critérios de legalidade e licitude no tratamento de dados e conceder aos controladores, operadores e titulares, segurança jurídica nestes tratamentos que, conforme demonstrado no desenvolvimento, em regra, no âmbito pessoal da titularidade dos dados e até mesmo no âmbito comercial, tendem a ser benéficos a todas as partes, desde que devidamente guarnecidos.

REFERÊNCIAS BIBLIOGRÁFICAS

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Campus, 1992.

BRASIL. BANCO CENTRAL DO BRASIL. **Circular nº 4.032**. 2020. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=4032. Acesso em: 24 jan. 2021

BRASIL. BANCO CENTRAL DO BRASIL. **Circular Nº 4.015**. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/circular-n-4.015-de-4-de-maio-de-2020-255164763. Acesso em: 24 abr. 2021.

BRASIL. BANCO CENTRAL DO BRASIL. **Relatório de Economia Bancária: 2019 – dezembro 2019**. 2020. Disponível em: https://www.bcb.gov.br/publicacoes/relatorioeconomiabancaria. Acesso em: 24 abr. 2021.

BRASIL. BANCO CENTRAL DO BRASIL. **Resolução CMN nº 4.553. 2017**. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4553. Acesso em: 24 abr. 2021.

BRASIL. BANCO CENTRAL DO BRASIL. **Resolução Conjunta nº 1. 2020**. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v2_P.pdf. Acesso em: 24 abr. 2021.

BRASIL. BANCO CENTRAL DO BRASIL. **Resolução Conjunta nº 2. 2020**. Disponível em: https://www.ancord.org.br/wp-content/uploads/2020/11/Resolucao-Conjunta-n-2-de-27_11_2020.pdf. Acesso em: 24 abr. 2021.

BRASIL. BANCO CENTRAL DO BRASIL. **Resolução nº 86. 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-bcb-n-86-de-14-de-abril-de-2021-314565458. Acesso em: 24 abr. 2021.

BRASIL. BANCO CENTRAL DO BRASIL. **Voto 44/2020-CMN**. 2020. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadVoto.asp?arquivo=/Votos/CMN/202044/Voto%200442020_CMN.pdf. Acesso em: 24 abr.

BRASIL. Lei nº 8.078, de 11 de Setembro de 1990. **Código de Defesa do Consumidor**. Brasília, DF: 1990. Disponível em https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 24 abr. 2021.

BRASIL. PLANALTO. **Lei nº 13.709, de 14.08.2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 14 jun 2021.

BRASIL. ***OPEN BANKING:* sistema simplificará relação entre bancos e clientes. Sistema simplificará relação entre bancos e clientes**. 2021. Disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/02/sistema-simplificara-relacao-entre-bancos-e-clientes#:~:text=E%20quais%20informa%C3%A7%C3%B5es%20poder%C3%A3o%20ser,%2FCNPJ%2C%20telefone%20e%20endere%C3%A7o. Acesso em: 24 abr. 2021.

CLAUDIA, Maria. **Banco Central altera norma para segunda fase do *open banking*: medida reforça segurança de dados dos clientes**. 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-04/banco-central-altera-norma-para-segunda-fase-do-open-banking. Acesso em: 23 abr. 2021.

Convenção nº 108 do Conselho Europeu – **Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais**. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37 Acesso em: 21 abr. 2021.

CARRETE, Liliam Sanchez; TAVARES, Rosana. **Mercado Financeiro Brasileiro**. São Paulo: Atlas, 2019, p. 24.

CHAVES, Antonio. **Direitos Autorais na Computação de Dados**. São Paulo: LTr, 1996, p. 97.

DATA GUIDANCE. ***BRAZIL: BACEN adds data protection to open banking rules***. 2021. Disponível em: https://www.dataguidance.com/news/brazil-bacen-adds-data-protection-open-banking-rules. Acesso em: 24 abr. 2021.

DOHMANN, Indra Spiecker Gen. **A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados Da União Europeia**.Tratado de Dados Pessoais. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

ELLINGWOOD, Justin. **Como usar o SFTP para transferir arquivos com segurança com um servidor remoto**. Maio, 2015. Disponível em: https://www.digitalocean.com/community/tutorials/como-utilizar-o-sftp-para-transferir-arquivos-com-seguranca-com-um-servidor-remoto-pt. Acesso em: 17 jun. 2021.

EUROPA. ***Guidelines On The Right To Data Portability***. WP 242. Article 29 Data Protection Working Party. Revisado em 05.04.2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611233. Acesso em 14 jun. 2021.

HERINGER, Leonardo; VIOLA, Mario. **A PORTABILIDADE NA LGPD**. ITS, Rio de Janeiro. Outubro, 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/A-Portabilidade-na-LGPD.pdf. Acesso em 14 jun. 2021.

IBGE. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal** 2018. Rio de Janeiro: IBGE, 2020. Disponível em: https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2101705. Acesso em: 20 mar. 2021.

KRAMER, Jan et al. ***MAKING DATA PORTABILITY MORE EFFECTIVE FOR THE DIGITAL ECONOMY***. *Economic Implications and Regulatory Challenges*. Junho, 2020. *CERRE – Centre on Regulation in Europe* p. 9. Disponível em: https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/. Acesso em: 17 jun. 2021.

LIFERAY. **O que é Web Portal**. Disponível em: https://www.liferay.com/pt/resources/l/web-portal. Acesso em: 17 jun. 2021.

MALDONADO, Viviane Nóbrega et al. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS COMENTADA**. São Paulo: Revista dos Tribunais, 2021.

MATOS, Everton de. **Desafios da implementação da Portabilidade de Dados em ambientes inteligentes conectados**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/Everton-internet-das-Coisas.pdf. Acesso em: 24 abr. 2021.

MIGNOT, Marin. ***Open Banking:* o novo passo na jornada de transformação do setor bancário**. 2021. Disponível em: https://computerworld.com.br/inovacao/open-banking-o-novo-passo-na-jornada-de-transformacao-do-setor-bancario/. Acesso em: 23 abr. 2021.

OPEN Banking: **Quem participa**. 2021. Disponível em: https://openbankingbrasil.org.br/quem-participa/. Acesso em: 23 abr. 2021.

RENZETTI, Bruno Polonio; ALMEIDA, Luís Felipe Rasmuss de; BANHO, Tiago Paes de Andrade. **Implicações da Lei do Cadastro Positivo para a Proteção de Dados Pessoais no Brasil: as dificuldades do sistema de *opt-out***. In: TOMASEVICIUS FILHO, Eduardo (org.). A lei geral de proteção de dados brasileira: uma análise setorial. São Paulo: Almedina Brasil, 2020. Cap. 4. p. 129-170.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade de hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

ROSATO, Fábio. ***Open Banking:* ameaça ou oportunidade?**. 2019. Disponível em: https://br.sensedia.com/post/open-banking-threat-or-opportunity. Acesso em: 24 abr. 2021.

THE ECONOMIST. ***The world's most valuable resource is no longer oil, but data***. 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 31. mar. 2021

UNESCO. **Marco de Avaliação Global da Alfabetização Midiática e Informacional: Disposição e Competências do País**. Brasília: UNESCO, Cetic.br, 2016. Disponível em https://nic.br/media/docs/publicacoes/8/246398POR.pdf. Acesso em: 21 abr. 2021.

VIOLA, Mario; HERINGER, Leonardo; COSTA, Janaina. ***Open Banking* e Proteção de Dados**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2020. Disponível em: https://itsrio.org/pt/publicacoes/open-banking-e-protecao-de-dados/. Acesso em: 24 abr. 2021.

VIOLA, Mario; THOMAZELLI, Patrícia. **Portabilidade de Dados, Interoperabilidade e *Open Banking***. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2021. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-portabilidade-de-dados-interoperabilidade-e-open-banking/. Acesso em: 17 abr. 2021.

PRATINI, Napala. ***An introduction to UK open banking***. 2019. Fin. Disponível em: https://fin.plaid.com/articles/an-introduction-to-uk-open-banking/. Acesso em: 26 abr. 2021.

SINGAPURA. SKINNER, Chris. ***DOING DIGITAL***. *Lessons from leaders*. Marshall Cavendish Business, Singapore, 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. ***The Right To Privacy***. *Harvard Law Review*. Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220. Disponível em: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C Acesso em: 28 abr. 2021.

Wikipedia. **OAuth**. Disponível em: https://pt.wikipedia.org/wiki/OAuth. Acesso em: 17 jun. 2021.

Wikipedia. **Web API**. Disponível em: https://pt.wikipedia.org/wiki/Web_API. Acesso em: 17 jun. 2021.

GARANTIAS CONTRATUAIS PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS NA AUSÊNCIA DE UMA DECISÃO DE ADEQUAÇÃO:

REGULAMENTAÇÃO COMO MECANISMO PARA EFETIVAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Dyemülly Christyna da Silva Pegos da Costa
Advogada e consultora em Soluções Jurídicas para Proteção de Dados, Pós-graduada em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito, Bacharela em Direito pelo UNIBRASIL
dyemully@dyemullypegos.com.br

RESUMO:
O presente artigo tem como objetivo explanar a respeito das hipóteses alternativas para transferência internacional de dados pessoais quando não há uma decisão de adequação reservada ao país destinatário do envio dos dados pessoais, uma vez que, diante do cenário tecnológico global, a necessidade de efetuar transferências internacionais de dados torna-se cada vez mais necessária, então, surge o questionamento a respeito de ser possível proteger os dados pessoais em tais transferências, em obstar as relações comerciais internacionais e estas questões que serão apontadas neste trabalho.

Palavras-Chave: Transferência internacional; Proteção de Dados; Autoridade Nacional de Proteção de Dados; Tecnologia; Relações comerciais.

Adequação; 4. Transferência Internacional Com Salvaguardas Especìficas; 4.1. Cláusulas Contratuais Específicas; 4.2. Cláusulas Padrão Contratuais; 4.3. Normas Corporativas Globais; 5. Conclusão; Referências Bibliográficas.

1. INTRODUÇÃO

Atualmente vivemos em uma nova era, a era da economia digital. Com o avanço tecnológico, todas as relações passaram a ter a informação como estrutura. E é nesse contexto que se faz necessária a reinvenção do Direito para regulamentar esse progresso social.

É incontroverso que o impacto da evolução tecnológica é muito amplo. Logo, deve ser imprescindível que as normas acompanhem essa transformação na mesma velocidade, assegurando que, as garantias e direitos dos indivíduos sejam preservados.

Neste ínterim a Lei Geral de Proteção de Dados – LGPD (13.709/20118), em vigor desde 18/09/2020, surge como um grande marco na legislação brasileira, pois possui como intuito controlar a circulação e proteger os dados pessoais, utilizando como molde o *General Data Protection Regulation – GDPR*, que se trata da legislação da União Europeia sobre proteção de dados pessoais e com base em qual a LGPD foi escrita.

A legislação de proteção de dados atinge todos os setores da sociedade, ou seja, qualquer pessoa física ou jurídica de direito público ou privado que, efetuar operações de tratamento de dados pessoais em território nacional ou que ofertar bens e serviços a pessoas que estejam no país, deverão observar os preceitos legais, para proteção dos direitos fundamentais de liberdade, privacidade e personalidade dos indivíduos, inclusive nas relações comerciais internacionais.

E considerando que, informação é a reunião de diversos tipos de dados e no cenário atual, há um grande tráfego de tais informações por todo o mundo, é fundamental que haja uma administração adequada e efetiva com base na legislação para que os dados pessoais não fiquem desprotegidos nas transferências internacionais em meio a esse grande avanço tecnológico.

Desta forma, é indispensável o estudo de mecanismos que possibilitem tais transferências internacionais de dados de forma segura, sem violação de direitos e sem interferir na economia global.

O presente artigo aborda a despeito das garantias contratuais que podem ser oferecidas quando há a necessidade extrema de uma transferência internacional para um país terceiro que não possui uma decisão de adequação. Para tanto, utiliza-se do direito comparado com base na metodologia qualitativa, abordando a prática executada pela Europa em situações análogas.

Portanto, serão feitos apontamentos sobre as transferências internacionais de dados na sociedade atual, em seguida passa-se a pontuar os requisitos de uma decisão de adequação e por fim analisa-se as salvaguardas contratuais positivadas pela lei que legitimam as hipóteses de transferência internacional para proteção dos dados pessoais no Brasil, possuindo, contudo, pontos pendentes de regulamentação pela Autoridade Nacional de Proteção de Dados – ANPD.

2. TRANSFERÊNCIA INTERNACIONAL – NOÇÕES E APONTAMENTOS

A tecnologia surge para facilitar, tanto a vida particular de cada indivíduo, quanto os negócios como um todo. Em meio a grandes transformações tecnológicas, o mundo se tornou palco de circulação de um enorme volume de informações.

Dentro de um ambiente digital, transportar dados de um continente para o outro tornou-se uma tarefa simples, onde a distância mais longa se resume a um clique.

Porém, juntamente com as facilidades do desenvolvimento tecnológico, surgem também diversos riscos da sociedade globalizada e um deles é com relação aos dados de pessoa natural, uma vez que, com o frenético fluxo de informações que vai e vem por todo o mundo, incorre em vulnerabilidades que os dados pessoais[1] certamente estão sujeitos.

Diante deste cenário, a regra geral da União Europeia - de onde vem a base da LGPD - é a proibição de toda e qualquer transferência de dados pessoais para fora do país onde está sendo efetuado o tratamento de dados[2], com o risco eminente de violação dos direitos fundamentais do titular[3] dos dados pessoais.

---

1 Dado Pessoal: É qualquer informação que possa identificar alguém. Pode ser tanto dados cadastrais como RG, CPF e endereço como também informações diversas como o restaurante que uma pessoa costuma frequentar ou uma marca de preferência, por exemplo.

2 Tratamento de dados: São todas as operações efetuadas com os dados pessoais dos titulares. Como a própria lei exemplifica: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3 Titular: É a própria pessoa natural, assim sendo, o indivíduo detentor dos

Todavia, é nítido que, para manter a economia global em movimento é necessário existir transferências transfronteiriças de dados, inclusive de dados pessoais.

Sendo assim, como é possível garantir a privacidade e proteção dos dados pessoais nessas idas e vindas de informações, sem comprometer as relações econômicas? Pois é sabido que nem todos os países possuem níveis de adequação necessários para tratar dados pessoais, muitas nações ainda não possuem sequer legislações que versem sobre proteção de dados.

As situações mencionadas acima contribuíram para que a União Europeia criasse critérios para transferência internacional de dados em casos específicos, os quais foram semelhantemente adotados pela LGPD em seu capítulo V. Contudo, vale lembrar que, tais hipóteses são admitidas desde que cumpridas as regras relativas a cada caso.

Antes de adentrar a explanação das circunstâncias em que é possível a transferência internacional de dados, vale elucidar o contexto em que ocorre esse tipo de tratamento de dados, bem como seu conceito técnico.

A transferência internacional de dados sucede quando é necessário enviar dados pessoais para fora do país. O nome em si já é autoexplicativo, no entanto, é importante distinguir a transferência internacional de dados de outros tipos de tratamentos, que por vezes podem ser confundidos, como seria o caso do trânsito de dados e o acesso de dados.

Nesse contexto, explica Luis Fernando Prado Chaves que:

---

dados pessoais.

> O primeiro ponto importante é entender que, pautando-se no melhor entendimento europeu sobre o tema, um simples acesso à aplicação de internet[4] não deve ser considerado uma transferência internacional de dados, sob pena de se banalizar a aplicação do conceito e transformar o regime internacional em geral, o que poderia culminar, inclusive, em uma potencial situação de desarmonia com as bases legais do artigo 7º da LGPD. Ademais, como nos recorda o *Information Commissioners's Office ("ICO")*, autoridade de proteção de dados do Reino Unido, não se deve confundir transferência de dados com trânsito de dados. Isso significa dizer, por exemplo, que, se para viabilizar a troca de e-mails entre diferentes áreas de uma organização 100% brasileira (no contexto de um tratamento de dados pessoais sujeito à LGPD), por uma questão meramente de infraestrutura tecnológica, dados pessoais transitam momentaneamente por um servidor localizado na Índia, tal atividade, por si só, não deveria ser considerada uma transferência internacional de dados àquele país. (CHAVES, 2019. p. 295).

Sendo pontuada essa diferenciação de conceitos e seguindo as diretrizes de extraterritorialidade das leis de proteção de dados, é correto afirmar que uma transferência internacional só pode ocorrer nas hipóteses previstas em lei, de forma taxativa, com observância estrita dos critérios específicos para que o país receptor possa manter a proteção dos dados pessoais, tal qual como no país de origem.

Para melhor entendimento, exemplificando de forma prática uma situação em que ocorre uma transferência internacional de dados, seria quando uma empresa que possui matriz no exterior envia informações de funcionários para uma eventual prestação de contas.

---

4 Nos termos do art 5º, VII da Lei Federal 12.965/2014 ("Marco Civil da Internet"), devemos considerar "aplicação de internet" como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

Ao enviar estes dados pessoais para fora do país de tratamento, a empresa está efetuando uma transferência internacional de dados, porque apesar das duas empresas fazerem parte do mesmo grupo econômico, estão fisicamente em países distintos, logo é essencial a aplicação dos critérios que garantam a proteção dos dados pessoais transferidos.

Este cenário é apenas um exemplo de todas as possibilidades que podem configurar uma transferência internacional de dados. Sendo assim, é indispensável seguir à risca os preceitos da legislação para que não sobrevenha violação dos direitos dos titulares, inclusive com relação às transferências internacionais ulteriores, sob pena de invalidar todas as medidas de segurança tomadas no primeiro momento. Nos termos do art. 44 do GDPR,5 observa-se que

> Artigo 44. Princípio geral das transferências
> Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento (UNIÃO EUROPEIA, 2016).

Ou seja, os agentes de tratamento[5] devem garantir que ao efetuar uma transferência internacional de dados, o padrão de proteção dos dados pessoais deve permanecer inabalável. Não se

5 Agentes de tratamento: São as pessoas físicas ou jurídicas que tratam os dados pessoais de titulares, ou seja, realizam operações com os dados pessoais.

olvidando que, prezando pelo princípio da transparência, devem sempre informar os titulares para onde estão sendo enviados seus dados pessoais, bem como seus direitos e formas de exercê-los.

3. TRANSFERÊNCIA INTERNACIONAL POR DECISÃO DE ADEQUAÇÃO

A Lei Geral de Proteção de Dados em seu artigo 33, dispõe que a transferência internacional de dados só será permitida nos casos ali previstos. A primeira hipótese de anuência, para esse tipo de tratamento, está preceituada no inciso I do referido artigo, sendo a possibilidade de transferência internacional para países ou organismos internacionais que demonstrem grau de proteção de dados pessoais suficiente e assim "garantir ao titular de dados, que possui dados tratados no âmbito da LGPD, a mesma proteção e zelo que lhe são garantidos pela legislação brasileira" (GODOY, 2020, p. 402). À vista disso:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL. Lei 13.709, 2018);

Ao analisar os critérios para decisão de adequação é imperioso não efetuar apenas "uma análise fria e textual da legislação de proteção de dados do país terceiro, mas deverá observar, especialmente, se tal país possui meios efetivos (enforcement) para tornar eficaz o regime legal instituído" (CHAVES, 2019, p. 306).

Em outras palavras, a LGPD autoriza a livre transferência de dados pessoais à países que possuírem grau de adequação reconhecido pela Autoridade Nacional de Proteção de Dados – ANPD, desde que observados os pressupostos legais, bem como demonstrarem de forma efetiva tais pressupostos. Os requisitos para reco-

nhecimento do nível de adequação estão preceituados no artigo 34 da lei.

Semelhantemente como na União Europeia, com a *adequacy decision*, os critérios de avaliação aduzidos na lei brasileira, levam em consideração se o país ou organismo internacional destinatário do dado pessoal oferece um nível adequado de proteção de dados em seu território. A avaliação é efetuada por meio de análise das normas em vigor, observância dos princípios e direito dos titulares, bem como fornecimento de garantias e adoção de medidas de segurança que resguardem a proteção dos dados pessoais, além da verificação da natureza dos dados da transferência internacional e demais circunstâncias específicas (BRASIL. Lei 13.709, 2018).

Após a avaliação dos requisitos pela ANPD e sendo o país terceiro ou organismo internacional apto, de acordo com os critérios necessários, então será legitimada a livre circulação de dados entre o Brasil e tal país ou organismo internacional, por meio de uma decisão de adequação, sendo essas decisões "benéficas à economia, pois reduzem consideravelmente o valor das transações para as companhias, gerando oportunidade de criação de novos negócios e parceiros comerciais" (GODOY, 2020, p.404), não necessitando de nenhum requisito adicional, assim como ocorre na União Europeia.

Neste ínterim, à luz do artigo 45 do GDPR, a Comissão Europeia já havia reconhecido doze países como adequados, para livre circulação de dados pessoais, sendo eles: Andorra, Argentina, Canadá (para fins comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça e Uruguai. Recentemente a Comissão Europeia avaliou a Coreia do Sul e o Reino Unido, concluindo que estes também garantem um nível de proteção essencialmente equivalente ao garantido pelo GDPR (European Comis-

sion: Adequacy decision, 2021).

Além dos países com decisão de adequação, o livre trânsito de dados pessoais também ocorre no Espaço Econômico Europeu - *European Economic Area (EEA)*, que é formado pelos Estados-Membros da União Europeia, Islândia, Liechtenstein e Noruega.

É ainda basilar pontuar que, na Europa, após a decisão de adequação, a Comissão Europeia acompanha o país adequado de quatro em quatro anos no mínimo, para verificar se o país terceiro continua oferecendo o nível adequado de proteção de dados, podendo revogar, alterar ou suspender a decisão de adequação, conforme o artigo 45, do GDPR:

> [...] 3. Após avaliar a adequação do nível de proteção, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.o 2 do presente artigo. O ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional.
> [...]
> 5. A Comissão, sempre que a informação disponível revelar, nomeadamente na sequência da revisão a que se refere o n.o 3 do presente artigo, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, deixou de assegurar um nível de proteção adequado na aceção do n.o 2 do presente artigo, na medida do necessário, revoga, altera ou suspende a decisão referida no n.o 3 do presente artigo, através de atos de execução, sem efeitos retroativos. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.o, n.o 2 (UNIÃO EUROPEIA, 2016).

E essa é uma das questões que a ANPD precisará regulamentar no Brasil, uma vez que, ao contrário do GDPR, não há na LGPD previsão de que a decisão de adequação poderá ser alterada, revo-

gada ou suspensa, caso o país chancelado se mostre omisso com a perpetuação de medidas que garantam a proteção de dados. De acordo com Luis Fernando Prado Chaves:

> Neste ponto, em homenagem ao princípio da legalidade que rege os atos praticados pelos entes da Administração Pública e considerando que os critérios aqui examinados estão atrelados a elementos dinâmicos e mutáveis, seria extremamente importante que a ANPD contasse com subsídio legal para revisar ou mesmo revogar suas decisões de adequação, tal como previsto no direito europeu e de forma similar ao previsto no artigo 35, §4º, da própria LGPD. (CHAVES, 2019. p. 306).

Além da recomendação apontada pelo autor, seria também fundamental o investimento na conscientização da população e das empresas, para que seja efetivada a cultura da proteção de dados pessoais no Brasil e assim, contribuir que o país possa proporcionar o grau de proteção apropriado aos dados pessoais, mediante os critérios do direito europeu, cominando para que no futuro possa integrar a lista de países que receberam a decisão de adequação da Comissão Europeia, consubstanciando para a livre circulação de dados de forma segura.

E ainda segundo Bruna Michele Wozne Godoy:

> Atualmente a transferência internacional de dados pessoais ocorre em uma escala massiva e constante, empresas e países que enfrentam restrições para executá-las definitivamente sofrerão danos significativos em diversas esferas. Em um mundo globalizado, em que o mercado único digital elimina fronteiras e conecta pessoas e negócios em todo o mundo, obter uma autorização que permita o livre fluxo de dados pessoais entre as economias mais importantes do mundo, como a União Europeia e os Estados Unidos, é um diferencial competitivo elementar (GODOY, 2020. p. 306).

A despeito disso, uma decisão de adequação da Comissão Europeia destinada ao Brasil, seria uma grande alavanca para econo-

mia brasileira, por conta do estreitamento das relações políticas já existentes com a União Europeia.

O livre trânsito de dados com toda a certeza reforçaria o vínculo de cooperação econômico-comercial, contudo, para que o Brasil esteja apto a alcançar uma decisão de adequação europeia, ainda há um grande caminho a ser percorrido, tendo em vista os rigorosos critérios para tanto.

Enquanto esse patamar não é atingido, as transferências internacionais advindas da União Europeia só podem ser concretizadas por meio das demais hipóteses trazidas pelo direito europeu, as quais analogamente também estão elencadas no art. 33 da LGPD, e serão abordadas sucessivamente no presente trabalho.

> Uma preocupação inerente à hipótese trazida pelo inciso em referência está no tempo que a ANPD tomará para decidir sobre o nível de adequação de cada país. Na Europa, um dos fatores muito criticados é o tempo que se toma para que seja adotada a decisão de adequação, o que acaba por representar impacto às relações comerciais entre os países. Portanto, a celeridade para decidir sobre o nível de adequação de países terceiros deve ser uma das preocupações da ANPD, de forma a evitar o atravancamento do fluxo internacional de dados - essencial para o avanço da tecnologia e da economia moderna. (CHAVES, 2019, p. 297).

Com base nos apontamentos do autor, conclui-se que a celeridade é um dos fatores primordiais para que a proteção de dados possa ser assegurada nas transferências internacionais, sem prejudicar a economia digital global.

4. TRANSFERÊNCIA INTERNACIONAL COM GARANTIAS ESPECÍFICAS

Além da hipótese de permissão para transferência internacional de dados por meio de uma decisão de adequação, prevista no inciso I do art. 33 da LGPD, alternativamente o legislador brasileiro disciplinou no inciso II do mesmo artigo, hipóteses onde o agente de tratamento pode oferecer a comprovação de salvaguardas contratuais a fim de garantir a proteção dos dados pessoais, objeto das transferências internacionais.

Isto posto, se o país destinatário ainda não possuir decisão de adequação, ainda assim, a transferência internacional de dados pessoais poderá ser concretizada, desde que, o agente de tratamento possa ofertar e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados consig-nados e previstos na LGPD

> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos (BRASIL. Lei 13.709, 2018).

O oferecimento de comprovação de garantias por meio do disposto acima é aplicável a qualquer país ou organismo internacional e deverão seguir as especificações técnicas, avaliação e aprovação da ANPD, conforme disciplinado no art. 35 e 36 da LGPD para que haja observância dos direitos, garantias e os princípios da lei.

> 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.
> Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade naci-onal (BRASIL. Lei 13.709, 2018).

Como não poderia ser diferente, o GDPR também estabelece em seu artigo 46 (UNIÃO EUROPEIA, 2016) mecanismos de garantia para transferência de dados para países terceiros, por intermédio de cláusulas, regras, códigos de conduta e certificados, servindo como inspiração para o inciso II, do artigo 33 da LGPD.

Assim como no tópico anterior "de maneira geral, uma das inerentes e principais preocupações sobre as garantias previstas nesse inciso diz respeito ao tempo que a ANPD tomará para editar o teor das cláusulas" (CHAVES, 2019, p. 299).

4.1. CLÁUSULAS CONTRATUAIS ESPECÍFICAS

As cláusulas contratuais específicas para determinada transferência, descrita na alínea "a" do inciso II do artigo 33 da LGPD é destinada para os casos isolados em que necessite de uma transferência internacional de dados pessoais.

Nestes casos são feitos ajustes de forma exclusiva para aquela transferência internacional. Um exemplo prático a ser abordado seria no caso em que, uma empresa que trata dados pessoais se depara com uma instabilidade técnica em seu servidor habitual e por conta disso, necessita transferir esses dados de forma temporária para outro servidor a fim de preservar a integridade dos dados e esse servidor alternativo encontra-se em um país terceiro, que não possui decisão de adequação brasileira, por isso, nessa situação podem ser utilizadas as cláusulas contratuais específicas.

Neste cenário, é então firmado um contrato entre os agentes de tratamento, consignando em cláusulas (a serem aprovadas pela autoridade de proteção de dados), as responsabilidades de cada parte, detalhamento da transferência e categoria de dados, sempre levando em consideração os princípios da legislação, bem como a observância dos direitos dos titulares, com garantia efetiva da proteção dos dados pessoais e privacidade.

4.2. CLÁUSULAS-PADRÃO CONTRATUAIS

As cláusulas-padrão contratuais da alínea "b" do inciso II do art. 33 da LGPD, são inspiradas nas cláusulas-tipo disciplinadas no artigo 46, 2 "c" do GDPR, mais co-nhecidas por *SCCs – Stantard contractual clauses* (UNIÃO EUROPEIA, 2016).

As SCCs são cláusulas-tipo que devem ser incluídas nos contratos entre agentes de tratamento, quando estes desejam enviar dados de um país para o outro. Estas cláusulas são indicadas para transferências internacionais de dados pessoais, que ocorrem repetidamente, geralmente entre partes que já possuem outros acordos comerciais.

Nesta esteira, objetivando garantir a proteção adequada aos dados pessoais presentes nas transferências, então deve-se adicionar as cláusulas-padrão contratuais como salvaguarda.

Nos termos do GDPR, as SCCs são utilizadas quando o agente de tratamento que irá transferir os dados pessoais está localizado na União Europeia e/ou no Espaço Econômico Europeu (EEE) e o destinatário dos dados está localizado em um país terceiro fora do Espaço Econômico Europeu (EEE) ou que não possua uma adequacy decision.

Nestes casos o agente de tratamento receptor dos dados pessoais deve concordar não só em receber os dados pessoais, mas também a cumprir com todos os termos consignados nas cláusulas-padrão contratuais.

A Comissão Europeia disponibiliza modelos de cláusulas-tipo de modo a auxiliar os agentes de tratamento, uma vez que tais modelos são "pré-aprovados" pela Comissão Europeia e se forem seguidos precisamente amparam a autorização para transferência internacional.

No Brasil, ainda não há regulamentação a respeito das cláusulas-padrão contratuais, mas seguindo as práticas da Comissão Europeia as quais possuem tendências de serem utilizadas pela ANPD como referência e/ou boas práticas (a exemplo de como vem sendo feito com outros temas), é possível observar diver-

sos requisitos inerentes a tais cláusulas contratuais adotados na prática.

A Comissão Europeia emitiu novas cláusulas contratuais padrão para transferências internacionais de dados de países da União Europeia e/ou Espaço Econômico Europeu (EEE) para países que estão fora da União Europeia e/ou Espaço Econômico Europeu (EEE), por meio da decisão de implementação nº 2021/914 de 04 de junho de 2021 da Comissão Europeia, atualizadas no âmbito do GDPR após o caso SCHREMS II.[6]

As novas *Standard Contractual Clauses (SCCs)* substituem os três conjuntos de SCCs que foram elaboradas de acordo com a Diretiva de Proteção de Dados 95/46, possuindo validade somente até 21 de setembro de 2021. As novas cláusulas são destinadas aos contratos entre controlador[7] - operador[8] e controlador - controlador e como se trata de "modelos" pré-aprovados pela Comissão Europeia, não são passíveis de alterações textuais, muito embora seja possível acrescentar no contrato outras cláusulas contratuais ou garantias adicionais, desde que não entrem em conflito direta ou indiretamente com as SCCs.

As cláusulas-padrão contratuais é a forma mais utilizada para legitimar as transferências internacionais de dados para países que não são considerados minimamente adequados. A decisão 2021/914 assim como sua antecessora, vincula todos os Estados-Membros da União Europeia, os quais, por conseguinte devem cumprir o previsto, inclusive as considerações, que são de extrema

6 SCHREMS II foi uma ação judicial interposta por Max Schrems, que questionava a vulnerabilidade da proteção dos dados pessoais transferidos aos EUA.
7 Controlador: É a pessoa física ou jurídica que realiza tratamento de dados pessoais dos titulares decidindo a forma como será feito.
8 Operador: É a pessoa física ou jurídica que trata os dados dos titulares em nome do controlador.

relevância e norteiam a legitimidade das transferências internacionais efetuadas por meio de cláusulas-padrão contratuais.

Tendo em vista que a evolução tecnológica facilitou e muito o fluxo de dados é fundamental que a Comissão Europeia assegure que, o nível de proteção que o GDPR oferece aos titulares, não seja comprometido quando os dados pessoais destes são transferidos para países terceiros, inclusive em transferências ulteriores.

Por este motivo, é determinado que os agentes de tratamento se certifiquem, antes de efetuarem a transferência internacional que, o país destinatário possa oferecer as garantias adequadas, bem como observem os direitos dos titulares, uma vez que as cláusulas-padrão contratuais são destinadas apenas às partes, não vinculando as autoridades do país para onde os dados serão enviados.

Os agentes de tratamento devem informar aos titulares a respeito de todas as transferências internacionais efetuadas, bem como lhes fornecerem uma cópia das cláusulas-padrão contratuais indicando quais categorias dos seus dados pessoais tra-tados foram transferidos para o exterior, respeitando o princípio da transparência, além de assegurar que os titulares possam exercer seus direitos como terceiros beneficiários.

As cláusulas-padrão contratuais elaboradas pela Comissão Europeia são compostas por cláusulas gerais e divididas em módulos, para contemplar diversos contextos de transferências, devendo os agentes de tratamento selecionar o módulo que melhor se aplica ao caso concreto.

Como se trata de uma relação contratual, cada parte, tanto o agente de tratamento exportador dos dados (que está em um

país pertencente à UE e/ou EEE), quanto o agente de tratamento importador dos dados (país fora da EU e/ou EEE) devem cumprir com as obrigações inerentes a cada um.

Nas cláusulas devem estar previstas regras com relação à responsabilidade, no caso de o titular sofrer danos em decorrência de qualquer violação dos seus direitos. Nestas situações, como terceiro beneficiário, o titular terá direito à indenização em face dos agentes de tratamento.

Assim como o agente de tratamento exportador dos dados, em observância do GDPR, o agente importador de dados deve disponibilizar todas as informações que possam demonstrar o cumprimento das cláusulas padrão contratuais, inclusive colaborar para que seja realizada auditorias de suas operações de tratamento pelo agente de tratamento exportador de dados.

Nos casos de necessidade de transferências ulteriores ao contrato, ou seja, para um novo agente de tratamento é preciso a autorização do agente de tratamento exportador dos dados, nos termos do artigo 28 do GDPR, para que este se certifique que o nível de proteção previsto nas cláusulas continuará sendo assegurado.

Os agentes de tratamento devem obrigatoriamente manter registros das atividades de tratamento sob sua responsabilidade, igualmente o importador de dados e caso não haja cumprimento das cláusulas, o exportador de dados deve ser informado para que suspenda a transferência e até rescinda o contrato, porque é imprescindível que todas as cláusulas sejam cumpridas em sua integralidade, sem prejuízo de aplicação de regras específicas da legislação em caso de descumprimento.

Imperioso destacar que, antes da transferência é necessário que o agente exportador dos dados verifique se o importador dos dados pode ser impedido de cuprir com as cláusulas contratuais diante da legislação local do país terceiro, tendo em vista a não vinculação destas. Caso haja disposições contrárias ao cumprimento do contrato, a transferência internacional não deve ser realizada, conforme pontua a decisão da Comissão Europeia:

> As partes devem ter em conta, em especial, as circunstâncias específicas da transferência (como o conteúdo e a duração do contrato, a natureza dos dados a transferir, o tipo de destinatário, a finalidade do tratamento), as legislações e as práticas do país terceiro de destino pertinentes à luz das circunstâncias da transferência e quaisquer garantias aplicadas para complementar as garantias previstas nas cláusulas contratuais-tipo (incluindo as medidas contratuais, técnicas e organizativas pertinentes aplicáveis à transmissão dos dados pessoais e ao seu tratamento no país de destino).(COMISSÃO EURO-PEIA, 2021, p. 36).

As cláusulas padrão contratuais devem prever que, se após a assinatura do contrato o importador dos dados não puder cumprir com as cláusulas consignadas, além da notificação imediata do exportador dos dados, também a previsão das medidas que serão tomadas a partir de então, bem como a notificação da autoridade de proteção de dados acerca do ocorrido.

A decisão 20121/914 ainda abordou que, as cláusulas-tipo elaboradas com base na Diretiva 95/46 podem ser utilizadas até 26 de setembro de 2021 e os contratos celebrados até esta data possuem vigência até 27 de dezembro de 2022, “desde que as operações de tratamento objeto do contrato permaneçam inalteradas e que o recurso a essas cláusulas garanta que a transferência de dados pessoais está sujeita a garantias adequadas” (COMISSÃO EUROPEIA, 2021, p 36).

Embora as cláusulas-padrão contratuais requeiram salvaguardas específicas para transferências internacionais, a sua eficácia na proteção dos dados pessoais ainda é questionada, como ocorreu no caso Scherms II, onde foi levantado que a validade das cláusulas-padrão contratuais não seria absoluta e dependeria das práticas do país terceiro com relação à privacidade e proteção de dados, sendo imperioso a análise precisa dos agentes de tratamento à respeito de todas essas questões, sob pena de violar os direitos dos titulares.

Para fins práticos, as cláusulas-padrão contratuais de maneira geral devem versar sobre:

- Finalidade e âmbito de aplicação;
- Efeito e invariabilidade das cláusulas;
- Terceiro beneficiário;
- Interpretação dos termos técnicos;
- Hierarquia contratual;
- Descrição pormenorizada das transferências;
- Cláusula de adesão;
- Garantias (limitações das finalidades, transparência, exatidão e minimização dos dados, limitação da conservação, segurança do tratamento, dados sensíveis, transferências ulteriores, documentação, cumprimento/descumprimento);
- Autorizações para transferências posteriores;
- Direito dos titulares;
- Canal de comunicação dos titulares;
- Responsabilidades;
- Controle das transferências efetuadas;
- Legislação e práticas locais que afetam o cumprimento das cláusulas;
- Obrigações do importador de dados em caso de acesso por parte de autoridades públicas;
- Descumprimento contratual e rescisão;

- Direito aplicável;
- Eleição de foro e jurisdição;
- E demais cláusulas facultativas adicionais.

No Brasil "é de se imaginar que a ANPD disciplinará o conteúdo mínimo das cláusulas relativas à transferência internacional de dados" (CHAVES, 2019, p. 298), sobre a premissa de que as cláusulas-padrão contratuais podem oferecer um grau adequado de proteção dos dados pessoais nas transferências internacionais desde que cumpridas rigorosamente pelos agentes de tratamento, bem como que não haja qualquer incompatibilidade com a legislação local do país terceiro para onde serão enviados tais dados pessoais.

4.3. NORMAS CORPORATIVAS GLOBAIS

No artigo 33, II, "c", estão previstas as normas corporativas globais, que por sua vez, são indicadas para transferências internacionais que ocorrem dentro de um ambiente corporativo B2B *(bussiness-to-bussiness)*.

Assim como no caso das cláusulas-padrão contratuais e das cláusulas específicas, as normas corporativas globais são mecanismos de garantia da proteção de dados pessoais, quando o país terceiro receptor dos dados não possui uma decisão de adequação.

As normas corporativas globais são regras a serem seguidas por empresas que desejam transferir dados dentro de uma corporação ou grupo empresarial, mas que as empresas em si estejam fisicamente em países distintos. Estas normas possuem correspondência no direito europeu com as regras corporativas vinculantes aplicáveis às empresas, as *binding corporate rules ("BCR")*, descritas no artigo 47 do GDPR (UNIÃO EUROPEIA, 2016). "Por lá, as BCRs são pensadas para multinacionais (transferência de dados

entre empresas do mesmo grupo), grupos de franquias e *joint ventures*, por exemplo, e devem passar por aprovação prévia da autoridade europeia" (CHAVES, 2019, p. 299).

Na definição de Thiago Luís Santos Sombra:

> As normas corporativas *vinculantes* ou *binding corporate rules (BCRs)* destinam-se a permitir que empresas multinacionais transfiram dados pessoais da União Europeia para os seus afiliados localizados fora do bloco. As BCRs promovem a adoção de padrões globais sobre proteção de dados e privacidade, bem como aumenta a conscientização dentro da organização (SOM-BRA, 2019, p. 131).

Na Europa, também como forma de auxiliar os agentes de tratamento, é disponibilizado pelo *European Data Protection Board (EDPB) guidelines* (orientações) sobre as BCRs, com o intuito de esclarecer a respeito do conteúdo mínimo esperado. "Mais uma vez, espera-se que a ANPD se aproveite das orientações europeias para estruturação das normas corporativas globais, seguindo, portanto, o padrão preten-dido pelo legislador brasileiro" (CHAVES, 2019, p. 299).

O GDPR traz ao longo do art. 47, prevê requisitos que devem estar presentes nas BCRs para serem aprovadas pela autoridade de proteção de dados.

As regras devem ser juridicamente vinculativas interna/externamente e aplicáveis a todas as empresas do grupo empresarial ou corporação, por meio de contrato específico nos moldes do artigo 28 do GDPR, incluindo os funcionários das empresas, os quais deverão garantir o cumprimento integral das normas, conferindo expressamente os direitos dos titulares dos dados pessoais tratados. Além disso deve (UNIÃO EUROPEIA, 2016):

• Constar a estrutura do grupo empresarial, bem como seus parceiros de negócios;
• Descrever as transferências, indicando as categorias dos dados pesso-ais tratados, o tipo de tratamento, finalidade, os tipos de titulares afetados, identificação dos países que receberão a transferência;
• Constar a necessidade de aplicação dos princípios gerais de proteção de dados, finalidade, minimização dos dados, limitação dos prazos de conservação, qualidade dos dados, p*rivacy by desgin*, *privacy by default*, bases legais, tratamento de categorias especiais de dados, medidas de garantia e segurança dos dados, bem com os requisitos para transferências posteriores;
• Indicar todos os direitos dos titulares e a forma de exercícios de tais direitos, inclusive o direito de não ser objeto de decisões automatizadas (incluído definição de perfis), o direito de apresentar reclamação às autoridades competentes de proteção de dados e tribunais como terceiro beneficiário com direito à indenização e/ou reparação pela violação das regras vinculativas apli-cáveis às empresas;
• A responsabilização do agente exportador dos dados pessoais por toda e qualquer violação das BCRs por uma entidade terceira envolvida, com exoneração de tal responsabilidade somente por meio de prova de que o fato que causou o dano não é imputável à referida entidade;
• Constar a forma de comunicação com os titulares para informar a respeito das transferências;
• Indicar as funções do responsável por fazer cumprir as BCRs a nível do grupo empresarial e não apenas do agente de tratamento;
• Apresentar os procedimentos de reclamação;
• Descrever os procedimentos existentes no grupo empresarial, incluindo auditorias (devendo o resultado ser enviado à autoridade de proteção de dados) e a efetivação de medidas que assegurem a proteção dos dados dos titulares;

• Descrever os procedimentos de elaboração de relatórios e registros, caso haja descumprimento ou alteração das regras;
• Descrever os procedimentos de cooperação com a autoridade de proteção de dados, atendendo aos eventuais pedidos desta;
• Descrever os procedimentos de comunicação com a autoridade de pro-teção e dados, de todos os critérios legais que o agente de tratamento importador de dados estiver sujeito no território do país terceiro que sejam passíveis de comprometimento as salvaguardas oferecidas pelas BCRs;
• Indicar orientações a todos que tenham acesso aos dados pessoais.

Este tipo de norma visa facilitar as relações comerciais ao redor do mundo, porém, assim como todas as outras garantias, é imprescindível que os agentes de tratamento avaliem se o país terceiro respeitará tais regras, determinando se os direitos dos titulares realmente serão cumpridos na prática, e se for o caso, utilizar-se de salvaguardas adicionais para garantir o nível de proteção adequado.

É preciso ainda reforçar que, a exemplo das outras garantias, as normas corporativas globais, também devem ser aprovadas previamente pela autoridade de proteção de dados.

5. CONCLUSÃO

Conforme explanado no presente artigo, o acelerado avanço da tecnologia acarreta também um elevado fluxo internacional de dados envolvendo países diversos. No entanto é sabido que nem todas as nações possuem grau ideal de adequação à proteção de dados, criando-se assim o risco iminente de incidentes e consequente violação dos direitos dos titulares.

O trabalho buscou demonstrar que, o correto seria que, nenhum dado pessoal fosse transferido para fora de seu país de origem. Todavia, tendo em vista que uma proibição de transferência internacional causaria um grande impacto na economia mundial, tanto a legislação Europeia, com o *General Data Protection Regulation – GDPR*, quanto a Lei Geral de Proteção de Dados – LGPD dispõem acerca de hipóteses em que é possível a transferência internacional de dados pessoais, quando estritamente necessárias, respeitando os preceitos legais.

Desta feita, conforme discorrido, o processo de obtenção de uma decisão de adequação por um país terceiro tende a ser moroso, porém com o oferecimento de salvaguardas específicas, observando as disposições da lei e após regulamentação da autoridade de proteção de dados, é possível garantir a expectativa de proteção dos dados pessoais nas transferências internacionais, sem obstar a realização de negócios transfronteiriços e sem interferências na economia global.

Deste modo, a exemplo das cláusulas contratuais específicas, cláusulas padrão contratuais e normas corporativas globais consistem em garantias contratuais que podem ser oferecidas em nome da proteção dos dados pessoais de maneira eficaz.

Porém, embora haja previsão na legislação, é imperioso que os agentes de tratamento possam analisar cada caso de maneira personalizada, tomando os devidos cuidados para que não haja qualquer indício de vulnerabilidade na proteção dos dados pessoais, bem como, respeitando a análise e aprovação prévia da autoridade de proteção de dados.

A proteção dos dados pessoais deve ser efetivada em todas as operações de tratamento, garantindo assim a efetivação dos direitos dos titulares.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei 13. 709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF, 15 de agosto de 2018 e modificações 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 07 ago. 2021.

CARVALHO, Angelo Gamba Prata. **Transferência Internacional de dados na Lei Geral de Proteção de Dados – Força normativa e efetividade diante do cenário transnacional**. In: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). Lei Geral de Proteção de Dados Pessoais: e suas repercussões no Direito brasileiro. 2. Ed. São Paulo: Thomson Reuters, 2019. p. 615-658.

CHAVES, Luis Fernando Prado. **Da Transferência Internacional e Dados**. In: MALDONADO, Viviane Nóbrega (Coord); OPICE BLUM, Renato. LGPD: Lei Geral de Proteção de Dados Comentada. 2. Ed. São Paulo: Thomson Reuters, 2019. p. 291-308

COMISSÃO EUROPEIA. ***Adequacy decision***. Disponível em https://ec.eu-ropa.eu/info/law/law-topic/data-protection/international--dimension-data-protec-tion/adequacy-decisions_en. Acesso em: 09 ago. de 2021.

COMISSÃO EUROPEIA. **Decisão de Execução (UE) 2021/914** da comissão de 4 de junho de 202. Disponível em https://eur-lex.europa.eu/legal-con-tent/PT/TXT/PDF/?uri=CELEX:32021D0914&-from=EN. Acesso em: 09 ago. de 2021.

GODOY, Bruna Michele Wozne, ***Privacy Shield* EUA x Brasil: é possível?** In PALHARES, FELIPE (coord). Temas atuais de proteção de dados. São Paulo: Thomson Reuters, 2020. p. 401-418.

SOMBRA, THIAGO LUÍS SANTOS. **Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva**. São Paulo: Thomson Reuters, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho** - *General Data Protection Regulation (GDPR)*. Disponível em https://eur-lex.europa.eu/legal-content/PT-EN/TXT/?from=EN&uri=CE-LEX%3A32016R0679. Acesso em: 09 ago. de 2021.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: PROCESSO PARA A GESTÃO DE RISCOS

DATA PROTECTION IMPACT ASSESSMENT: PROCESS FOR RISK MANAGEMENT

Jean Carlo Jacichen Luz
Advogado. *Certified Information Privacy Manager (CIPM)* pela *International Association of Privacy Professionals (IAPP)*. Certificado *Privacy and Data Protection Foundation e Essentials e Information Security Foundation* pela EXIN. Pós graduado em Direito Administrativo e Processual Civil. Bacharel em Direito pela PUC/PR.

RESUMO:
Embora a LGPD tenha instituído um regime jurídico complexo, com potencial de atingir todo e qualquer segmento econômico, não havendo fórmula única para o compliance, em seu núcleo pode ser identificada a governança da proteção de dados pessoais. Isto significa que o foco da LGPD está na proteção dos direitos e liberdades dos titulares de dados, que podem ser consumidores, pacientes, usuários de serviços ou mesmo colaboradores. Nesse sentido, a presente pesquisa buscou abordar a LGPD na complexidade das operações de tratamento de dados, a qual demanda uma abordagem baseada no risco e torna flexíveis as obrigações dos agentes conforme o risco representado aos titulares. Dentre estas obrigações figura o relatório de impacto à proteção de dados pessoais, cuja falta de definições na lei brasileira torna ainda mais necessário o estudo da experiência estrangeira sobre o assunto, especialmente considerando a inspiração direta no modelo regulatório europeu. Para tanto, utilizou-se o método de abordagem hipotético-dedutivo e a técnica de pesquisa docu-

mental indireta através de levantamento de legislação, doutrina e recomendações de autoridades nacionais e estrangeiras. Os resultados apontaram que o RIPD é, para além de obrigação legal, um instrumento de gestão de riscos e boa prática para auxiliar estar em conformidade com a lei, e as origens da LGPD possibilitam aprender com as práticas estrangeiras consolidadas.

Palavras-Chave: Privacidade. Dado pessoal. Relatório de impacto à proteção de dados. Risco.

ABSTRACT:
Although the LGPD has instituted a complex legal regime, with the potential to reach any and every economic segment, with no one-size-fits-all formula for compliance, at its core can be found the governance of personal data protection. This means that the LGPD's focus is on protecting the rights and freedoms of data subjects, who may be consumers, patients, service users or even collaborators. In this sense, this research sought to address the LGPD in the complexity of data processing operations, which demands a risk-based approach and makes agents' obligations flexible according to the risk represented to the data subjects. Among these obligations is the data protection impact assessment, whose lack of definitions in brazilian law makes it even more necessary to study foreign experience on the subject, especially considering the direct inspiration in the european regulatory model. For that, the method of hypothetical-deductive approach and the technique of indirect documentary research were used,

through a survey of legislation, doctrine and recommendations from national and foreign authorities. The results showed that the RIPD is, in addition to a legal obligation, a risk management instrument and good practice to help comply with the law, and the origins of the LGPD make it possible to learn from consolidated foreign practices.

Keywords: *Privacy. Personal data. Data Protection Impact Assessment. Risk.*

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD), acompanhando transformações sentidas a nível global, inaugura relevante marco legal no Brasil ao instituir um regime jurídico às operações de tratamento de dados pessoais, capaz de afetar todo e qualquer segmento de mercado e mesmo o Poder Público[1].

Em outras palavras, a LGPD estabelece as regras do jogo para tudo que é feito com informações que possam identificar pes-

1 A abrangência da aplicação da lei deve-se aos conceitos amplos de dado pessoal e tratamento, previstos no artigo 5º, incisos I e X, da LGPD, respectivamente: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; X - 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.

soas físicas, denominadas titulares de dados, verdadeiro foco de proteção do sistema.

A inspiração para a estrutura deste novo regime jurídico origina-se diretamente do modelo estabelecido pelo regulamento europeu de proteção de dados, conhecido *General Data Protection Regulation (GDPR)* ou Regulamento Geral sobre a Proteção de Dados (RGPD), no português de Portugal.

Dentre as inúmeras inovações deste marco, cada uma com relevantes impactos e desdobramentos, este artigo ocupar-se-á, por meio da análise teórica e prática, do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento que se presta à análise de riscos e que pode se revelar de extrema utilidade a um programa de governança em privacidade e proteção de dados bem como para incutir o ideal de *privacy by design* nas práticas organizacionais, corrigindo o curso do desenvolvimento de novos projetos desde o seu princípio.

A premissa fundamental deste sistema é o reconhecimento da proteção de dados como um direito fundamental[2], constituindo o objetivo da legislação a proteção da pessoa em relação ao tratamento de seus dados pessoais.

Em relação a metodologia, se utilizou-se do método de abordagem hipotético-dedutivo e a técnica de pesquisa documental indireta, com levantamento bibliográfico de legislação, doutrina e recomendações de autoridades nacionais e europeias, analisando

2 O direito à proteção de dados está expresso na Carta de Direitos Fundamentais da União Europeia. No Brasil, houve este reconhecimento pelo Supremo Tribunal Federal no julgamento da MP 954, valendo citar também a PEC nº 17/2019, recentemente aprovada pelo Congresso Nacional para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

a aplicação da LGPD e relacionando aos modelos estrangeiros.

Para tanto, primeiramente, será apontada a contribuição da abordagem baseada no risco para o compliance com a legislação de proteção de dados tal como concebida no sistema do GDPR.

Em seguida, serão apresentados alguns modelos estrangeiros de avaliação de riscos à privacidade, optando-se, além do modelo europeu, pelo modelo australiano de avaliação e identificando os principais elementos que os constituem.

Por fim, será feito um levantamento e análise sobre o que a LGPD efetivamente trouxe ao ordenamento brasileiro sobre o instrumento em questão, ressaltando a grande lacuna regulatória ainda existente quanto à sua realização e a necessidade de suplementação por parte da Autoridade Nacional de Proteção de Dados (ANPD).

2. A ABORDAGEM BASEADA NO RISCO NAS LEIS DE PRIVACIDADE

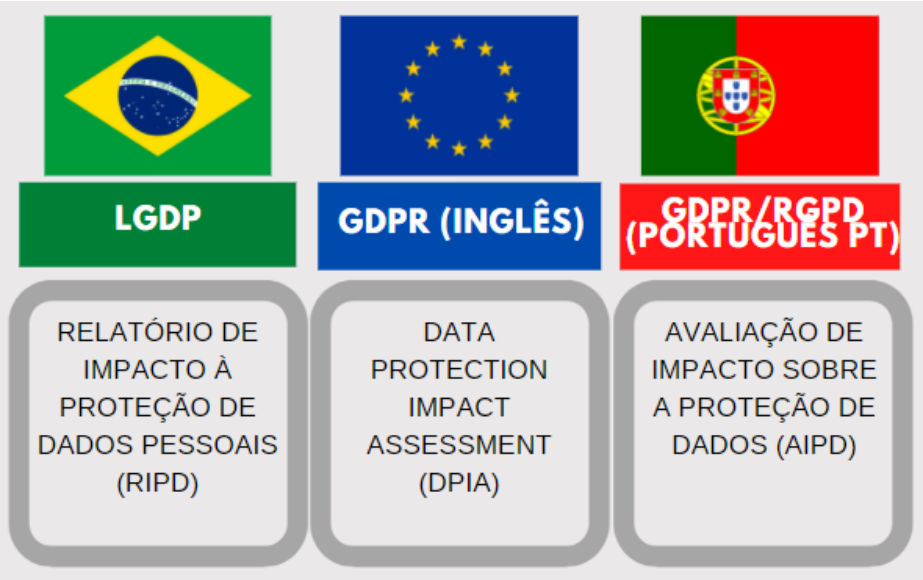
A legislação de proteção de dados, tanto brasileira quanto sua contraparte europeia, estabelece um complexo sistema de regras e princípios para regular o tratamento de dados pessoais. O sistema, no entanto, não possui fórmula única para o compliance, isto é, não há uma receita exata que direcione as organizações ao atendimento de seus requisitos e conformidade.

O modelo regulatório de proteção de dados do GDPR, do qual optou a legislação brasileira, possui abordagem baseada no risco (*risk-based approach*), o que torna necessário entender o papel do risco dentro do sistema de proteção de dados pessoais.

Para facilitar o entendimento das nomenclaturas existentes entre

os sistemas da LGPD e do GDPR, considerando, este último, sua variação para o inglês e para o português de Portugal:

Figura 1: Comparativo de nomenclatura



Fonte: AUTORIA PRÓPRIA (2021)

Deve-se esclarecer logo que não se trata, contudo, de qualquer espécie de risco, e tampouco trata-se do risco jurídico ou reputacional à empresa que está realizando o tratamento dos dados. O risco em questão é aquele que está para os direitos e liberdades dos indivíduos cujos dados são objeto de tratamento, isto é, dos titulares.

Com isto se quer dizer que o modelo regulatório instituído pelo GDPR, sobre o qual a LGPD compôs seus fundamentos, deixa em aberto que as medidas a serem adotadas para o compliance sejam definidas conforme a avaliação de risco em relação aos direitos e liberdades dos titulares dos dados. São estes aspectos o ponto de referência para a análise de risco.

Ora, quando uma organização realiza alguma operação de tratamento de dados pessoais (coleta, utilização, armazenamento, transferência, entre outros), os respectivos titulares podem estar expostos a riscos cuja identificação e avaliação são circunstanciais, podendo ser maiores ou menores.

Nenhuma operação é isenta de riscos. Assim, é necessário que os agentes de tratamento, diante de um risco identificado, tomem as medidas adequadas para garantir que tais dados sejam tratados de forma segura e de acordo com a legislação.

O regulamento europeu, no entanto, não estabelece um passo-a-passo para a realização desta avaliação, sendo inúmeras as metodologias disponíveis e aplicadas pelos agentes de tratamento.

O problema nesta suposta liberdade de avaliação está na seleção do método para a identificação de riscos pelo controlador e se tal não está "orientada por um embasamento técnico-científico e se resume a conclusões subjetivas, orientadas pela perspectiva pessoal do agente de tratamento" (GOMES, 2020, p. 255).

Disto, pode-se visualizar que os controladores são responsáveis pela forma com que implementam a legislação, isto é, transportam o que está abstratamente previsto para a prática. E para que isto ocorra, a noção de risco é essencial para determinar quais as medidas técnicas e organizacionais que devem ser adotadas.

Segundo Claudia Quelle (2017, p. 2), a abordagem baseada no risco objetiva otimizar a aplicação da legislação, preenchendo a lacuna entre o nível de proteção de dados estabelecido abstratamente pelos princípios de privacidade e as reais práticas de compliance.

A referida autora relaciona que a abordagem baseada no risco

repercute diretamente no atendimento às obrigações impostas pelo regulamento no caso concreto. Explica ainda que a noção de risco aplicada habilita os controladores a calibrar suas obrigações legais, funcionando como ponto de referência para a determinação das medidas em concreto a serem adotadas para alcançar os requisitos legais (QUELLE, 2017, p. 3).

Ainda sob a égide da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, o *Article 29 Working Party (WP 29)*[3], que viria a ser substituído pelo *European Data Protection Board (EDPB)*, na vigência do GDPR, emitiu a *Opinion 03/2010*, contendo sugestões para garantir a efetividade do princípio da prestação de contas (*accountability*), no qual afirma que as medidas a serem implementadas pelos controladores devem variar conforme o risco da atividade de tratamento e dos dados envolvidos (WP 29, 2010, p. 5).

O WP 29 afirma também que algumas obrigações são somente aplicáveis se diante de operações de tratamento de maior risco, citando-se justamente o caso da realização de um *Privacy Impact Assessment*[4], o que se traduz em programas de compliance escaláveis (2010, p. 4).

Também neste sentido, a autoridade de proteção de dados do Reino Unido, *Information Commissioner's Office (ICO)*, apresenta em seu site o seguinte questionamento:

3 O Grupo de Trabalho do Artigo 29 (WP29) foi constituído sob o regime da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. No regime do GDPR, foi sucedido pelo *European Data Protection Board (EDPB)*, que endossou algumas das guidelines produzidas pelo WP29, aproveitando o rico trabalho realizado até então. A lista de documentos endossados pode ser consultada em: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en. Acesso em 14 jul. 2021.

4 Atualmente denominado no âmbito do GDPR como *Data Protection Impact Assessment*.

> *Why don't you tell me exactly what to do?*
> *Every organisation is different and there is no one-size fits-all answer. Data protection law doesn't set many absolute rules. Instead it takes a risk-based approach, based on some key principles. This means it's flexible and can be applied to a huge range of organisations and situations, and it doesn't act as a barrier to doing new things in new ways.*[5] *(ICO, 2018)*

O brocardo *"there is no one-size fits-all answer"* (não existe uma resposta que sirva para todos) reforça justamente a noção de não haver fórmula única para o compliance de proteção de dados. Ainda no mesmo documento, a ICO alerta que esta flexibilidade regulatória impõe ao agente, por consequência, a responsabilização deste quanto à definição das medidas que são adotadas no uso de dados pessoais.

A abordagem baseada no risco do GDPR aparece em particular nos artigos 24, 25(1) e 35 do regulamento.

O artigo 24 refere-se à responsabilidade do controlador na adoção das medidas técnicas e organizacionais tendentes à conformidade com o regulamento e de acordo com a "a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares". O artigo 25, por sua vez, foca nos tipos de medidas que podem ser adotadas pelo controlador.

Em ambos os casos, há referência de que o controlador deve levar em conta, na definição das medidas a serem adotadas, os riscos

5 Por que você não me diz exatamente o que fazer? Cada organização é diferente e não existe uma resposta única e que se encaixe para todos. A lei de proteção de dados não estabelece muitas regras absolutas. Em vez disso, adota uma abordagem baseada no risco, baseada em alguns princípios-chave. Isso significa que é flexível e pode ser aplicada a uma grande variedade de organizações e situações, e não atua como uma barreira para fazer coisas novas de novas maneiras (tradução livre).

aos direitos e liberdades dos indivíduos, comprovando que o foco da análise de riscos reside precisamente no titular dos dados.

Esta obrigação vem também estampada no Considerando 74 do regulamento, que dispõe que o controlador:

> (...) deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares.

Trata-se da noção de risco, portanto, que o controlador deve abarcar em seu plano de adequação e governança em proteção de dados pessoais, e os direitos e liberdades do titular, por sua vez, são o ponto de referência para esta análise.

Menciona-se que esta obrigação, no entanto, não é isenta de limites. O artigo 25(1) estabelece que o controlador leve em consideração o estado da arte e os custos da aplicação das medidas, o que demonstra a sensibilidade do regulamento em dispensar o agente de tratamento de obrigações excessivamente onerosas. Ao mesmo tempo, isto não isenta o agente da adoção das medidas de segurança apropriadas conforme o risco representado por sua operação de tratamento.

O artigo 35 complementa esta abordagem ao exigir que o controlador avalie o impacto das operações de tratamento pretendidas em determinadas situações, ou seja, que tenha de realizar uma avaliação de impacto sobre a proteção de dados pessoais, conhecida *data protection impact assessment (DPIA)*, quando a operação implicar em elevado risco ao titular.

Requer-se, basicamente, que o controlador avalie a proporcionalidade das operações de tratamento pretendidas bem como os riscos aos direitos e liberdades dos indivíduos envolvidos a fim de identificar as medidas suficientes para endereçar estes riscos.

O DPIA, portanto, é ferramenta que habilita o controlador a projetar suas próprias medidas técnicas e organizacionais a proteger os indivíduos envolvidos e garantir o compliance com o regulamento.

A LGPD, de maneira semelhante, também traz esta noção, não apenas por importar o DPIA na forma do denominado "Relatório de Impacto à Proteção de Dados" (RIPD), como também há a menção ao risco em diversos dispositivos, dentre eles o artigo 44, que estabelece parâmetros para identificar quando uma operação de tratamento de dados pode ser considerada irregular, isto é, em desconformidade com a lei, um *non-compliance*.

O referido artigo prevê o seguinte fator de análise para a verificação da irregularidade de determinado tratamento de dados:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> (...)
> II - o resultado e os riscos que razoavelmente dele se esperam. (LGPD, 2018)

Assim, mesmo no quadro normativo da LGPD, a abordagem baseada no risco impacta as medidas que devem ser adotadas para se estar compliant, devendo ser considerado cada caso em particular.

A escalabilidade das obrigações do controlador na LGPD pode ser verificada no RIPD, sendo uma das medidas implementáveis quando diante de uma operação de tratamento que represente maior risco.

O RIPD dá suporte à esta noção à medida que funciona como instrumento do controlador na avaliação de suas operações, identificando riscos e habilitando-o a tomar as decisões necessárias para o seu devido endereçamento e gestão.

3. MODELOS ESTRANGEIROS DE AVALIAÇÃO DE RISCOS À PRIVACIDADE

Em que pese a novidade legislativa em solo brasileiro, as avaliações de risco na seara da privacidade não são recentes, contando com largo histórico de desenvolvimento de seu ideal e utilização pelos setores público e privado[6].

Ademais, a regulação de proteção de dados não significa engessamento de atividades econômicas e do desenvolvimento de novas ideias, prezando, em seu cerne, pela viabilização dos fluxos transnacionais de dados pessoais, sem os quais não seria possível a prestação de serviços online de qualquer parte do mundo e a concretização de negócios em meio à economia digital e *data-driven* atual.

A título de curiosidade para evidenciar este propósito, um importante marco foi a celebração da Convenção 108 do Conselho da Europa de 1981[7], o primeiro tratado internacional, aberto a todos

6 Sobre as origens e desenvolvimento do PIA, recomenda-se a leitura de CLARKE, Roger. *Privacy impact assessment: Its origins and development*. *Computer Law & Security Review*. Volume 25, Issue 2, 2009. Fl. 123-135.

7 Inclusive, é em razão deste documento que se celebra, em 28 de janeiro, data da abertura do documento para signatários, o Dia Internacional da Pro-

os países, sobre proteção de dados pessoais, precedente que passou a pavimentar o caminho para a construção de uma regulamentação mais uniforme sobre o tema a nível global, do qual inclusive figuram como signatários Argentina e Uruguai, representando a elevação desta pauta na américa-latina.

O tratamento de dados pessoais oferece, de forma inerente, risco aos seus respectivos titulares, o que, naturalmente, varia de acordo com a natureza e o escopo da atividade de tratamento. Dados podem ser perdidos, acessados por pessoas não autorizada ou tratados em desacordo com a lei.

Com o surgimento de novas tecnologias, as operações de tratamento de dados tendem a ficar cada vez mais complexas, sendo responsabilidade do controlador o endereçamento dos riscos envolvidos antes mesmo de iniciar o tratamento.

3.1. DPIA NO MODELO EUROPEU (RGPD/GDPR)

A nomenclatura *data protection impact assessment (DPIA)* adotada no GDPR, ou Avaliação de Impacto sobre a Proteção de Dados (AIPD), na tradução do regulamento para Portugal, diferindo de *privacy impact assessment*, advém, primariamente, da divisão, no sistema de direitos fundamentais da União Europeia, entre os direitos à privacidade e à proteção de dados pessoais, concebidos como direitos distintos, cujos conteúdos protegem aspectos diversos da dignidade humana[8].

teção de Dados Pessoais (Data Protection Day).

8 Sobre o ponto, recomenda-se a obra de DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters, 2019

O Considerando 84 estabelece primordialmente o escopo do DPIA:

> (84) A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.

Em que pese careça de definição pelo GDPR, o *Article 29 Working Party* emitiu orientações quanto ao DPIA do GDPR na guideline WP 248 rev.01[9], conceituando como sendo um:

> (...) processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos (WP29, 2017, p. 4).

Destaque para compreensão do DPIA pelo WP29 como um processo, ao invés de relatório, na terminologia da LGPD, ponto relevante que será abordado mais adiante neste trabalho.

A especificação do conteúdo mínimo que deve incluir o DPIA vem no artigo 35º, n. 7:

9 A WP 248 rev.01 foi uma das guidelines endossadas pelo EDPB.

> 7. A avaliação inclui, pelo menos:
> a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
> b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
> c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o nº 1; e
> d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

Neste sentido, o WP29 relaciona a realização do DPIA ao princípio da responsabilização por ser ferramenta que auxilia o controlador a cumprir o regulamento ao mesmo tempo que o habilita a demonstrar este mesmo cumprimento. Isto é, o DPIA é instrumento para a demonstração da conformidade pelo agente de tratamento.

Quanto à sua realização, tem-se como mandatória em especial quando a operação de tratamento de dados "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares", devendo realizá-lo antes mesmo de iniciar o tratamento (artigo 35º, n. 1).

Os casos que tornam obrigatória a realização do DPIA estão especificados no artigo 35º, n. 3:

> 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é obrigatória nomeadamente em caso de:
> a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

> b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou
> c) Controlo sistemático de zonas acessíveis ao público em grande escala.

Ainda, outras operações de tratamento de dados poderão estar sujeitas ao requisito do DPIA conforme definidas em lista elaborada e publicada pela autoridade de controle de cada país sujeito ao regulamento, mediante comunicação ao Comitê Europeu para a Proteção de Dados. De igual modo, também poderá haver listas contendo as operações que estão dispensadas da realização do DPIA.

Como se vê, o regulamento não estabelece, e nem poderia pretender, um rol exaustivo de operações reconhecidamente de elevado risco que elevam a necessidade da realização de um DPIA.

Isto se coaduna com o argumento da utilidade desta ferramenta ainda que diante de uma situação não mandatória da sua realização (MOTA, 2019, p. 182).

Portanto, ainda que não seja caso da realização obrigatória do DPIA, sua utilização pode revelar-se não apenas uma boa prática, mas ferramenta útil para auxiliar os controladores a prever incidentes e endereçar medidas para a mitigação dos riscos, também servindo à demonstração de sua própria conformidade às autoridades.

Seus benefícios envolvem tanto o aumento da conscientização e comprometimento da organização em seus diversos departamentos, quanto serve de apoio à gestão e direção na tomada de decisões melhor informadas e embasadas. Assim, garante-se que novas ideias sejam projetadas e desenvolvidas levando em con-

sideração a proteção de dados desde a sua concepção, imbricada em seu próprio design[10].

Conforme mencionado anteriormente sobre o regulamento ser uma norma com *risk-based approach*, o risco específico que se deve prezar e utilizar-se como parâmetro do DPIA não é qualquer tipo de risco, mas àquele que potencialmente impacta os direitos e liberdades do titular.

A natureza do risco com que se preocupa o regulamento está descrita detalhadamente no Considerando 75:

> (75) O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titula-

10 Esta noção é comumente referida como *privacy by design*.

res de dados.

Na já referida guideline, o WP 29 buscou indicar nove fatores de análise para, previamente, verificar a necessidade de se realizar um DPIA, isto é, para a averiguação se uma determinada operação de tratamento de dados pessoais deve ser considerada passível de implicar um elevado risco aos titulares (WP29, 2017, p. 10-12):

> 1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de "aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados" (...).
> 2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar (...).
> 3. Controlo sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um "controle sistemático de zonas acessíveis ao público" (...).
> 4. Dados sensíveis ou dados de natureza altamente pessoal (...).
> 5. Dados tratados em grande escala (...).
> 6. Estabelecer correspondências ou combinar conjuntos de dados (...).
> 7. Dados relativos a titulares de dados vulneráveis (...).
> 8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais (...).
> 9. Quando o próprio tratamento impede os titulares dos dados "de exercer um direito ou de utilizar um serviço ou um contrato" (...).

O WP 29 considera que quanto maior o número de critérios preenchidos, maior a probabilidade de o tratamento de dados sob análise implicar num elevado risco aos direitos e liberdades dos titulares, atraindo, por consequência, a obrigatoriedade da realização de um DPIA.

Desta forma, evidencia-se que, previamente ao próprio processo do DPIA, seja realizada uma análise preliminar acerca da sua necessidade.

Quanto ao processo para a realização do DPIA em si, o GDPR deixa livre que a gestão de risco aos direitos e liberdades dos titulares seja integrada às práticas de gestão de risco e governança da empresa.

Sobre este aspecto, o WP 29 (2017, p. 19) ilustra-o com as seguintes etapas, mas alerta que "(...) na prática, é provável que cada uma das etapas seja revisitada várias vezes antes de a AIPD poder ser concluída":

Figura 2: Processo iterativo genérico para a realização de uma AIPD

Fonte: WP 29 (2017, p. 19)

Ao final deste processo, se o risco residual aos titulares ainda for alto, isto é, se as medidas endereçadas aos riscos identificados

não forem suficientes, deverá o controlador consultar a autoridade de controle antes de proceder à operação de tratamento.

3.1.1. MODELOS DENTRO DO ESPECTRO DO GDPR

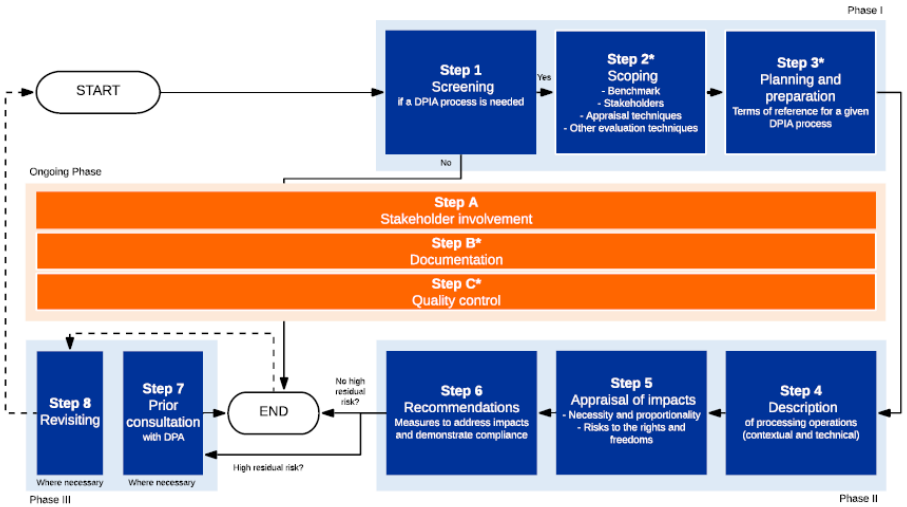
Conforme se viu, o GDPR optou por não estabelecer metodologia para o processo de DPIA e não há consenso quanto à exata forma de sua realização. O próprio WP29 reconhece a existência de inúmeros métodos de avaliação de riscos e indica que, seja qual for a metodologia adotada, "uma AIPD deve avaliar genuinamente os riscos, permitindo assim que os responsáveis pelo tratamento tomem medidas para dar resposta a esses riscos" (2010, p. 20). Inclusive, incentiva o desenvolvimento de métodos setoriais específicos, de modo a permitir a adaptação do DPIA a operações de tratamento de dados existentes em determinado setor (WP29, 2010, p. 20).

Há, em verdade, uma série de metodologias de DPIA diferentes desenvolvidas, variando em formato, etapas e conteúdo.

Um dos modelos de realização de DPIA mais interessantes que podem ser citados é o desenvolvido pelo *Brussels Laboratory for Data Protection & Privacy Impact Assessments*, da Universidade Livre de Amsterdã (VUB, 2020), composto de onze etapas, das quais seis são consecutivas, duas eventuais a depender das condições verificadas, e outras três etapas desempenhadas em paralelo ao longo de todo o processo.

A proposta é ilustrada da seguinte forma:

Figura 3: Visão geral do método de avaliação



Fonte: VUB (2020, p. 3).

O modelo conta, além da descrição de cada uma das etapas sugeridas, de diversos templates de tabelas para o preenchimento de informações de forma sistemática.

O primeiro passo do modelo proposto contempla a avaliação preliminar para a verificação da necessidade de realização do DPIA.

O segundo envolve identificar o quadro jurídico aplicável, as categorias de partes interessadas a serem envolvidas no processo, as técnicas de avaliação que possam ser necessárias para além da avaliação de necessidade e de proporcionalidade e avaliação de risco.

O terceiro determina o planejamento e preparação para a realização do DPIA, estabelecendo os termos de referência do processo, tais como objetivos, critérios, papeis e responsabilidades, recursos disponíveis, prazo dentre outros.

A descrição detalhada do tratamento pretendido, incluindo a possibilidade de representação por diagrama dos fluxos de dados envolvidos, constitui o quarto passo.

O quinto passo objetiva avaliar a necessidade e a proporcionalidade do processo pretendido em relação às suas finalidades, além de avaliar os riscos decorrentes aos direitos e liberdades dos titulares.

O sexto passo trata de levantar as medidas aptas a endereçar os riscos que foram identificados ou mesmo apontar a desnecessidade ou a desproporcionalidade do tratamento pretendido.

As três etapas paralelas e contínuas desenvolvidas ao longo de todo o projeto envolvem a consulta aos stakeholders, que podem ser internos ou externos, nestes últimos incluídos os próprios titulares de dados, o controle de qualidade para verificação se o processo está aderente a um determinado standard de performance, e a manutenção de registros de tudo que for realizado ao longo do processo.

Pode-se citar, ainda, outros modelos relevantes para a execução do DPIA no âmbito do GDPR a exemplo do constante no guia *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, da autoridade de proteção de dados da Espanha, *Agencia Española de Protección de Datos* (AEPD, 2021), e o guia disponibilizado no site da autoridade do Reino Unido, *Information Commissioner's Office* (ICO, 2021), todos referindo-se ao DPIA como sendo um processo.

3.2. PIA NA AUSTRÁLIA

A seleção do modelo proposto na Austrália como demonstrativo de avaliação de riscos em privacidade se deu pelas circunstâncias diversas daquele país a respeito do tema e que servem ao objetivo do presente estudo para demonstrar que uma avaliação desta natureza se revela como ferramenta de grande utilidade aos agentes de tratamento, ainda que não seja uma obrigatoriedade legal.

A legislação da Austrália, muito embora acolha a proteção da privacidade do indivíduo, não estabelece a obrigatoriedade da realização de uma avaliação de impacto à privacidade às organizações do setor privado, reservada a possibilidade desta determinação pela autoridade australiana apenas no caso das agências.

Em que pese este aspecto regulatório diverso se comparado com o modelo aplicado ao Espaço Econômico Europeu, a autoridade australiana, *Office of the Australian Information Commissioner (OAIC)*, regulador nacional independente quanto à privacidade e liberdade da informação, incentiva amplamente a realização do PIA mesmo para as organizações do setor privado, tendo publicado seu próprio *Guide to undertaking privacy impact assessments* nos anos de 2006, 2010 e, sua versão mais recente, em 2020, direcionado aos setores público e privado.

Desde a sua introdução e ao longo de todo o guia, a OAIC refere-se ao PIA como um processo, composto de dez etapas no modelo proposto.

Seu conceito é estabelecido sendo *"a privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating*

that impact". (OAIC, 2020, p. 2)[11].

Ressalta-se a recomendação da aplicabilidade do PIA sobre um projeto, termo entendido de forma ampla como qualquer atividade ou iniciativa que possa gerar implicações sobre a privacidade.

Quanto ao momento de sua realização, a OAIC indica que o PIA funciona melhor quando parte integrante do processo de planejamento do projeto sob análise, e não numa reflexão tardia, devendo ser realizado cedo o suficiente para poder influenciar e ajudar a moldar o desenvolvimento do projeto ou ao menos para permitir a reconsideração do procedimento que vem sendo desenvolvido se houver impactos negativos à privacidade (2020, p. 4-5).

Esta constatação é proveitosa à empresa na medida em que assegura que os riscos à privacidade sejam identificados antecipadamente, nos primeiros estágios do desenvolvimento, e, com isso, sejam tomadas as decisões necessárias para verificar caminhos alternativos no desenvolvimento do projeto e promover a correção de seu curso.

A OAIC acrescenta que o PIA não é finalizado com a publicação de seu relatório, devendo ser revisitado durante a implementação do projeto bem como quando mudanças ocorram, podendo inclusive demandar a realização de um novo PIA (2020, p. 5).

Inclusive, este é mais um fator que evidencia que o PIA seja pensado enquanto processo e que eventual relatório produzido ao seu final com este não se confunde, sendo meramente uma de

11 "Uma avaliação sistemática de um projeto que identifica o impacto que este pode ter sobre a privacidade dos indivíduos e estabelece as recomendações para o gerenciamento, minimização e eliminação deste impacto" (tradução livre).

suas etapas integrantes.
O modelo sugerido pela OAIC contém orientações para a realização do PIA em dez etapas (2020, p. 7), quais sejam:

1. *Threshold assessment;*
2. *Plan the PIA;*
3. *Describe the project;*
4. *Identify and consult with stakeholders;*
5. *Map information flows;*
6. *Privacy impact analysis and compliance check;*
7. *Privacy management — addressing risks;*
8. *Recommendations;*
9. *Report;*
10. *Respond and review*[12].

Em relação à primeira etapa, a OAIC sugere, de forma semelhante à exposta na guideline do WP29, uma avaliação prévia da necessidade da realização da avaliação de impacto no projeto selecionado. Importa ressaltar que nem todo projeto demandará a realização de uma avaliação desta natureza, interessando aqueles que impliquem em riscos significativos aos indivíduos envolvidos na operação. Assim, esta etapa presta-se a analisar e eleger o projeto a ser submetido ao processo do PIA.

Resumidamente, faz-se uma breve descrição do projeto, verifica-se se há a pretensão de tratamento de dados pessoais, quais são os dados envolvidos e sua natureza, para quais finalidades serão tratados, o posicionamento das partes interessadas sobre o seu impacto e, caso seja um projeto que não envolva mudanças

12 1. Avaliação de limite; 2. Planeje o PIA; 3. Descreva o projeto; 4. Identifique e consulte as partes interessadas; 5. Mapeie os fluxos de informação; 6. Análise de impacto de privacidade e verificação de conformidade; 7. Gestão de privacidade: endereçamento de riscos; 8. Recomendações; 9. Relatório; 10. Resposta e revisão. (Tradução livre).

nas práticas de tratamento de dados, a descrição sobre como os riscos envolvidos já foram endereçados. Ao final, a indicação do time responsável pela realização desta avaliação e a indicação pela realização do PIA ou não (OAIC, 2020, p. 7-8).

A segunda etapa refere-se ao planejamento da realização do PIA, contendo a definição do seu escopo e a identificação de quem irá conduzi-lo. A terceira destina-se à ampla descrição do projeto. A quarta envolve a consulta às partes interessadas ou afetadas pelo projeto sob análise, comumente denominados na prática como *stakeholders*. A consulta aos *stakeholders* exerce um papel fundamental no processo de PIA, pois auxilia que sejam levantadas questões-chave envolvendo a privacidade (OAIC, 2020, p. 8-13).

A quinta etapa envolve um trabalho mais detalhado para que sejam mapeados os fluxos da informação, compreendendo-se como serão coletadas, utilizadas, quem terá acesso, quais medidas de segurança já estão ou ainda serão postas e os períodos de retenção e forma de eliminação. Para esta tarefa, a OAIC recomenda o uso de diagramas ou tabelas (2020, p. 14).

A sexta etapa ocupa-se da análise de risco do projeto à privacidade dos indivíduos e adiciona um elemento interessante: a verificação das expectativas e aceitação da comunidade em relação ao tratamento das informações pelo projeto, o que pode ser avaliado por meio de consulta ou até um olhar sobre a resposta desta a projetos semelhantes. Esta etapa ainda considera a verificação do cumprimento aos treze *Australian Privacy Principles (APPs) listados no Privacy Act*[13], bem como das demais legislações

13 Princípios australianos de privacidade, em tradução livre. Os APPs representam, basicamente, o núcleo da legislação de privacidade australiana, aos quais todas as entidades submetidas à legislação devem observar. São ao todo treze princípios definidos no *Privacy Act* de 1988, com inclusões até o

relevantes à agência ou organização.

Dos riscos identificados na etapa anterior, é necessário, na sétima etapa, definir quais as opções existentes para o endereçamento destes riscos, seja para eliminá-los ou mitigá-los a um nível aceitável, que podem incluir controles de natureza técnica ou operacional (OAIC, 2020, p. 28).

A oitava etapa trata de levantar as recomendações necessárias ao projeto e que foram evidenciadas nas etapas anteriores e devem ser integradas na nona etapa, que representa o relatório compondo todas as informações e descobertas obtidas ao longo do processo do PIA. O guia inclusive disponibiliza um sugestivo de formato para o relatório do PIA.

Por fim, na última etapa devem ser endereçadas medidas para todas as recomendações levantadas no relatório, além da constante revisão e atualização do PIA, considerado como um processo contínuo, que não se exaure na elaboração do relatório (OAIC, 2020, p. 32).

Disto tudo, ressalta-se, novamente, a importância da concepção da avaliação de impacto como um processo e não meramente um relatório. Além disso, mais do que um mero *checklist* de compliance, o PIA:

> *Should 'tell the full story' of a project from a privacy perspective, going beyond compliance to also consider the broader privacy implications and risks, including whether the planned uses of personal information*

Act No. 13, 2021. Segundo a OAIC, a violação de um APP significa uma interferência na privacidade do indivíduo e pode levar a penalidades e ações regulatórias. Para maiores elucidações, recomenda-se a leitura de OAIC – *OFFICE THE AUSTRALIAN INFORMATION COMMISSIONER AUSTRALIA.*. *Australian Privacy Principles*. Disponível em: https://www.oaic.gov.au/privacy/australian-privacy-principles.

in the project will be acceptable to the community[14]*. (OAIC, 2020, p. 3)*

Mesmo que a realização do PIA não seja legalmente mandatória como regra, a própria autoridade nacional australiana incentiva o processo como parte de uma abordagem de *privacy by design*, tornando a privacidade uma peça-chave a ser considerada desde os estágios iniciais e ao longo do ciclo de vida de um projeto.

4. O RIPD NA LEI BRASILEIRA

Ainda que sua condução compita ao controlador em determinados casos, viu-se que o PIA/DPIA configura boa prática, pois importante ferramenta de aferição de riscos e direcionamento de ações em operações de tratamento de dados pessoais em geral, sendo recomendável e útil mesmo quando a lei não o indique como procedimento obrigatório.

Pense-se, por exemplo, na ideação de um novo projeto na empresa que, por meio de operações específicas de perfilamento de dados pessoais de clientes, promete revolucionar o alcance das atividades da empresa, oportunizando uma grande possibilidade de atuação em um novo segmento.

Evidente que, simplesmente por haver o tratamento de dados pessoais, a operação deve estar aderente à legislação de proteção de dados. No caso da LGPD, semelhantemente ao sistema regulatório do GDPR, as operações de tratamento de dados devem observar como requisitos os princípios da legislação além de estarem legitimadas em alguma das hipóteses justificantes de

14 Deve 'contar a história completa' de um projeto de uma perspectiva de privacidade, indo além da conformidade para também considerar as implicações e riscos mais amplos de privacidade, incluindo se os usos planejados de informações pessoais no projeto serão aceitáveis para a comunidade (tradução livre).

tratamento definidas em lei.

Recomenda-se, contudo, que isto seja abordado desde a ideação do projeto, de maneira proativa, isto é, que a privacidade e a proteção de dados sejam pensadas desde o início do projeto, aferindo-se os riscos aos titulares e identificando as medidas aptas a endereçá-los, seja para eliminá-los ou para mitigá-los, e o RIPD é um dos instrumentos para concretizar isso.

Este posicionamento tem o potencial de evitar gastos exacerbados de última hora na reestruturação e reformulação do projeto ou mesmo de impedir, em momento avançado de desenvolvimento, eventual decisão pela inviabilidade do próprio projeto, importando em severos prejuízos e a perda de oportunidades.

4.1. O QUE PREVÊ A LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) estrutura-se de forma muito semelhante ao regulamento europeu (GDPR). Assemelham-se em conceitos, princípios e na lógica de funcionamento em geral, girando em torno de regular o tratamento de dados no objetivo de proteger o titular, tudo isto fiscalizado por uma autoridade nacional especializada no tema.

Diferentemente do regulamento europeu quanto ao DPIA, a LGPD traz o conceito do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) estampado no rol de definições do artigo 5º XVII:

> XVII: relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; (LGPD, 2018)

Inclusive, é criticável a adoção da terminologia relatório pela LGPD. Palhares alerta que a nomenclatura é inadequada quando, em verdade, o RIPD deveria ser interpretado como um processo de avaliação de riscos (2021, p. 143).

De certa forma, a nomenclatura e a definição estabelecidas podem passar a impressão de que o RIPD seja reduzido a um mero documento autodeclaratório produzido pelo controlador, não envolvendo todo o processo de análise e avaliação do DPIA ou do PIA.

O termo *assessment*, que compõe o DPIA, por sua vez, pode ser traduzido como avaliação, não havendo dúvidas ou confusão a ponto de que seja reduzido a um mero relatório do controlador.

A nomenclatura adotada pela LGPD, portanto, não significa que uma avaliação efetiva dos riscos aos direitos e liberdades dos titulares envolvidos no tratamento pretendido esteja dispensada. Pelo contrário, o RIPD não se resume a mero preenchimento de *checklist* de compliance com a lei.

Por outro lado, a definição fornecida pela lei demonstra a preocupação do sistema em abarcar a necessidade de avaliação do risco aos titulares bem como as medidas para o seu endereçamento.

Contudo, as definições param por aí, visto que a LGPD pouco traz a respeito do recém inaugurado instituto, não estabelecendo regras claras quanto ao momento da sua realização, seu formato, situações em que é mandatório, forma de publicação ou disponibilização à ANPD etc.

Ao todo, a LGPD cita o RIPD apenas 4 (quatro) vezes, reforçando que a sua realização seja atribuição do controlador, isto é, do responsável pelo tratamento dos dados, estipulando, em duas opor-

tunidades, que a ANPD "poderá" solicitar/determinar ao referido agente a sua realização (arts. 10, §3º e 38, *caput*).

Por óbvio que a LGPD deve ser interpretada e aplicada em consonância com o ordenamento jurídico preexistente, inserindo-se num complexo sistema de fontes normativas já estabelecidas, as quais busca-se o diálogo, o que não significa ignorar as lições e conteúdos apreendidos no âmbito de aplicação dos sistemas de proteção de dados estrangeiros. Pelo contrário, as práticas sedimentadas em outros sistemas regulatórios sobre este assunto global fornecem caminho sólido para a sua utilização e melhor aproveitamento[15].

Ainda assim, resta clara a opção inscrita na LGPD pelo modelo regulatório europeu, o que pode ser observado, dentre tantos outros pontos, quanto à natureza do risco que o RIPD deve se ocupar, que não é qualquer risco, e tampouco um risco à empresa, mas aquele às liberdades civis e aos direitos fundamentais dos titulares de dados, o verdadeiro objeto de proteção do sistema.

A inspiração europeia também pode ser evidenciada quanto ao conteúdo mínimo que deve constar no RIPD, previsto no parágrafo único do artigo 38, que se assemelha, embora muito menos esclarecedor, ao artigo 35, n.º 7, do GDPR, conforme quadro comparativo a seguir:

15 Inclusive, a própria ANPD externou estar atenta ao GDPR e guidelines do EDPB em seu Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Para mais informações sobre o tema, recomenda-se a leitura do referido documento, disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf.

Tabela 1: Comparativo RIPD e DPIA

LGPD – artigo 38, parágrafo único	**GDPR – artigo 35, n.º 7**
Parágrafo único. Observado o disposto no *caput* deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.	7. A avaliação inclui, pelo menos: a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento; b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos; c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.o 1; e d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

Fonte: AUTORIA PRÓPRIA (2021).

Quanto ao vácuo regulatório em torno do RIPD, fica a cargo da ANPD o hercúleo trabalho de oferecer, a este e a tantos outros pontos deixados em aberto[16], a pavimentação da segurança jurídica imprescindível aos agentes de tratamento, visto que:

> Art. 55-J. Compete à ANPD:
> (...)
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

Positivamente, este debate vem sendo amadurecido recentemente diante da atuação da ANPD, que, mesmo com pouco tempo de existência, e ainda em sua primeira diretoria, tem empenhado grandes esforços e avançado sobre a questão, a qual foi incluída na Fase 1 de sua agenda regulatória para o biênio 2021-2022, consistente nas "iniciativas da agenda regulatória cujo início do processo regulatório acontecerá em até 1 ano" (ANPD, 2021).

Representativo destes esforços foi a realização pela ANPD, no mês de junho deste ano, de uma série de reuniões técnicas sobre o relatório de impacto, divididas em três grandes blocos de perguntas que contaram com a participação de vários expositores: Bloco 1 - Metodologias e critérios para elaboração e análise do relatório de impacto; Bloco 2 - Situações/circunstâncias que ensejam a necessidade ou dispensa de elaboração de relatório de impacto; e Bloco 3 - Transparência e publicidade dos relatórios de impacto para o setor público e o setor privado(ANPD, 2021).

16 Em relação às incertezas regulatórias e a dependência de suplementação da lei pela ANPD, recomenda-se o artigo da ALVES, Fabrício da Mota. Sem a ANPD, a LGPD é um problema, não uma solução (ALVES, 2020).

Tem-se com grande otimismo as atividades até então desempenhadas pela ANPD, pois é de suma importância que a regulação a suplementar o sistema da LGPD seja precedida de diálogo com os diferentes setores econômicos, diretamente afetados na condição de agentes de tratamento. Com isso, espera-se a publicação de resolução ou, ao menos, de um guia orientativo à sociedade.

Tais definições são imprescindíveis à segurança jurídica de que necessitam os agentes de tratamento, que poderão dimensionar com precisão os limites de sua atuação e as sanções a que estão sujeitos.

4.2. O RIPD ENQUANTO PROCESSO

Viu-se, tanto no caso do PIA quanto do DPIA a concepção deste instrumento enquanto um verdadeiro processo, constituído de diversas etapas, e não apenas um mero relatório.

Entende-se que a melhor aplicação e aproveitamento do instituto seja também por meio desta concepção, pelas claras origens estrangeiras, destinado à aferição do risco de um determinado projeto aos direitos dos titulares dos dados a serem afetados. Aqui, adota-se a terminologia "projeto" para referir-se aquilo que será objeto de um RIPD, entendido de forma ampla para abarcar iniciativas, políticas, ideias, processos, produtos e serviços que, de alguma forma, impliquem, por si só, ou impactem o tratamento de dados pessoais.

O artigo 38, parágrafo único, chega a mencionar o termo "metodologia", mas não estabelece quaisquer especificações a respeito.

Conforme visto, sequer o GDPR estabelece metodologia para a realização do DPIA.

Contudo, a definição da metodologia é aspecto de extrema relevância para que os riscos aos titulares sejam verdadeiramente avaliados, pois somente assim cumpre-se com o que objetiva a LGPD, que é a proteção do titular em relação ao tratamento de seus dados pessoais.

E a respeito disso, segundo Gomes:

> A forma como o risco será avaliado em operações de tratamento depende intrinsecamente da metodologia que será aplicada, e metodologia é método científico, não é opinião. O mais importante é ter clareza que o referencial dessa metodologia é o próprio titular dos dados, de modo que o produto final seja, de fato, uma documentação que mensura os riscos às liberdades civis e aos direitos fundamentais dos titulares (2020, p. 268).

Assim, uma metodologia de análise de riscos do ponto de vista da LGPD deve ser operacionalizada de forma lógica, fundamentada e condizente com as regras e princípios deste sistema.

Embora a LGPD traga consigo esta ferramenta de análise de riscos à proteção de dados pessoais, oriunda de um sistema mais avançado sobre a matéria, peca pela ausência do estabelecimento de regras claras quanto à sua obrigatoriedade, forma, conteúdo, prazo, publicação etc.

A legislação não fornece parâmetros suficientes para estas avaliações de risco, o que abre margem à proliferação de metodologias criadas pelos próprios agentes de tratamento. E não há nada de errado com isto. É, em verdade, proveitoso que metodologias diferentes surjam e sejam melhor aplicadas a determinados tipos de projetos ou segmentos de mercado, considerando-se as peculiaridades e circunstâncias de cada.

A metodologia não precisa ser demasiadamente complexa, mas suficiente para incorporar as informações relevantes quanto ao projeto concebido, as operações de tratamento de dados envolvidas, a natureza dos próprios dados e titulares afetados e o levantamento dos riscos existentes e indicação das medidas para endereçá-los.

Novamente, ressalta-se que a problemática reside justamente na implementação de metodologia segura que efetivamente direcione a análise de risco em relação aos direitos e liberdades dos titulares dos dados. São os direitos e liberdades dos titulares que constituem o ponto referencial da análise de risco deste instrumento.

5. CONSIDERAÇÕES FINAIS

Viu-se que a abordagem baseada no risco presente na LGPD, oriunda do modelo regulatório de proteção de dados europeu, impacta diretamente no que é considerado estar compliant e o que a lei requer em um caso em particular para o seu cumprimento, sendo o RIPD uma demonstração clara disso, pois orienta a identificação e análise dos riscos associados a determinado tratamento de dados pessoais pretendido por um agente e possibilita a modulação do próprio processo que está sendo concebido, de modo a proteger os titulares dos dados.

Contudo, a falta de definições e aprofundamento pela LGPD quanto à própria execução deste instrumento implica que o tema ainda será muito controvertido até, pelo menos, haver alguma suplementação normativa ou orientação por parte da Autoridade Nacional de Proteção de Dados, que mantém o assunto em sua agenda regulatória atual.

De todo modo, a legislação não estabelece metodologia obrigatória para a sua realização, o que poderá ser concebido e moldado por cada segmento de mercado, considerando suas particularidades.

Contudo, a experiência estrangeira mostra-se proveitosa ao fornecer pavimentação sólida para o uso do instituto em questão, especialmente considerando a origem comum compartilhada com a lei brasileira.

Assim, a avaliação de risco em privacidade e proteção de dados, seja na forma do PIA ou do DPIA, para além da mera condição de obrigatoriedade legal, é uma excelente ferramenta de análise e gestão de riscos, útil para conceber novos projetos colocando a privacidade em pauta desde os seus estágios iniciais, gerando benefícios à medida que fornece subsídios para a tomada de decisão na empresa.

Disto, a experiência estrangeira, especialmente no âmbito de aplicação do GDPR, deve ser considerada sob pena de serem aplicados institutos de maneira equivocada ou deixando-se de aproveitar todo seu potencial inerente.

A realização do RIPD, compreendendo-o enquanto processo, e não apenas um relatório, aplicando-o de forma metodológica, é capaz de erigir a proteção de dados dentro da ordem do dia nas atividades da empresa, elevando a conscientização da equipe ao longo do desenvolvimento de novos projetos.

Para isso, o processo deve ser realizado em etapas, visando, inicialmente, obter a descrição pormenorizada do tratamento de dados pretendido para, então, poder-se identificar e analisar os riscos aos titulares de dados, os quais deverão ser endereçados, seja para eliminá-los ou mitiga-los. Neste ponto, é importante

reforçar que os riscos são em relação ao titular de dados, e não à empresa.

Este processo tem o potencial de auxiliar a aprimorar o design do projeto bem como a comunicação sobre os riscos relacionados à privacidade entre as diferentes partes interessadas no contexto organizacional, protegendo, em último grau, os direitos e liberdades dos titulares de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

AEPD - AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. ***Gestión del riesgo y evaluación de impacto en tratamientos de datos personales***. Disponível em: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-nueva-guia-gestionar-riesgos-y-evaluciones-impacto. Acesso em 15 jun. 2021.

ALVES, Fabrício da Mota. **Avaliação de impacto sobre a proteção de dados**. In: MALDONADO, Viviane Nóbrega, BLUM, Renato Opice (coord.) Comentários ao GDPR. 2. ed. São Paulo: Thomson Reuters, 2019. p. 181-209.

ALVES, Fabrício da Mota; VIEIRA, Gustavo Afonso Sabóia. **Sem a ANPD, a LGPD é um problema, não uma solução**. 06 jan. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/anpd-lgpd-problema-solucao-06012020 Acesso em: 10 mar. 2021.

ANPD. **ANPD divulga cronograma completo de reuniões técnicas sobre relatório de impacto à proteção dos dados pessoais**. Governo Federal. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-cronograma-completo-de-reunioes-tecnicas-sobre-relatorio-de-impacto-a-protecao-dos-dados-pessoais. Acesso em: 17 jun. 2021.

GOVERNO FEDERAL (Autoridade Nacional de Proteção de Dados). **Portaria ANPD nº 11, de 27 de janeiro de 2021**. Portaria ANPD 11/2021. Brasilia, DF: Diário Oficial da União, 28 jan. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 Acesso em: 17 jun. 2021.

ARTICLE 29 DATA PROTECTION WORKING PARTY – WP 29. ***Opinion 3/2010 on the principle of accountability***. 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 18 jun. 2021.

ARTICLE 29 DATA PROTECTION WORKING PARTY – WP 29. WP 248 rev. 01. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento** (UE) 2016/679. 2017. Disponível em: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711 Acesso em: 13 mar. 2021.

AUSTRALIA. ***OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER***. *Guide to undertaking privacy impact assessments*. 2020. Disponível em: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/ Acesso em: 15 jun. 2021.

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

CLARKE, Roger. ***Privacy impact assessment: Its origins and development***. *Computer Law & Security Review*. Vol. 25, Issue 2, 2009. p. 123-135.

UNIÃO EUROPEIA. ***General data protection regulation***. 25/05/2018. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj Acesso em: 10 mar. 2021.

GOMES, Maria Cecília Oliveira. **Entre o método e a complexidade: compreendendo a noção de risco na LGPD**. In: PLAHARES, Felipe (Coord.) Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020. p. 245-272.

BRASL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF, 15 de agosto de 2018 e modificações 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 18 jun 2021.

ICO - INFORMATION COMMISSIONER'S OFFICE. ***Data protection impact assessments*** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments. Acesso em 18 jun. 2021.

ICO - INFORMATION COMMISSIONER'S OFFICE. ***Introduction to DPA 2018: Some basic concepts***. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/#3. Acesso em 18 jun. 2021.

PALHARES, Felipe. **Procedimentos específicos a serem adotados pelos agentes de tratamento**. In: NOBREGA, Viviane 4(Coord.). Manual do DPO: *Data Protection Officer*. 1 ed. São Paulo: Thomson Reuters Brasil, 2021. p. 129-151.

QUELLE, Claudia. ***The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too***. SSRN. 19/07/2017. Disponível em: https://ssrn.com/abstract=3000382. Acesso em 18 jun. 2021.

KLOZA, Dariusz; et. al. ***Data protection impact assessment in the European Union: developing a template for a report from the assessment process***. *VUB - Vrije Universiteit Brussel*. 11/11/2020. Disponível em: https://researchportal.vub.be/en/publications/data-protection-impact-assessment-in-the-european-union-developin Acesso em: 5 jun. 2021.

SANDBOX REGULATÓRIO NO BRASIL E NO MUNDO

Adriana Siliprandi
Advogada e Administradora, mestranda em Direito Empresarial pela Unicuritiba. Consultora em projetos com protocolos blockchain.

Ana Gabriela Bandeira
Acadêmica de Direito da Universidade Estadual do Oeste do Paraná – UNIOESTE.
anagabiband@hotmail.com

Rodrigo Benez Baracat
Administrador de Empresas
rodbaracat@gmail.com

RESUMO:
A tecnologia financeira entrou em uma fase de rápido desenvolvimento, marcada pela proliferação de startups e outros novos *players*, como empresas de TI e comércio eletrônico, que estão fragmentando o mercado de serviços financeiros. Essa nova era apresenta novos desafios para os reguladores e evidencia que a criação de novos produtos para o mercado financeiro necessita que a regulação seja desenvolvida em paralelo. Em particular, os reguladores devem desenvolver uma estrutura robusta que promova a inovação e a confiança do mercado, sendo apontado como ferramenta para isso, por diversas autoridades reguladoras no mundo, o *Sandbox* regulatório. O presente trabalho demonstra brevemente, por meio de pesquisa bibliográfica, como funciona a regulação tradicional do mercado financeiro e quais são os seus objetivos, as principais características do *Sandbox* regulatório, bem como os modelos que estão sendo utilizados

no mundo. Por fim, serão apresentados os modelos brasileiros de *Sandbox*, iniciativas lançados pelas três maiores autarquias brasileiras no mercado financeiro, o Banco Central do Brasil, a Comissão de Valores Mobiliários e a Superintendência de Seguros Privados.

Palavras-Chave: Direito; Regulação. *Sandbox*. Novas tecnologias. Inovação.

Sumário: 1. Introdução; 2. Regulação No Mercado Financeiro; 3. *Sandbox* Regulatório; 3.1. *Sandbox* No Mundo; 3.2. *Sandbox* No Brasil; 4. Conclusão; Referências Bibliográficas.

1. INTRODUÇÃO

Nas últimas décadas, a expansão do acesso à internet e sua capacidade de gerar valor e conectar pessoas remodelou a sociedade e o modo com que os indivíduos se relacionam.

Nesse contexto marcado pelo surgimento de inovações tecnológicas como inteligência artificial e a *blockchain*, vários empreendimentos têm testado e lançado produtos disruptivos nos mercados regulados.

Contudo, tais empreendimentos encontram barreiras em algumas indústrias, como o mercado financeiro de capitais, devido às limitações regulatórias, que podem sufocar o potencial inovador de novos produtos.

Tais barreiras surgem visto que o regulador tem tido dificuldade de acompanhar a rapidez com que essas tecnologias são inseridas na vida do consumidor, causando insegurança jurídica aos novos empreendedores, frente ao desconhecimento dos limites legais em que a lei os permite operar.

O Direito, em diversas situações disruptivas, vem a reboque dos fatos, pois tais modelagens avançam na vida social e velocidade incompatível com os movimentos normativos; o que se observa na maioria dos casos é um grande lapso temporal separando a popularização da utilização de novas dinâmicas e tecnologias e a regulamentação legal.

Entretanto, diante da grande relevância na economia, tem caráter urgente a compreensão e a incorporação dessas tecnologias no estudo e aplicação do Direito, pois se consolidam como elementos integrantes das relações sociais e suas instituições.

Em tal contexto, é pertinente que a construção da regulação ocorra em concomitância com o surgimento das novas dinâmicas criadas a partir das inovações tecnológicas.

Visando responder a está necessidade, autoridades regulatórias de vários países, incluindo Inglaterra, Cingapura e Brasil tem apresentado uma postura ativa para encontrar a solução regulatória apropriada, estabelecendo programas de *Sandboxes* Regulatórios, ambientes em que empresas são autorizadas a lançar seus produtos ao mercado sob supervisão do regulador, estimulando a inovação e ao mesmo tempo garantindo estabilidade ao mercado.

2. REGULAÇÃO NO MERCADO FINANCEIRO

Conforme descreve Armour et. al (2016, p. 61) a regulação financeira é frequentemente justificada pela necessidade de corrigir falhas de mercado relevantes.

Nesse conceito se enquadram as metas perseguidas pelos formuladores de políticas públicas nessa área. Portanto, olhar para os objetivos legítimos da regulação financeira ajuda a avaliar os

méritos das possíveis soluções propostas para resolver esse problema (ARMOUR et. al, 2016, p. 61).

Consideram-se como objetivos da regulação financeira: (i) proteção ao investidor; (ii) proteção do consumidor no financiamento de varejo; (iii) estabilidade financeira; (iv) eficiência do mercado; v) concorrência; (vi) prevenir crimes financeiros (ARMOUR et al., 2016, p. 63).

A atuação tradicional dos órgãos reguladores geralmente é pautada por processos poucos flexíveis e em resposta a práticas de mercado que já se encontram amplamente difundidas, uma postura reativa frente à evolução das condutas dos regulados (COUTINHO, 2018, p. 2).

Especialmente quando a discussão gira em torno de modelos de negócios totalmente disruptivos, como está ocorrendo com ativos digitais no momento, há preocupações razoáveis de que uma medida regulatória inadequada possa sufocar a inovação, impondo uma obrigação excessivamente onerosa aos empreendimentos (BARBOSA, 2019, p. 17).

Por exemplo, equívocos na aplicação ou desenvolvimento da regulação de novos mercados poderiam tornar os novos negócios menos competitivos em comparação com participantes tradicionais do mercado, que tem maior facilidade de absorver os custos agregados à carga regulatória (BARBOSA, 2019, p. 17).

Sobre o marco regulatório Barbosa argumenta que:

> (...) Por padrão, existe um marco regulatório para o setor financeiro já estabelecido. Independentemente de ser mais ou menos adequado para regular novas tecnologias, fato é que ele precisa ser aplicado, como consequência do Estado de Direito. Ou seja, até que sobrevenha norma que suspenda ou afaste a aplicação das normas regulatórias

> vigentes para o caso ou um novo estatuto seja aprovado suplantando o anterior, o antigo marco regulatório precisa ser aplicado sempre que couber. (BARBOSA, p. 17).

Desta maneira por tratarem-se novos produtos financeiros ou atividades disruptivas, a regulação em muitos casos, fica entre o vazio normativo e as zonas de penumbra das normas já vigentes, evidenciando que a busca por novos meios de se produzir a regulação, com a aproximação entre o regulador e os jurisdicionados pode ser a melhor resposta. Entre os elementos de regulação pode-se citar o *Sandbox* traduzido do inglês como caixa de areia, sendo uma terminologia adotada pelos profissionais da área de tecnologias da informação, consistindo em experimentos realizados segundo um conjunto de regras pré-definidas, mas que não se encontram necessariamente regulamentadas (EXAME, 2020).

3. SANDBOX REGULATÓRIO

Sandboxes Regulatórios concedem licença temporária para empresas elegíveis testarem suas soluções, em um ambiente livre de consequências legais (ARNER et. al, 2017, p. 22).

Para a doutrina jurídica, é um "instrumento regulatório de fomento baseado em incentivo regulatório por meio de experimentalismo estruturado, tendo como pilar indutivo a isenção normativo-regulatória temporária" (BRUZZI; KNOB, 2019).

São iniciados por instituições públicas com função regulatória ou monetária e comumente estabelecido após processos de consulta pública nos quais as partes interessadas do ecossistema estão engajadas para ajudar a moldar as atividades da área restrita (BROMBERG et. al, 2017, p. 5).

Em suma, o *Sandbox* Regulatório permite que as empresas testem seus produtos e serviços com um número limitado de consu-

midores e investidores, enquanto os reguladores supervisionam a atividade, sem ter que cumprir as mesmas regras estabelecidas para o setor (ALLEN, 2017, p. 709).

Esse instrumento busca aproveitar a período de incerteza quanto à melhor resposta regulatória para observar e aprender mais sobre a tecnologia, ao tempo em que testa medidas regulatórias e mede as consequências de sua implantação em um ambiente controlado. Em regra, a ideia é que também haja tempo para acompanhar o desenvolvimento da matéria em outros lugares do mundo, comparando os modelos regulatórios adotados em outros países e as seus efeitos práticos (FINCK, 2018, p. 665).

É um modelo que incentiva a aproximação entre o regulador e o mercado, criando um canal de diálogo e cooperação para superar em conjunto as incertezas de uma nova tecnologia, tornando possível controlar o risco de sufocar a inovação e ao mesmo tempo que se protege o interesse público, objetivo da regulação.

Fan (2018, p. 347), destaca que os sandboxes não eliminam o risco de falência comercial, um fator determinante da inovação, mas sim, reduzem as consequências dos testes para os consumidores e para a estabilidade do mercado financeiro. Consequentemente, os *sandboxes* reduzem o risco sistêmico.

Nesse sentido, uma das grandes vantagens do modelo é oferecer uma resposta regulatória aos primeiros empreendimentos lançados no mercado, enviando uma mensagem positiva aos empreendedores ao proporcionar alguma segurança jurídica e incentivando a inovação, em vez de onerá-los em estágio inicial com uma regulação excessiva ou inaplicável.

3.1 SANDBOX NO MUNDO

A abordagem de *Sandboxing* foi lançada pelo Reino Unido em 2015 pela *Financial Conduct Authority (FCA)*, chamado de *Project Innovate*, aprovando em 2016 a primeira *Fintech* a oferecer serviços em *Sandbox* (FCA, 2021).

A *Financial Conduct Authority*, a entidade reguladora inglesa, anunciou que o seu *Sandbox* é um "Espaço seguro no qual as empresas podem testar produtos, serviços, modelos de negócios e mecanismos de entrega inovadores sem incorrer imediatamente em todas as consequências regulatórias normais de se envolver na atividade em questão" (FCA, 2021).

O modelo britânico permite que os empreendedores testem novas tecnologias em um ambiente leve, mas claramente regulamentado, sob estreita supervisão e por um período definido de tempo.

Os três principais objetivos do *Sandbox* são: reduzir o *time-to--market*; melhorar o acesso ao financiamento e encorajar a inovação (MOYLE; MACLEAN, 2016)

Visando proteger os consumidores e a estabilidade sistêmica do mercado, a entidade propôs abordagens alternativas para facilitar o envolvimento do consumidor dentro do *Sandbox*. Para alguns foi exigido consentimento informado para experimentar das inovações, em outros foi concedido ao consumidor os mesmos direitos desfrutados por clientes fora do ambiente regulado (FCA, 2021).

A *Financial Conduct Authory* também focou em analisar a capacidade das empresas compensarem os participantes, exigindo a demonstração de disposição de recursos financeiros para com-

pensar qualquer perda sofrida pelos clientes em razão do uso de seu produto (MOYLE; MACLEAN, 2016).

Assim, infere-se que o FCA assumiu a liderança no desenvolvimento de uma estrutura robusta e estruturada para o teste eficiente de produtos e serviços financeiros inovadores, visto que os *sandboxes* apresentam grande promessa no suporte e desenvolvimento do direito regulatório e da atividade regulatória estatal em novas tecnologias.

Baseadas nesse modelo, diversas autoridades regulatórias de outras jurisdições também expressaram abertura ao uso de *sandboxes*, incluindo Abu Dhabi, Austrália, Malásia, Hong Kong, Cingapura, Suíça e Tailândia.

3.2. SANDBOX NO BRASIL

O Brasil tem atualmente três iniciativas de *Sandbox* Regulatório iniciados em conjunto com o Ministério da Economia, cada uma com suas regras e cronogramas específicos, liderados por três importantes reguladores: Superintendência de Seguros Privados (SUSEP), Comissão de Valores Mobiliários (CVM) e o Banco Central DO Brasil (BACEN), que trabalharão em conjunto em projetos que estejam inclusos em suas competências, com a formação de comitê formado por membros das três instituições (BRASIL, 2019).

A opção pela criação de três ambientes independentes, com três focos distintos, diferencia o Brasil do Reino Unido, por exemplo, que tem apenas um *Sandbox* Regulatório, instituído pela *Financial Conduct Authority – FCA*, a entidade reguladora da atividade financeira local.

3.2.1. SANDBOX REGULATÓRIO DA SUSEP

O *Sandbox* Regulatório da SUSEP foi o primeiro a ser lançado no Brasil, por meio da disponibilização dos editais de Consulta Pública n. 09/2019 e 10/2019.

Após a conclusão das consultas públicas e das contribuições apresentadas pela sociedade civil, foi criado o ambiente regulatório experimental em âmbito securitário, pela edição da Resolução n. 381/2020 do Conselho Nacional de Seguros Privados (CNSP) e da Circular n. 598/2020 da SUSEP.

O objetivo é criar as condições especiais, limitadas e exclusivas, para autorizar, por tempo determinado, o funcionamento das sociedades seguradoras participantes, para o desenvolvimento de projetos inovadores.

Foi considerado pela Resolução como projeto inovador, o produto ou serviço no mercado de seguros que seja oferecido ou desenvolvido a partir de novas metodologias, processos, procedimento ou de tecnologias existentes aplicadas de modo diverso (BRASIL, 2020). Observou-se que, para ser elegível para o projeto, o participante deveria demonstrar de forma contundente, como seu produto pode ser empregado no mercado e os benefícios finais que trará aos consumidores.

Além disso, foi analisada a capacidade de emprego da nova tecnologia, a redução de custos para o consumidor, a escalabilidade do produto e possibilidade de ser comercializado fora do *Sandbox*, a experiencia dos sócios e se o processo de contratação é simplificado (BRASIL, 2020).

Foram analisados 14 projetos inscritos e selecionados 11 participantes para o primeiro ciclo do Sandbox, aos quais foi concedida

uma autorização por tempo determinado para operar no setor de seguros com regras diferenciadas, por até 36 (trinta e seis) meses (BRASIL, 2020).

Os serviços oferecidos pelos participantes aprovados incluem tablets, smartphones e dispositivos portáteis, automóveis, animais domésticos, acidentes pessoais, funeral, residência e estabelecimentos comerciais. Haverá oferta de seguros intermitentes, utilizados sob demanda, bem como seguros paramétricos para desastres, de acordo com alertas das autoridades públicas de cada Estado (BRASIL, 2020).

3.2.3. SANDBOX REGULATÓRIO DA COMISSÃO DE VALORES MOBILIÁRIOS

O *Sandbox* da Comissão de Valores Mobiliários (CVM) foi o segundo a ser lançado no Brasil, proporcionando autorização temporária para que empresas participantes recebam autorização temporária para testar seus modelos de negócio no mercado de capitais. O processo teve início com a publicação do edital de Audiência Pública SDM 2019, que foi elaborado com base nas experiências do Reino Unido e Cingapura, com objetivo de criar um ambiente seguro para o lançamento de produtos e serviços inovadores no mercado de capitais (CVM, 2020).

Um dos temas abordados no Relatório de Análise da Audiência Pública SDM n. 05/19, em resposta aos questionamentos das empresas *HashInvest*, MD8 e da Associação Brasileira de Criptoativos e *Blockchain* (ABCB), foram as criptomoedas, que atualmente não possuem nenhuma regulação por parte da CVM, por não serem considerados formalmente como ativos financeiros. (CVM, 2019)

Apesar disso, em resposta, a autarquia respondeu que a ausência de caracterização como criptoativos não significa necessariamente a inelegibilidade das atividades relacionadas a criptoativos para o *Sandbox* (CVM, 2019). Assim, infere-se que mesmo que criptomoedas não possuam nenhuma regulação no Brasil, dentro do ambiente regulado da CVM, caso aprovados, poderão ser oferecidos produtos que utilizem tal tecnologia.

A principal diferença no modelo adotado pela CVM é a exigência de que o projeto inovador tenha sido validado previamente e esteja pronto para ser lançado no mercado, com todos os ônus exigíveis, excetos aqueles para os quais o participante tenha obtido dispensas regulatórias específicas, não permitindo a participação de empresas que desenvolvam seus produtos dentro do ambiente do *Sandbox* (CVM, 2021, p. 20).

Ademais, também foi ressaltado pelo regulador que o processo de admissão para o *Sandbox CVM* não deve ser utilizado como instância consultiva e as eventuais incertezas consignadas nas propostas de participação podem indicar um grau de imaturidade no projeto que torne inadequado para participação no programa (CVM, 2021, p. 20)

Ao final, para obter o registro junto à CVM, os participantes devem solicitar formalmente ao Comitê de *Sandbox*, responsável por orientá-los sobre o pedido de registro junto à Superintendência do respectivo órgão, a quem cabe à análise do requerimento, levando em consideração os dados obtidos durante o período de monitoramento no ambiente regulado.

Até o momento não foi divulgado pela autarquia quais participantes serão aprovados para participar do *Sandbox*. Foram recebidos 33 projetos, mas em primeira análise apenas 6 (seis) foram considerados aptos, mas ainda precisam de um maior aprofunda-

mento do Comitê de *Sandbox* no tocante à operacionalização dos modelos de negócio, razão pela qual foi anunciada a prorrogação do prazo para análise em relação a essas propostas até o dia 30 de setembro de 2021 (CVM, 2021, p. 19). Entretanto, a prorrogação não implica que todas as propostas em analise serão aprovadas, ainda sendo necessária decisão do Colegiado quanto à concessão da autorização temporária, após de prestados os esclarecimentos necessários.

Na sequência a CVM publicou documento sobre Considerações do Comitê de *Sandbox* Acerca do 1o Processo de Admissão, com esclarecimentos sobre o processo de admissão e a razão pela qual a maioria das propostas foi considerada inapta.

Nesse documento foi ressaltado que o *Sandbox* Regulatório abarca apenas atividades contidas dentro do perímetro regulatório da CVM, não sendo possível conferir autorizações temporárias para atividades as quais a Autarquia não tem competência legal para autoriza ou conceder dispensas de requisitos estabelecidos por força de lei (CVM, 2021, p. 6).

A comissão esperava que os proponentes indicassem claramente os obstáculos específicos que os impedem de exercer atividades regulamentadas no regime ordinário e as dispensas de requisitos regulatórios pretendidas para o exercício de tais atividades em regime diverso (CVM, 2021, p. 6).

Contudo, pelas informações apresentadas pela CVM, várias propostas solicitaram a dispensa de registro e o afastamento completo da aplicação de determinadas normas, mesmo quando indicavam a pretensão de exercer as atividades por elas reguladas no âmbito do *Sandbox* Regulatório (CVM, 2021, p. 11).

Nesses casos, a autarquia considerou incompatíveis os pedidos

de autorização para o exercício de determinada atividade e a concomitante solicitação de dispensa de registro ou do afastamento da aplicação de toda a regulamentação que dispõe sobre o exercício de tal atividade, recusando tais propostas por inaptidão, com base no inciso II do art. 6o da Resolução CVM 29 (CVM, 2021, p. 11).

Também foi indicado o encaminhamento de propostas que requeriam o desenvolvimento de novos regimes regulatórios, o que foi rejeitada pela CVM, que argumentou que a característica do Sandbox é conceder autorizações com base na regulação vigente, tendo menos flexibilidade para propostas que de partida já indiquem a necessidade de construção de um regime novo para o exercício de determinada atividade na qual se basearia para conceder tal autorização (CVM, 2021, p. 15).

A justificativa para a rejeição dessas propostas é de que, mesmo o mais inovador dos modelos de negócios poderia, em tese, assimilar parte do ônus regulatório de uma regulamentação vigente e testar o regime modulado com as dispensas de requisitos regulatórios que não se coadunam ao seu modelo de negócios, permitindo ao regulador avaliar a capacidade da inovação implantada em cumprir os objetivos da regulação vigente, mesmo sem a imposição de toda a carga regulatória, servindo de subsidio para o aprimoramento de suas normativas (CVM, 2021, p. 15).

Da mesma forma, foram consideradas inaptas as propostas em que foi solicitado a dispensa de autorização para exercer atividades reguladas com o fim único de viabilizar a própria captação do participante ou a comercialização de seus produtos, visto que não são voltadas a prestação de serviços a terceiros, de forma a oportunizar o acesso ao mercado a outros emissores interessados, mas apenas para viabilizar emissões próprias dos proponentes (CVM, 2021, p. 14).

3.2.3. SANDBOX REGULATÓRIO DO BANCO CENTRAL DO BRASIL

O *Sandbox* lançado pelo Banco Central do Brasil (BACEN) tem o objetivo de permitir que empresas ofereçam seus produtos com segurança jurídica e seu acompanhamento em tempo real (BACEN, 2021).

Foi baseado nas experiências internacionais, principalmente do Reino Unido e da Espanha.

Com essa iniciativa, o Banco Central busca abrir o mercado para novos players e trazer mais soluções bancárias e de meio de pagamento ao consumidor, acompanhando projetos já amadurecidos, nos quais há a necessidade de validar o modelo de negócio por meio de sua implementação efetiva, oferecendo produtos e serviços a clientes reais.

As entidades aprovadas a participar são autorizadas, para testar, por período determinado, projetos inovadores na área financeira ou de pagamento, observando um conjunto específico de disposições regulamentares que amparam a realização controlada e delimitada de suas atividades (BRASIL, 2020).

Ao mesmo tempo, o banco irá monitorar a implementação e os resultados dos projetos, sendo capazes de avaliar os riscos associados aos novos produtos e serviços e, caso identifique inadequação no gerenciamento dos riscos associados à execução do projeto pelo participante, poderá determinar o aperfeiçoamento do projeto ou até estabelecer limites para a sua comercialização em larga escala (BACEN, 2021).

Ao longo do ciclo do *Sandbox*, o regulador avaliará se a execução dos projetos e o fornecimento de produtos e serviços estão

sendo satisfatórios. Caso positivo, poderá promover ajustes na regulamentação e permitir que esses produtos e serviços sejam fornecidos de maneira permanente no Sistema Financeiro Nacional e no Sistema de Pagamentos Brasileiro (BACEN, 2021).

O BACEN recebeu 52 inscrições de projetos interessadas a participar da seleção e devido a esse grande número de propostas o Comitê Estratégico de Gestão do *Sandbox* prorrogou em 90 (noventa) dias o prazo final para avaliação dos projetos, com previsão para divulgação em 23 de setembro de 2021.

4. CONCLUSÃO

Quando confrontados com novas tecnologias que têm o potencial de causar movimentos disruptivos no mercado regulado, o regulador tem o trabalho dificultoso de decidir se lhe é exigida alguma ação e qual é o momento correto para intervir.

No momento atual, em que diversos novos produtos e serviços que desafiam a estrutura regulatório tradicional estão sendo lançados ao mercado, a ferramenta mais utilizada pelos reguladores em todo o mundo tem sido os *Sandboxes* regulatórios.

Em primeira análise tal ferramenta aparenta ser benéfica para todas as partes, visto que permite testar abordagens novas e mais flexíveis que criem um ambiente de dialogo saudável com os empreendedores, sem lhes impor a totalidade da carga regulatório na fase de validação de seus produtos, mas ainda protegendo os consumidores com estruturas e procedimentos de mitigação de riscos.

Seu verdadeiro potencial transformador reside na sua capacidade de permitir o monitoramento em tempo real do mercado, facilitando uma renovação no método de criação da

regulação financeira.

Em especial nos casos brasileiros apresentados ao longo do artigo, observa-se que apesar de estarem em fases iniciais, já se mostraram muito bem estruturados e fomentaram a inovação no mercado financeiro, principalmente na criação de canais de comunicação e interação direta entre os participantes e o regulador.

Contudo, é necessário observar de perto como se desenvolverão os projetos nos Sandboxes e a regulação que será criada em consequência para afirmar se essa nova abordagem trará benefícios efetivos ao mercado ou não.

Conclui-se que, essa nova ferramenta já aponta para uma tendência por parte de reguladores de todo o mundo de trazer mais dinamismo e eficiência a maneira como se desenvolve a regulação do mercado financeiro, ao reconhecer que as estruturas tradicionais não são suficientes para acompanhar a maneira como as dinâmicas sociais estão evoluindo.

REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, Hilary J., ***Regulatory Sandboxes***. George Washington Law Review. Washington College of Law. vol. 87, n. 3, p. 580-644, 2019. Disponível em: https://ssrn.com/abstract=3056993. Acesso em: 19 nov. 2021.

ARMOUR, John; AWREY, Dan; DAVIES, Paul; ENRIQUES, Luca; GORDON, Jeffrey N.; MAYER, Colin; PAYNE, Jennifer, ***Principles of Financial Regulation***. New York, NY: Oxford University Press, 2016.

ARNER. Douglas; JANOS, Barberis; Ross, Buckley. F***intech and Regh-Tech in a nutshell, and future in a sandbox***. *Research Foundation Briefs*, p. 1-20, 2017. Disponível em: https://www.cfainstitute.org/research/foundation/2017/fintech-and-regtech-in-a-nutshell-and-the-future-in-a-sandbox. Acesso em: 01 ago.2021.

BACEN – BANCO CENTRAL DO BRASIL. ***Sandbox* Regulatório**. 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/sandbox. Acesso em 01. ago. 2021.

BARBOSA, Marcos Vinicius Cardoso. ***Blockchain* e o Mercado Financeiro e de Capitais: Riscos, Regulação e *Sandboxing***. Disponível em: https://www.insper.edu.br/wp-con-tent/uplo-ads/2019/04/20190821_blockchain_mer-cado_financeiro_capi-tais_riscos_regulacao_sand-boxing.pdf. Acesso em: 11 ago. 2021.

BRASIL. Secretaria Especial da Fazenda do Ministério da Economia; Banco Central do Brasil; Comissão de Valores Mobiliários; Superintendência de Seguros Privados. **Comunicado Conjunto, de 13 de junho de 2019**. Disponível em: https://bit.ly/2Ynj0hc. Acesso em: 01 ago. 2021.

_____. Ministério da Economia/ Banco Central do Brasil. **Resolução CMN nº 4.865, de 26 de outubro de 2020**. Resolução nº 4.865/20. Brasília, Diário Oficial da União, 27 out 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n--4.865-de-26-de-outubro-de-2020-285019649. Acesso em: 11 ago. 2021.

_____. Ministério da Economia / Conselho Nacional de Seguros. **Resolução nº 381, de 4 de março de 2020**. Resolução n. 381/2020. Brasília, Diário Oficial da União, 06 mar 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-381-de-4-de--marco-de-2020-246507718. Acesso em: 01 ago. 2021.

_____. Ministério da Economia / Conselho Nacional de Seguros. **Circular nº 598, de 19 de março de 2020**. Circular n. 598/2020. Brasília, Diário Oficial da União, 20 mar 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/ circular-n-598-de-19-de-marco%20de-2020-249021945. Acesso em: 01 ago. 2021.

BROMBERG, Lev; GODWIN, Andrew; RAMSAY, Ian. ***Fintech sandboxes: achieving a balance between regulation and innovation***. Journal of Banking and Finance Law and Practice, v. 28, n. 4, p. 314-336, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090844. Acesso em: 01 ago. 2021.

BRUZZI, Eduardo; KNOB, Yasmin. ***Sandbox* regulatório no Brasil**. Justiça & Cidadania, Opinião e Editoriais, 4 jan. 2021. Disponível em: https://editorajc.com.br/sandbox-regulatorio-no-brasil/. Acesso em 11 ago. 2021.

COUTINHO FILHO, Augusto. **Regulação *'Sandbox'* como instrumento regulatório no mercado de capitais: principais características e prática internacional**. Revista Digital de Direito Administrativo. Universidade de São Paulo. vol. 5, n. 2, p. 264-282,

2018. Disponível em: https://www.revistas.usp.br/rdda/article/view/141450. Acesso em: 19 nov. 2021.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Considerações do Comitê de *Sandbox* Acerca do 1o Processo de Admissão**. Disponível em: http://conteudo.cvm.gov.br/export/sites/cvm/menu/investidor/30062021__Documento_de_Consideracoes_do_CDS. Acesso em 08/09/2021.

CVM - COMISSÃO DE VALORES MOBILIÁRIOS. **Instrução CVM nº 626**, de 15 de maio de 2020. Dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental (*sandbox* regulatório). Disponível em: http://conteudo.cvm.gov.br/legislacao/instrucoes/inst626.html. Acesso em: 11 ago.2021.

_____. Relatório de Análise. **Audiência Pública SDM nº 05/19. 2019**. Disponível em: http://conteudo.cvm.gov.br/export/sites/cvm/audiencias_publicas/ap_sdm/anexos/2019/sdm0519_relatorio.pdf. Acesso em: 11 ago.2021.

EXAME. ***Sandbox* Regulatório: entenda o que é e para que serve**. *Future of Money*, 30.11.2020. Disponível em: https://exame.com/future-of-money/sandbox-regulatorio-entenda-o-que-para-que-serve/. Acesso 11 ago. 2021.

FAN, Pei Sai. ***Singapore approach to develop and regulate FinTech***. *Handbook of Blockchain, Digital Finance, and Inclusion. Amsterdam*, v.1, p. 347-357, 2017. Disponível em: https://doi.org/10.1016/B978-0-12-810441-5.00015-4. Acesso em: 11 ago.2021.

*FCA - FINANCIAL CONDUCT AUTHORITY. **Regulatory Sandbox The regulatory sandbox allows businesses to test innovative propositions in the market with real consumers***. Publicada em 10/05/2015. Atualizada 17.08.2021. Disponível em: https://www.fca.

org.uk/firms/innovation/regulatory-sandbox. Acesso em: 19 nov. 2021.

FINCK, Michele. ***Blockchains: Regulating the Unknown***. *German Law Journal, 19(4), 665-692*. Disponível em: https://www.cambridge.org/core/journals/german-law-journal/article/blockchains--regulating-the-unknown/38770CD33494CE55811A546F6FB949B7. Acesso em: 11 ago.2021.

MOYLE, Andrew; MACLEAN, Fiona. ***World-First Regulatory Sandbox Open for Play in the UK***. *Latham & Watkins Technology Transactions Practice and Financial Institutions Industry Group, n. 1964, May 9, 2016*. Disponível em: https://www.lw.com/thoughtLeadership/LW-world-first-regulatory-sandbox-open-for-play-in-UK. Acesso em: 01 ago. 2021.

SECRETÁRIA ESPECIAL DA FAZENDA DO MINISTÉRIO DA ECONOMIA; BANCO CENTRAL DO BRASIL; COMISSÃO DE VALORES MOBILIÁRIOS E SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **Comunicado Conjunto, de 13 de junho de 2019**. Disponível em: https://www.gov.br/cvm/pt-br/assuntos/noticias/comunicado-conjunto-de-13-de--junho-de-2019-8dd7407271404b5ebe04f5150d3aa36c. Acesso em 01/08/2021.

VIANNA, Eduardo Araújo Bruzzi. **Regulação das *fintechs* e sandboxes regulatórias**. Dissertação (Mestrado). Fundação Getúlio Vargas - FGV, Rio de Janeiro, RJ. Disponível em: https://bibliotecadigital.fgv.br/dspace/themes/Mirage2/pages/pdfjs/web/viewer.html?file=http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27348/DISSERTAC%cc%a7A%cc%83O_EDUARDO_BRUZZI.pdf?sequence=1&isAllowed=y. Acesso em: 01 ago. 2021.

CYBER GROOMING COMO VIOLÊNCIA SEXUAL CONTRA CRIANÇAS E ADOLESCENTES

CYBER GROOMING AS SEXUAL VIOLENCE AGAINST CHILDREN AND ADOLESCENTS

Andrea Damasceno de Barros
Advogada. Cursando pós-graduação em Direito Penal e Criminologia pelo Instituto de Criminologia e Política Criminal - ICPC. Especialista em Direito pela Escola do Ministério Público do Paraná - FEMPAR. Graduada em direito pela Pontifícia Universidade Católica do Paraná - PUCPR.
andreadbarros.adv@gmail.com

RESUMO:
O surgimento de novas tecnologias propiciou a prática de condutas ilícitas através dos meios virtuais. O aumento dos crimes sexuais contra crianças e adolescentes no meio virtual demanda especial atenção do Estado e da sociedade civil, culminando com o desenvolvimento de políticas públicas visando a prevenção, mas também a criminalização de novas práticas, assim como agravamento das penas daquelas já existentes, adequando o tratamento à realidade cibernética. Tratamos especialmente da previsão legal do *cyber grooming* no Brasil, por meio de uma pesquisa bibliográfica, apontando dados de pesquisas de diversas entidades de combate à violência infanto juvenil, assim como a abordagem adotada na prática dos julgamentos, mencionando também o tratamento dado por outros países. Ressalta-se a necessidade de ações conjuntas objetivando, mais do que tudo, a mudança da cultura que ainda hoje acaba por normalizar a violência praticada contra crianças e adolescentes.

Palavras-Chave: Violência. Criança e adolescente. Crimes virtuais. *Cyber Grooming*.

ABSTRACT:
The emergence of new technologies has led to the practice of illicit conduct through virtual means. Special attention has been paid to the in sexual crimes against children and adolescents in the virtual en vironment, which demands special attention from the State and civil society, culminating in the development of public policies aimed at prevention, but also the criminalization of new practices and aggravation existing sentences, appropriated the treatment of cyber reality. We deale specially with the legal forecast of cyber grooming in Brazil, pointing to research data from various entities to combat y outh violence as wellas the approach adopted in the practice of judgments, also mentioning the treatment given by other countries. We emphasize the need for joint actions aiming, more than anything, the change of culture that still ends up normalizing the violence practiced against children and adolescents.

Keywords: *Violence. Child and adolescent. Virtual crimes. Cyber grooming.*

1. INTRODUÇÃO

As evoluções tecnológicas vivenciadas pela sociedade moderna causaram notável impacto na vida quotidiana. Incontáveis benefícios surgem dia após dia em todas as áreas do conhecimento.

Infelizmente não é apenas o bônus que impacta. Uma gama numerosa de condutas ilícitas passou a ser praticada no meio virtual. Novos crimes foram tipificados e outros adequados à realidade do ciberespaço, que vem sendo utilizado indiscriminadamente em razão da sensação de anonimato e consequente impunidade dos agentes. Neste contexto, os crimes de ordem sexual praticados contra crianças e adolescentes acabam sendo foco da preocupação constante dos diversos órgãos de poder e da sociedade civil.

A legislação precisou evoluir, assim como as técnicas de acompanhamento, investigação, processamento e aplicação de penas. Além de quebrar as barreiras entre o mundo real e o cibernético é necessário atingir agentes que estão fora das fronteiras do país.

O presente artigo busca traçar a evolução do sistema de proteção da criança e do adolescente, principalmente no tocante às normas de natureza penal que criminalizam condutas praticadas no meio virtual, tratando especificamente do *cyber grooming* ou aliciamento/assédio, um ato preparatório para a prática de crimes mais graves, tanto no meio virtual quanto real, que acabou por ser criminalizado na tentativa de barrá-los, já que por si só representa um ato de violência contra a criança, causador de danos permanentes.

A pesquisa utiliza metodologia descritiva qualitativa baseada em fontes bibliográficas como bancos de registros de dados, artigos científicos, legislações, decisões de tribunais, dissertações e

reportagens jornalísticas relativas ao tema.

2. EVOLUÇÃO HISTÓRICA DA PROTEÇÃO À CRIANÇA

Análises históricas permitem afirmar que a preocupação com a infância é uma realidade moderna. Na antiguidade havia poucos registros sobre as crianças, às quais a sociedade reservava a indiferença. Ausente qualquer sentimentalismo, predominava a ideia de que a superação da infância, entendida como situação de animalidade, irracionalidade e ausência de consciência moral, era a garantia de se tornar cidadão humano, detentor de caráter, inteligência e competência. (CECCIM; PALOMBINI, 2009).

Os índices de mortalidade infantil eram altíssimos, reflexo da carência de higiene que dominava a população. A criança era vista como um adulto em miniatura, por isso não gozava de proteção e cuidados especiais.

Até a era cristã o infanticídio era comum. Expunham-se as indesejadas à morte pelo abandono, lançamentos ao mar e à fogueira, sacrificadas em rituais e mutilações. Os números eram tão altos que a partir do século XIII a Igreja passou a orientar os hospitais para que recolhessem os indesejados, quando se tornou hábito a entrega dos filhos a Deus.

Na sequência, a Igreja atribui caráter angelical às crianças, representando a pureza e bondade, que deviam ser substituídos na vida adulta, definitivamente, pela moral. Vistas, então, como a imagem da esperança, no século XVI houve a disseminação de colégios religiosos, os quais estavam mais para reformatórios com foco no "adestramento moral, disciplinamento físico e rigidez de pensamento" (CECCIM; PALOMBINI, 2009). Elas deveriam se tornar o adulto ideal, que quando homem tornaria-se o pai (a mulher e os filhos integravam os direitos patrimoniais do pai),

detentor único de direito e proteção.

> O modelo de caracterização do humano que veio sendo construído no plano da visibilidade (no interior da moral e da lei) desde a Antiguidade até a Modernidade é o modelo de homem como sexo masculino, raça branca, adulto, de orientação heterossexual, detentor das faculdades de raciocínio lógico e consciência, possuidor de grande força física, que dá nome à família, possuindo bens e patrimônio que honram esse nome. Temos aí uma representação proposta como ideal, um imaginário representativo (fixação, identidade, forma). (CECCIM; PALOMBINI, 2009, p.302)

O rigor de tratamento evoluiu para práticas cruéis e abusos de toda ordem ao longo do século XVIII, o que criou uma cultura social de aceitação do menosprezo e da violência, tanto de quem praticava quanto de quem sofria, o que em diversos locais perdura até hoje.

Foi neste contexto que surgiram as primeiras ações de assistência à criança, as chamadas "Roda dos enjeitados", ligadas a instituições que recolhiam bebês rejeitados pelas mães, mantendo o anonimato. Perduraram ao longo de séculos - no Brasil até 1940 em Porto Alegre/RS.

Ao longo de toda a história a consolidação do poder, dos direitos e da proteção estiveram diretamente ligados à detenção de propriedade, ou seja, aquele homem que a detinha (pai de família), tornava-se senhor de todos os demais (mulher, filhos, escravos). A relação de poder incondicional em face das filhas era ainda mais marcante, já que reuniam três características justificadoras do dever de submissão e obediência: criança, mulher, filha.

A organização social fundava-se basicamente na obediência, o que afastava vínculos de afeto, situação que passou a mudar apenas na virada do século XVIII para o XIX justificada pela necessidade

de manter a disponibilidade de mão de obra durante a ascensão industrial. O resultado foi a produção de um discurso moralista direcionado à suposta proteção da maternidade, que elegeu a mãe como integralmente responsável pela higiene, saúde, beleza e vida do filho desde a gestação.

Aos poucos a criança passou a ser percebida como alguém que viria a ser o adulto do futuro e por isso merecia cuidados. Era o que garantiria a existência de cidadãos adequados para povoar um mundo capitalista em ascensão. O Estado decidiu regular o poder do pai limitando-o a mero tutor dos cidadãos do futuro: o pai provedor. A mãe, então, tornou-se a garantidora do desenvolvimento saudável das crianças até a idade escolar, quando seriam direcionadas aos colégios, preferencialmente internos, onde seu caráter seria moldado até que fossem capazes de se reinserir no seio familiar e integrar a sociedade como cidadãos.

Gradativamente, a infância adquiriu status de etapa especial da vida, momento determinante para a constituição psíquica do indivíduo. O foco passa para a garantia da alteridade por meio da educação do cuidado.

3. SISTEMA DA PROTEÇÃO INTEGRAL

Neste conceito moderno, nascem políticas e programas organizados e promovidos pelo Estado e pela sociedade com o objetivo de garantir a manutenção de condições adequadas ao desenvolvimento da cidadania dos menores, como sujeitos humanos de direitos. Partindo da ordem principiológica da Declaração Universal dos Direitos do Homem (1948) do Brasil desenvolveu internamente as previsões da Constituição Cidadã que adotou a lógica da proteção integral da criança e do adolescente, oposta à regra da situação irregular até então vigente, como dever da família, da sociedade e do Estado; a Lei de Diretrizes e Bases da Educação;

Convenção da ONU sobre os Direitos da Criança (1989); O Conselho da Criança e do Adolescente (1990); Plano Nacional da Educação; Estatuto da Criança e do Adolescente (1990), Convenção de Nova York sobre os Direitos da Criança (2000), Lei da Escuta Protegida (13.431/2017), etc.

A criança e o adolescente passaram a gozar de proteção, figurando como sujeitos de direito vulneráveis, focos da preocupação constante da sociedade principalmente a partir do séc. XX, alterando-se uma perspectiva de abusos generalizados que perdurou durante séculos.

> (...) de forma transversal em todas as classes sociais, não respeitando sexo, credo, idade e cor. Pais estupram e mantêm relações sexuais com suas filhas sem que a mulher/mãe reaja, pois seu parceiro se constitui chefe da casa. Filhos são espancados, torturados, tendo em vista a prática de uma educação autoritária/violenta que deverá desde cedo transmitir regras, valores e comportamentos de submissão aceitos em nossa sociedade. (Roure, 1996, p. 78)

A violência disseminada por todo o tecido social é considerada o desafio do século, representando altíssimo impacto na saúde com custo econômico e social imenso. Segundo a Associação brasileira de Saúde Coletiva - ABRASCO baseada em estudos do Ministério da Saúde, as maiores causas da morte de adolescentes são acidentes e violência (causas externas) (Flaeschen; REIS, 2019), sendo a de ordem sexual responsável pela maioria dos atendimentos nas unidades de saúde, seguida pela violência psicológica e depois a física, que ocorrem em mais de 50% dos casos, cometidos em especial por aqueles que têm o dever de guarda e proteção, justificadas pelo dever de educar o que fundamenta certa dose de aceitação social.

> Nessa perspectiva, essa síndrome do pequeno poder é reforçada por três fatores básicos: (a) perpetuação de uma cultura transgressora

> dos Direitos da Criança, (b) idealização da família patriarcal/autoritária (Gelles, 1979; Poster, 1979) e (c) cultura da violência, seja como recurso pedagógico, seja como arma para solução de conflitos (Mello, 1997). Tal síndrome é coerente com nossa argumentação sobre a estruturação hierárquica da sociedade, a partir da violência perpetrada pelos adultos, de modo que o discurso de defesa da criança e do adolescente aparece como dispositivo para "barrar" o gozo desse sujeito (adulto) que objetifica o outro (a criança). (TEIXEIRA FILHO et al., 2013, p. 92)

Mesmo com a evolução da legislação, inclusive a de ordem penal, a cultura da exploração e do abuso permanece. Infelizmente a criminalização de condutas consideradas extremamente danosas para o desenvolvimento da criança e do jovem, embora necessária, não é suficiente para modificar a concepção enraizada ao longo do tempo.

4. ASPECTOS DA VIOLÊNCIA VIRTUAL

A violência envolve conceitos complexos e hoje é tratada como um problema de saúde pública que implica custos humanos e econômicos às nações, devendo ser combatida em diversas frentes. Por sua definição é evidente que o meio virtual propicia a prática da violência. A Organização Mundial da Saúde define violência como:

> O uso intencional da força ou do poder, real ou em ameaça, contra si próprio, contra outra pessoa, ou contra um grupo ou uma comunidade, que resulte ou tenha possibilidade de resultar em lesão, morte, dano psicológico, deficiência de desenvolvimento ou privação. (KRUG et al, 2002, p. 5).

Ao quadro alarmante já relatado, soma-se o crescente acesso aos meios virtuais[1] que traz consigo uma infinidade de possibilidades

1 Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil - TIC Kids Online Brasil 2019 mostra que 83% das crianças e jovens brasileiros são

para a violação de crianças e adolescentes, embora tenha se tornado meio essencial para o desenvolvimento, inclusive escolar. Pesquisa organizada pela Secretaria Nacional dos Direitos da Criança e do Adolescente (SNDCA) em parceria com a entidade civil Viração Educomunicação em 2019 constatou que 66% das crianças entrevistadas iniciaram o uso da internet antes dos 12 anos e mentiram a idade para ter acessos a sites e aplicativos. Apenas metade possui supervisão de adultos. Ainda, 51% informaram que se sentem mais à vontade para se abrir com as pessoas no mundo virtual, o que os torna alvos fáceis para a ação de criminosos. (RELATÓRIO, 2019)

Neste ambiente os agentes, confiando no anonimato, se permitem a desconexão com as suas identidades pessoais e a liberação de instintos criminosos os quais, em muitos casos, permanecem controlados no mundo real, seja pelo temor das instituições de controle formal ou pelo dever ético e moral com a família, amigos, escola, religião, etc. Os resultados, principalmente psíquicos, são aterrorizantes.

Em 2020, o Ministério da Mulher, da Família e dos Direitos Humanos apurou que os 5 tipos de denúncias mais frequentes no Disque 100 estão relacionados à exposição de crianças e adolescentes na internet (MINISTÉRIO DA MULHER DA FAMÍLIA E DOS DIREITOS HUMANOS, 2020).

A situação pandêmica tornou os dados ainda mais preocupantes: a ONG Safernet Brasil[2] (DENÚNCIAS, 2021) divulgou que entre

usuários da internet. CGI.br/NIC.br. Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC, 2019).

2 A Safernet é uma organização não governamental que promove a defesa dos Direitos Humanos na Internet no Brasil. A Safernet mantém a Central Nacional de Denúncias de Crimes Cibernéticos operada em parceria com os Ministérios Públicos.

janeiro e abril de 2021 houve um crescimento de 33,45% nas denúncias em relação ao mesmo período de 2020, ano em que ocorreu o recorde histórico (desde 2006) de denúncias anônimas de pornografia infantil na internet. De acordo com os índices, somente no primeiro mês de distanciamento - março - os casos de pedofilia virtual subiram 190%. Ainda, segundo a entidade, o acesso de páginas de pornografia infantil subiu 69%.

Diversas são as condutas criminosas ("pedofilia", pornografia infantil, tráfico de pessoas, *cyber bullying*, *cyber grooming*, etc) praticadas através do mundo virtual contra estas vítimas, as quais, embora nativos digitais, evidenciam vulnerabilidade.

Atualmente existem tratativas específicas da legislação brasileira. Recentes alterações legislativas, principalmente de natureza penal como as Leis 13.772/2018, 13.718/2018 e 14.132/2021 no Código Penal e no ECA - Lei 11.829/2008, acrescentaram diversos tipos penais relacionados a condutas nos meios virtuais, não apenas contra crianças. Passaremos a tratar especificamente do *cyber grooming*.

5. CYBER GROOMING

Como vem se tornando natural em nosso ordenamento jurídico, *cyber grooming* é mais um termo importado incorporado à nossa cultura legislativa virtualizada.

O *grooming* "envolve um processo de socialização por meio do qual um ofensor busca interagir com a criança (...), possivelmente compartilhando de seus interesses numa tentativa de ganhar sua confiança e prepará-la para o abuso sexual". (LANDINI, 2018, p. 518 apud DAVIDSON, 2011, p. 5)

> Está intimamente ligado à conduta o *sextortion* e estupro virtual. É denominado *'sextorsion'*, um crime exclusivo da era digital. Predadores fingem ser jovens na rede social e sites de jogos. Eles fazem amizade com os jovens, ganham sua confiança e os induzem a enviar fotos obscenas de si mesmos. Então eles usam as fotos para extorquir mais e mais imagens ilícitas.[3] (BELLO, 2014, p. 225)

As crianças e adolescentes são hoje os alvos principais dos criminosos sexuais, em razão do uso intenso de redes sociais ou de aplicativos e jogos. A intenção é manipular o entendimento das vítimas, conquistando sua confiança e convencendo-as a se expor sexualmente para a prática de atos libidinosos através de pressão psicológica, constrangimento, promessas ou ameaça de fazer mal para familiares da vítima com a intenção de forçar um encontro e, a partir disso, consumar a prática de outras condutas como o estupro ou tráfico de pessoas.

É um meio amplamente utilizado com o intuito de conseguir material sexual, o que acaba sendo divulgado posteriormente, principalmente na *deep web.*

A conduta do aliciamento, podendo ser entendida também como assédio, caracterizando-se como um tipo de violência contra a criança na medida em que causa prejuízos sociais, psicológicos e espirituais, tomando diferentes proporções e encurtou o caminho até as vítimas pelo meio virtual. Nesse sentido, LANDINI (2018) explica que as:

> Três características das tecnologias da informação e da comunicação foram apresentadas como justicativa para o aumento perceptível dessa nova ameaça, as quais facilitariam ou acentuariam o problema

3 Do original:*"It's called 'Sextortion', a crime exclusive to the digital age. Predators pretend to be teens on social media and gaming sites. They befriend young people, gain their trust and entice them to send lewd photos of the mselves. Then they use the photos to extort more and more illicit images"*.

> da agressão sexual contra crianças: 1) o fato de a Internet poder ser utilizada como meio de contato por um número incalculável de pessoas, bem como uma plataforma para encontrar diferentes conteúdos e materiais; 2) a falta de fronteiras geográficas, o que dificulta o policiamento e permite maior acessibilidade; 3) a Internet poderia produzir um sentimento de anonimato entre os usuários, facilitando a execução de crimes nesse ambiente. (LANDINI, 2018, p. 523)

A criminalização desta conduta iniciou-se ao redor do mundo (Estados Unidos, Canadá, Austrália, Reino Unido e Irlanda, Noruega, Suécia e Holanda) a partir dos anos 2000 quando passou a ser considerada comportamento independente, digno de reprovação criminal. Anteriormente a conduta era compreendida como mero ato preparatório para a prática de outros crimes.

Em grande medida ocorreu em razão do surgimento, na época, do hoje chamado pânico sexual, conceito desenvolvido por Roger N. Lancaster *in Sex Panic and the Punitive State* (2011) em analogia com a Teoria do Pânico Moral de Stanley Cohen e Jock Young[4], para explicar a postura do Estado de penalizar cada vez mais condutas, de forma cada vez mais grave, como meio de conter a criminalidade. (LANDINI, 2018, p. 524 apud LANCASTER, 2011)

No Brasil, o aliciamento de crianças e adolescentes foi criminalizado pelo Estatuto da Criança e Adolescente a partir de 2008. O art. 241-D, *caput* estabelece:

---

4 De acordo com Stanley Cohen, autor de um estudo sociológico sobre a cultura e mídia juvenil chamado Folk Devils and Moral Panics ("demônios folclóricos e pânicos morais"), de 1972, um pânico moral ocorre quando existe uma série de episódios, em que uma pessoa (ou um grupo) acaba por simbolizar uma ameaça aos valores e interesses do grupo social majoritário. Aqueles que começam o pânico quando temem uma ameaça aos valores sociais ou culturais predominantes são conhecidos pelos pesquisadores como "empreendedores morais", enquanto as pessoas que supostamente ameaçam a ordem social têm sido descritas como "demônios folclóricos". (COHEN, 2011)

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Nas mesmas penas incorre quem: I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.(BRASIL, 2021)

A intenção primordial da Lei é a de reafirmar o pacto de cidadania, direitos humanos e proteção integral da criança e do adolescente. Neste sentido cabe rememorar que o dever de combate à injustiça social, econômica e jurídica não é apenas do Estado, mas também da família e sociedade.

O art. 241-D foi incluído no Estatuto da Criança e do Adolescente - ECA pela Lei 11.829/2008, a qual alterou o diploma legal criando os tipos penais previstos nos arts. 141-A até 141-E, agravando o tratamento e as penas dos crimes, intoleráveis, objetivando tutelar a integridade moral das vítimas. A principal intenção foi combater práticas de comércio sexual virtual, que também exige o treinamento especializado das polícias, do Ministério Público e do Judiciário.

De início cabe frisar que o texto exclui a figura do adolescente, o que nos parece um grande equívoco, já que é o grupo que mais se expõe nos meios virtuais, conforme indicado nas pesquisas mencionadas no início deste texto. Apesar disso, há quem defenda a ideia de que o adolescente possui maior discernimento.

De qualquer forma, tais atos praticados contra adolescentes podem atrair a aplicação do Código Penal, configurando inclusive o estupro virtual, conforme os mais recentes entendimentos dos Tribunais Superiores.

Com a intenção de atualizar o ECA e corrigir tal equívoco, atendendo a demandas de agentes público que trabalham na linha de frente do combate aos crimes de sexuais praticados contra crianças e adolescentes, está em trâmite na Câmara dos Deputados Projeto de Lei nº 1130/2020, apresentado em 30/03/2020, "Altera o art.241-D da Lei nº 8.069, de 13 de julho de 1990 — Estatuto da Criança e Adolescente, a fim de inserir o termo 'adolescente' no tipo penal e aumentar a pena para reclusão de 1 (um) a 5 (cinco) anos e multa." (BRASIL, 2021)

As condutas descritas no art. 241-D são as que visam a prática de ato libidinoso, sendo este o elemento subjetivo do tipo. As mesmas condutas dissociadas desta finalidade serão atípicas.

Aliciar traz a ideia de atrair a partir de histórias e promessas enganosas; assediar significa perseguir com propostas, importunar, sugerir com insistência; e instigar que significa estimular, fazer nascer a ideia da prática do ato libidinoso. Constranger, obrigar, forçar, coagir, por qualquer meio sem que haja necessariamente a violência ou grave ameaça.

Só admite a forma dolosa, sendo possível a tentativa. Classifica-se como crime de perigo, ou seja, não se exige a efetiva prática do ato libidinoso para a consumação. Pela análise de casos concretos julgados, percebe-se que na prática a notícia do crime ocorre quando já esgotados os atos previstos por este artigo e consumados outros crimes, como o próprio ato libidinoso; estupro; estupro de vulneráveis; a produção, armazenamento, disponibilização de material pornográfico; etc.

Portanto, que este tipo penal criminaliza os atos preparatórios que viabilizam atos libidinosos quaisquer, o que evidencia mais uma vez a intenção do legislador de tornar efetivas as políticas de proteção integral e irrestrita às crianças e adolescentes com foco

na prevenção das consequências danosas a que estão sujeitos.[5]

O bem jurídico tutelado pelo tipo penal do art. 241-D do ECA é, não só a integridade física infantojuvenil, mas também a formação moral e psíquica destes indivíduos ainda em desenvolvimento diante da propagação da cultura do abuso sexual no meio virtual. Diversas pesquisas apontam que a quase totalidade dos agressores sofreram violências enquanto crianças, o que garante que o ciclo de abuso-abusador se repete infinitamente e precisa urgentemente ser quebrado se quisermos garantir uma sociedade verdadeiramente equilibrada, formada por indivíduos saudável mentalmente focados na garantia e preservação da dignidade da pessoa humana.

6. LEGISLAÇÃO NO DIREITO COMPARADO

Em razão da situação especial da vítima deste crime e da abrangência mundial das condutas praticadas pelo meio virtual, percebe-se uma preocupação de quase todos os países do globo em criminalizar o *cyber grooming*, principalmente porque é o primeiro passo do criminoso que pretende consumar diversos outros crimes sexuais contra crianças e adolescentes (mas é claro que a prática pode ocorrer inclusive contra adultos).

O combate a todo tipo de violência contra a criança faz parte de protocolos internacionais com foco na promoção da cooperação internacional no combate à exploração sexual de crianças. Alguns

5 Investigando possíveis consequências psicológicas da vitimização, uma questão de múltipla escolha, que obteve 265 respostas, indicou que 65.3% disseram não ter notado nenhuma consequência (32.9% VDS e 46.9% VS), 6.8% apresentaram dificuldades para dormir (50.0% VDS e 33.3% VS), 9.8% baixa autoestima (34.6% VDS e 42.3% VS), 3.8% dificuldades para se alimentar (60.0% VS), 1.5% fugas de casa, 4.2% comportamentos agressivos e 1.9% revelaram não se lembrar se houve consequências psicológicas.(TEIXEIRA FILHO et al, 2013, p. 96)

exemplos serão citados a seguir.

A Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais - Convenção de Lanzarote de 2007 foi o primeiro documento internacional a prever como criminosa a conduta do aliciamento de crianças para fins sexuais no art. 23 (ABRANTES, 2016):

> Artigo 23.º – Abordagem de crianças para fins sexuais Cada Parte toma as necessárias medidas legislativas ou outras para qualificar como infracção penal o facto de um adulto propor de forma dolosa, através de tecnologias de informação e comunicação, um 18 encontro a uma criança que não tenha atingido a idade estabelecida em aplicação do n.º 2 do artigo 18.º, com a finalidade de cometer nesse encontro qualquer uma das infracções estabelecidas em conformidade com a alínea a) do n.º 1 do artigo 18.º ou com a alínea a) do n.º 1 do artigo 20.º, desde que essa proposta seja seguida de actos materiais que visem a tal encontro. (PORTUGAL, 2021)

Na mesma dimensão daquele documento internacional, inúmeros países deram visibilidade a situação.

Em Portugal, por exemplo, houve alteração legislativa em 2015 para incluir o art 176º A no Código Penal (PORTUGAL, 2021):

> Artigo 176º - A
> Aliciamento de menores para fins sexuais
> 1 - Quem, sendo maior, por meio de tecnologias de informação e de comunicação, aliciar menor, para encontro visando a prática de quaisquer dos atos compreendidos nos n.os 1 e 2 do artigo 171.º e nas alíneas a), b) e c) do n.º 1 do artigo anterior, é punido com pena de prisão até 1 ano. 2 - Se esse aliciamento for seguido de atos materiais conducentes ao encontro, o agente é punido com pena de prisão até 2 anos. Aditado pelo/a Artigo 3.º do/a Lei n.º 103/2015 - Diário da República n.º 164/2015, Série I de 2015-08-24, em vigor a partir de 2015-09-23

Já no Canadá houve, em 2002, aprovação pelo Parlamento do art 172.1 do Código Criminal (CANADA, 2021) que prevê:

> 172.1 (1) Comete ofensa toda pessoa que, por qualquer meio de telecomunicação, comunica-se com
> (a) uma pessoa que seja, ou que o acusado acredite ser, menor de 18 anos, com o objetivo de facilitar a comissão de uma ofensa sob a subseção 153(1)
> [exploração sexual], seção 155 [incesto], 163.1 [pornografia infantil], 170 [pais ou responsáveis que procuram atividade sexual] ou 171 [permitir atividade sexual em sua propriedade] ou subseção 212(1), (2), (2.1) ou (4) [proxe-netismo e prostituição] com respeito àquela pessoa;
> (b) uma pessoa que seja, ou que o acusado acredite ser, menor de 16 anos, com o objetivo de facilitar a comissão de uma ofensa sob a seção 151 [interferência sexual] ou 152 [convite ao toque sexual], subseção 160(3) [bestialidade na presença de uma criança] ou 173(2) [exposição] ou seção 271 [agressão sexual], 272 [agressão sexual com arma], 273 [agressão sexual agravada] ou 280 [sequestro de pessoa menor de 16 anos] com respeito àquela pessoa; ou
> (c) uma pessoa que seja, ou que o acusado acredite ser, menor de 14 anos, com o objetivo de facilitar a comissão de uma ofensa sob a seção 281 [sequestro de uma pessoa menor de 14 anos] com respeito àquela pessoa.[6](LANDINI, 2018, p. 519)

6 Do original: *"Agreement or arrangement — sexual offence against child 172.2 (1) Every person commits an offence who, by a means of telecommunication, agrees with a person, or makes an arrangement with a person, to commit an offence (a) under subsection 153(1), section 155, 163.1, 170, 171 or 279.011 or subsection 279.02(2), 279.03(2), 286.1(2), 286.2(2) or 286.3(2) with respect to another person who is, or who the accused believes is, under the age of 18 years; (b) under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to another person who is, or who the accused believes is, under the age of 16 years; or (c) under section 281 with respect to another person who is, or who the accused believes is, under the age of 14 years. Marginal note: Punishment (2) Every person who commits an offence under subsection (1) (a) is guilty of an indictable offence and is liable to imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year; or (b) is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than two years less a day and to a minimum punishment of imprisonment for a term of six*

Na Alemanha, algumas alterações legislativas ocorreram mais recentemente. Hoje, de acordo com o § 176 do *Strafgesetzbuch* (Código Penal) (ALEMANHA, 2021) , é crime aliciar uma criança (até 14 anos) com a finalidade sexual ou utilizar qualquer meio de telecomunicação para tentar induzi-la à prática de atos sexuais ou pornografia infantil.

> Código Criminal (StGB)
> Seção 176 Abuso Sexual de Crianças
> (1) Uma pena de prisão não inferior a um ano é punida para qualquer pessoa que 1. se envolver em atos sexuais com uma pessoa menor de quatorze anos (criança) ou permitir que a criança fazê-lo, 2. uma criança destinada a praticar atos sexuais contra uma terceira pessoa ou a fazê-los por uma terceira pessoa, 3. oferece ou promete provar uma criança por um ato nos termos do número 1 ou número 2.
> (2) Nos casos do parágrafo 1 número 1, o tribunal pode renunciar à punição ao abrigo desta disposição se o ato sexual entre o perpetrador e a criança for amigável e a diferença de idade, nível de desenvolvimento ou grau de maturidade for pequena, a menos que o agressor tira vantagem da incapacidade da criança de autodeterminação sexual.7 (tradução livre).

---

months. Marginal note: Presumption (3) Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of 18, 16 or 14 years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. Marginal note: No defence (4) It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least 18, 16 or 14 years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person. Marginal note: No defence (5) It is not a defence to a charge under paragraph (1)(a), (b) or (c) (a) that the person with whom the accused agreed or made an arrangement was a peace officer or a person acting under the direction of a peace officer; or (b) that, if the person with whom the accused agreed or made an arrangement was a peace officer or a person acting under the direction of a peace officer, the person referred to in paragraph (1)(a), (b) or (c) did not exist.2012, c. 1, s. 23. 2014, c. 25, s. 10. 2015, c. 23, s. 12"

7 Do original: "*Strafgesetzbuch (StGB) § 176 Sexueller Missbrauch von Kindern (1) Mit Freiheitsstrafe nicht unter einem Jahr wird bestraft, wer 1. sexuelle Han-*

Em janeiro de 2020, a lei alemã foi estendida para incluir casos de tentativa de preparação cibernética as quais eram descobertas por investigadores ou pais infiltrados enquanto o criminoso acreditava tratar-se de uma criança. (HALLAM, 2020)

Já nos Estados Unidos, o 18 U.S.C.§ 2422 (CORNEL, 2021) tornou um crime federal utilizar correio, ou qualquer outra facilidade de comércio interestadual ou internacional, ou persuadir conscientemente, induzir, incitar ou coagir menores de 18 anos a prostituição ou outra atividade sexual aplicando a pena de no mínimo 10 anos ou prisão perpétua.

As leis de combate ao *grooming* foram aplicadas pela primeira vez em 2009 com pena aplicada de 20 anos, acrescida de mais 20 pela distribuição e posse de material pornográfico infantil. (GROOS, 2009)

> 18 U.S. Code § 2422 Coerção e sedução (a) Quem quer que conscientemente persuadir, induzir, seduzir ou coagir qualquer indivíduo a viajar em comércio interestadual ou estrangeiro, ou em qualquer Território ou Posse dos Estados Unidos, a se envolver em prostituição ou em qualquer atividade sexual pela qual qualquer pessoa possa ser acusada de um ofensa criminal , ou tentativas de fazê-lo, serão multados sob este título ou prisão não mais de 20 anos, ou ambos. (b) Quem quer que, usando o correio ou qualquer facilidade ou meio de comércio interestadual ou estrangeiro, ou dentro da jurisdição marítima e

---

dlungen an einer Person unter vierzehn Jahren (Kind) vornimmt oder an sich von dem Kind vornehmen lässt, 2. ein Kind dazu bestimmt, dass es sexuelle Handlungen an einer dritten Person vornimmt oder von einer dritten Person an sich vornehmen lässt, 3. ein Kind für eine Tat nach Nummer 1 oder Nummer 2 anbietet oder nachzuweisen verspricht. (2) In den Fällen des Absatzes 1 Nummer 1 kann das Gericht von Strafe nach dieser Vorschrift absehen, wenn zwischen Täter und Kind die sexuelle Handlung einvernehmlich erfolgt und der Unterschied sowohl im Alter als auch im Entwicklungsstand oder Reifegrad gering ist, es sei denn, der Täter nutzt die fehlende Fähigkeit des Kindes zur sexuellen Selbstbestimmung aus.”

> territorial especial dos Estados Unidos, conscientemente persuadir, induzir, incitar ou coagir qualquer indivíduo que não tenha atingido a idade de 18 anos, a se envolver em prostituição ou qualquer atividade sexual pela qual qualquer pessoa possa ser acusada de um crime , ou tentar fazê-lo, será multada sob este título e condenada a pelo menos 10 anos de prisão perpétua.[8] (tradução livre)

Na Holanda, em 1 de janeiro de 2010, a seção 248e foi adicionada ao Código Penal holandês (HOLANDA, 2021), tornando um crime organizar online ou por telefone uma reunião com alguém que ele conhece ou que razoavelmente deveria assumir ser uma criança menor de 16 anos, com a intenção de abusar sexualmente da criança, assim que qualquer preparação para esta reunião seja feita. A pena máxima é de 2 anos de reclusão ou multa de quarta categoria.

> Artigo 248e Uma pessoa que, por meio de trabalho automatizado ou usando um serviço de comunicação, propõe um encontro com uma pessoa que conhece ou deveria razoavelmente suspeitar que ainda não completou dezesseis anos com a intenção de cometer atos obscenos com essa pessoa ou para fazer a imagem de um comportamento sexual em que essa pessoa esteja envolvida, se ele praticar qualquer ato com o objetivo de conseguir esse encontro, é punido com uma pena de prisão não superior a dois anos ou com multa de

8 Do original: *"18 U.S. Code § 2422 - Coercion and enticement. (a)Whoever knowingly persuades, induces, entices, or coerces any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both. (b)Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life."*

quarta categoria.[9] (tradução livre)

No México, em abril de 2021, as comissões legislativas federais do México aprovaram a proposta de alteração do Código Penal para incluir a conduta do *cyber grooming* no texto legal. Define penas de 4 a 8 anos de prisão podendo chegar até 16 anos quando praticada por adultos se fazendo passar por crianças. (HIDALGO, 2021)

> Artigo 211.º Quater.- Quem coagir, intimidar, molestar, exigir ou enganar outra pessoa, para a preparação ou remissão de imagens ou gravações de voz ou conteúdos audiovisuais de natureza erótica, sexual ou pornográfica, sob pena de revelação, publicação, divulgação ou exibição sem o seu consentimento o material da mesma natureza que a vítima tenha anteriormente partilhado directamente ou que tenha obtido por qualquer outro meio, ou, para marcação de encontro ou abordagem física, será aplicada de três a sete anos de reclusão e um multa de duzentas a quatrocentas unidades de medida e atualização. Da mesma forma, quem, por meio de ameaças e engano, fingir ou conseguir marcar encontro físico ou abordagem com pessoa para obter concessões de natureza sexual ou material audiovisual com conteúdo explícito, será punido com pena de quatro a oito anos de prisão e multa de duzentas a quatrocentas unidades de medição e atualização. A pena será aumentada para o dobro, quando a vítima for menor ou declarada incapaz; Da mesma forma, ao obter imagens ou gravações de voz ou conteúdo audiovisual de natureza erótica, sexual ou pornográfica, a vítima se encontra em estado de embriaguez ou sob a influência de drogas, enervantes e outros análogos que produzem efeitos semelhantes e que o fazem perder o controle de sua pessoa.[10]

---

9 Do original: *"Artikel 248e Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst een persoon van wie hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van zestien jaren nog niet heeft bereikt, een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met die persoon te plegen of een afbeelding van een seksuele gedraging waarbij die persoon is betrokken, te vervaardigen wordt, indien hij enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie."*

10 Do original: *"Artículo 211 Quater.- A quien coaccione, intimide, hostigue,*

(MÉXICO, 2021)

Já na Argentina a previsão do cyber grooming ocorreu em 2013, conforme texto do art. 131 do Código Penal da Argentina, tendo sido motivo de fortes críticas pelos estudiosos da matéria sob a alegação de que não protege com efetividade o bem jurídico a que se propõe tutelar. (SCHNIDRING, 2016)

> ARTIGO 131. - Todo aquele que, por meio de comunicações eletrônicas, telecomunicações ou qualquer outra tecnologia de transmissão de dados, contate menor, com a finalidade de cometer crime contra a integridade sexual do mesmo. (Artigo incorporado pelo art. 1º da Lei nº 26.904 B.O. 11/12/2013)[11](tradução livre) (ARGENTINA, 2021)

---

exija o engañe a otra persona, para la elaboración o remisión de imágenes o grabaciones de voz o contenidos audiovisuales de naturaleza erótico, sexual o pornográfico bajo la amenaza de revelar, publicar, difundir o exhibir sin su consentimiento el material de la misma naturaleza que previamente la víctima le haya compartido directamente o que haya obtenido por cualquier otro medio, o bien, con la finalidad de concertar un encuentro o acercamiento físico, se le impondrá de tres a siete años de prisión y multa de doscientas a cuatrocientas unidades de medida y actualización. Asimismo, a quien mediante amenazas y engaños pretenda o logre concertar un encuentro o acercamiento físico con una persona para obtener concesiones de índole sexual o material audiovisual con contenido explícito, se le impondrá de cuatro a ocho años de prisión y multa de doscientas a cuatrocientas unidades de medida y actualización. La pena se aumentará hasta el doble, cuando la víctima sea menor de edad o sea declarada incapaz; así también, cuando para la obtención de imágenes o grabaciones de voz o contenidos audiovisuales de naturaleza erótico, sexual o pornográfico, la víctima se encuentre en estado de ebriedad o bajo el influjo de drogas, enervantes y otras análogas que produzcan efectos similares y que les hagan perder el control de su persona"

11 Do original: "ARTICULO 131. - *Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. (Artículo incorporado por art. 1° de la Ley N° 26.904 B.O. 11/12/2013)."*

Em grande parte dos países do mundo, ao menos os de cultura ocidental, há criminalização do *cyber grooming* como objetivo de tutelar a integridade do sujeito ainda em formação, seguindo orientações das instituições internacionais de defesa de direitos humanos.

Ainda, é importante avaliar se o fato de haver legislação sobre o tema traz alguma diferença ao fenômeno, conforme se verá no próximo tópico.

7. FUNCIONALIDADE DA LEI

Assim como ocorre com todos os crimes praticados através do meio virtual, sem contato físico com a vítima, a investigação e produção probatória acabam encontrando barreiras. No caso da conduta de aliciamento/assédio de crianças é ainda mais difícil realizar a prova dos fatos.

Em primeiro lugar porque se trata de crime que viola a liberdade sexual, e delitos desta espécie, na regra constatada por diversas estatísticas criminais, têm altíssimos níveis de subnotificação. Em segundo, porque é praticado no ambiente virtual, envolvendo apenas o agente e a vítima através de acessos com utilização de senhas, que muitas vezes são desconhecidas pelos próprios pais/responsáveis.

Ainda, podemos acrescentar o fato de que muitas vezes quando a conduta criminosa é constatada pelos pais/responsáveis da criança, estes são tomados por tamanho horror e aversão, somados a sentimentos de culpa e medo, que acabam simplesmente bloqueando os usuários, contatos, deletando o conteúdo, o que destrói a prova, inviabilizando, muitas vezes, a investigação.

Em casos como estes é imprescindível que se mantenham intactos todos os registros das conversas trocadas entre autor e a criança, inclusive com as imagens e vídeos, pois é através da análise destes conteúdos que a conduta criminosa será adequada ao tipo penal, principalmente quanto à caracterização do dolo e presença indubitável do elemento subjetivo do tipo (finalidade de praticar ato libidinoso).

Nos casos em que há condenação, pela natureza do crime, o depoimento das vítimas possui valor especial, mas é a partir da análise conjunta deste com o histórico dos acessos e do conteúdo compartilhado que se classifica a conduta no artigo de Lei.

Em praticamente todos os casos julgados as provas demonstram a prática de vários outros delitos em concurso material (assédio, estupro de vulnerável, estupro virtual, armazenar e divulgar conteúdo com cena de sexo ou pornagrafia envolvendo criança ou adolescente, etc.).

As teses mais comuns da defesa são a de alegar erro de tipo por desconhecer a tenra idade da vítima; ausência do elemento subjetivo do tipo e pleitear o reconhecimento da continuidade delitiva, além da aplicação do princípio da consunção (absorção do crime de assédio pelo estupro de vulnerável uma vez que aquele é meio para a prática deste).

8. CONCLUSÃO

Em uma sociedade em que os infantes se entregam à exploração sexual com o incentivo dos genitores, para garantir o sustento de famílias marginalizadas pela extrema pobreza, quando não são estes os agressores, seria de ingenuidade ímpar acreditar que a solução está na criação de tipos penais e agravamento de penas, ainda que se adequem às novas realidades do mundo tecnológico.

A miséria e a fome causam violência social, mas o constante estado de inconsciência, alienação e irresponsabilidade resulta permanente insatisfação exteriorizada em condutas pervertidas e violentas.

O meio virtual, realidade cada vez mais presente na vida de crianças e jovens, apesar de nos mostrar inúmeros benefícios, acabou fazendo o par ideal com esta normalização odiosa, já que facilita a caça pela vítima ideal. Isso se deve também pela falsa sensação de segurança da vítima que está em sua casa, longe dos estranhos que aprendemos a evitar.

A criminalização pode ser um caminho para reduzir a prática de condutas odiosas que ferem as vítimas muito além do corpo, fabricando sequelas permanentes e, por vezes, reproduzindo a violência. O ciclo precisa ser quebrado através do esclarecimento, da educação, da disponibilização de espaços de convivência e troca de experiências confiáveis, em conjunto com a evolução da legislação penal e modos de aplicação da lei.

Pela natureza da conduta tratada e meio empregado, a porcentagem de ações relatadas aos órgãos de controle e proteção são mínimas. Menor ainda é o número de casos em que se chega aos autores e em que eles são verdadeiramente punidos. O enrijecimento da legislação precisa ser acompanhado por ações nas

áreas social, educacional e de saúde (divulgação - elucidação - suporte) para que a proteção integral seja efetiva, já que o abuso sexual contra crianças e adolescentes ainda é normalizado em certos grupos.

Como todas as questões do Direito, o problema é antes social do que jurídico. A criminalização do aliciamento sexual de menores como forma de violência psíquica e espiritual altamente condenável, vem com a intenção de barrar o fato social, de mudar paradigmas construídos ao longo dos séculos.

O objetivo primordial é identificar condutas de risco - como o *cyber grooming* - que por si já caracterizam a violação da personalidade dos indivíduos em formação, evitando a consumação dos atos mais graves. Aqui as investigação e monitoramentos dos órgãos de controle formal, assim como o acompanhamento e supervisão constante da família, em conjunto com orientações nas escolas, são essenciais.

A proteção integral da criança somente será efetiva quando houver o exercício pleno da cidadania por todas as pessoas, que devem conhecer seus direitos através da educação e cultura e serem capazes de garantir o exercício pleno do direito do outro em um processo de re- ou nascimento do ser humano como ser social.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRANTES, Alexandra Catarina Silva. **O Problema do Aliciamento de Menores através da internet para fins sexuais**. 2016. 42f. Dissertação (Mestrado em Direito). Faculdade de Direito da Universidade Católica Portuguesa - Escola do Porto. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/21940/1/Alexandra%20Catarina%20Silva%20Abrantes.pdf. Acesso em: 19 ago. 2021.

ALEMANHA. ***Bundesministerium der Justiz und fur Verbraucherschutz***. Bundesamt fur Justiz. Disponível em: <https://www.gesetze-im-internet.de/stgb/__176.html>. Acesso em: 17 ago. 2021.

ARGENTINA. **Código Penal Argentino**. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#17>. Acesso em: 18 ago. 2021.

AZAMBUJA, Maria Regina Fay de. **O Olhar da Justiça nos casos de Violência Sexual praticada contra Criança**. In: 4 º Simpósio Mineiro de Assistentes Sociais, 2016, Belo Horizonte. Anais do 4 º Simpósio Mineiro de Assistentes Sociais. Disponível em: https://www.cress-mg.org.br/Upload/Pics/fe/fe799774-d341-4b3d-8773-3f5b3425b2ba.pdf. Acesso em: 14 ago. 2021.

BARBOSA, Cristiana; MANITA, Celina. **O aliciamento sexual de menores na internet: contributos para o seu conhecimento e prevenção**. *International Journal of Developmental and Educational Psychology INFAD* Revista de Psicología, Portugal, nº2, p. 197-202, 2019. ISSN: 0214-9877.Disponível em: https://revista.infad.eu/index.php/IJODAEP/issue/view/40. Acesso em: 13 ago. 2021.

BELLO, Marisol. ***'Sextortion' is an online 'epidemic' against children***. USA Today. 02 jul. 2014. Disponível em: https://www.usatoday.com/story/news/nation/2014/07/01/sextortionteens-online/11580633/. Acesso em: 17 ago. 2021.

BRASIL. **Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal**. Brasília, DF, 7 de dezembro de 1940 Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 ago. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 ago. 2021.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990. Institui Estatuto da Criança e do Adolescente**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 1a ago. 2021.

BRASIL. **Relatório descritivo e analítico com os resultados da pesquisa**. Dezembro de 2019. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/agosto/201912_RelatorioPesquisaEAtividadesConsultaBrasilViracaoRedeCS.pdf>. Acesso em: 15 ago. 2021.

BRASIL. **Projeto de Lei nº 1130/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242199. Acesso em: 17 ago. 2021.

CANADÁ. ***Criminal Code*** (R.S.C., 1985, c. C-46). Disponível em: https://laws-lois.justice.gc.ca/eng/acts/c-46/fulltext.html. Acesso em: 17 ago. 2021.

CASTIGLIONE, Yuri Giuseppe. **Pedofilia, exploração sexual infanto-juvenil e as recentes alterações do estatuto da crinça e do adolescente à luz da realidade social brasileira**. ECA comentado: ARTIGO 241A/241E – TEMA: Dos Crimes. Fundação Telefonica Vivo. 02 dez. 2016. Disponível em: https://fundacaotelefonicavivo.org.br/noticias/eca-comentado-artigo241a241e-tema-dos-crimes/. Acesso em: 17 ago. 2021.

CECCIM, Ricardo Burg; PALOMBINI, Analice de Lima. **Imagens da infância, devir-criança e uma formulação à educação do cuidado**. Psicologia & Sociedade; 21 (3): 301-312, 2009. Disponível em: https://www.scielo.br/j/psoc/a/C7q7MLNhgBcgrGxkzgJRWJx/?lang=pt&format=pdf. Acesso em: 19 ago. 2021.

CETIC. **TIC Kids Online Brasil - 2019 Crianças e adolescentes**. CETIC. Disponível em: https://cetic.br/pt/pesquisa/kids-online/indicadores/ Acesso em: 15 ago. 2021.

COHEN, Stanley. ***Folk Devils and Moral Panics: The Creation of the Mods and Rockers***. 1ª ed. Londres: Routledge, 2011

CONSULTA BRASIL. **Relatório descritivo e analítico com os resultados da pesquisa**. Dezembro de 2019. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/agosto/201912_Relatorio_PesquisaEAtividadesConsultaBrasilViracaoRedeCS.pdf. Acesso em: 16 ago. 2021.

DE ARAÚJO. Gabriela Moraes Lopes. **Estupro Virtual: a lesão da liberdade sexual no ciberespaço**. 2019. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/1336/1/Monografia%20-%20Gabriela%20Lopes.pdf. Acesso em: 16 ago. 2021.

DENÚNCIAS de pornografia infantil cresceram 33,45% em 2021, aponta a Safernet Brasil. Safernet. 2021. Disponível em: https://new.safernet.org.br/content/denuncias-de-pornografia-infantil--cresceram-3345-em-2021-aponta-safernet-brasil. Acesso em: 16 ago. 2021.

DICIONÁRIO Cambridge Inglês- Português. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/grooming. Acesso em: 14 ago. 2021.

DIGIÁCOMO, Murilo José. **Estatuto da criança e do adolescente anotado e interpretado**. Ministério Público do Estado do Paraná. Centro de Apoio Operacional das Promotorias da Criança e do Adolescente. [2020?]. 7ª ed.,Curitiba, 2017.

EDWARDS, Susan. ***Cyber-Grooming Young Women for Terrorist Activity: Dominant and Subjugated Explanatory Narratives***. *Viano E. (eds) Cybercrime, Organized Crime, and Societal Responses, International Approaches.* Switzerland,pp 23-46, 2017. Disponível em: https://www.researchgate.net/publication/311584397_Cyber--Grooming_Young_Women_for_Terrorist_Activity_Dominant_and_Subjugated_Explanatory_Narratives. Acesso em: 19 ago. 2021.

CORNEL Law School. ***Legal Information Institute***. US Code. Disponível em: https://www.law.cornell.edu/uscode/text/18/2422. Acesso em: 18 ago. 2021.

EXPOSIÇÃO de crianças e adolescentes na internet ocupa 5ª posição no ranking do Disque 100. Gov.br. 11 nov. 2020. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet--ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100. Acesso em: 15 ago. 2021.

FERREIRA, Luiz Antonio Miguel; DÓI, Cristina Teranise. **A Proteção Integral das Crianças e dos Adolescentes Vítimas (Comentários ao art. 143 do ECA)**. [2020?]. Disponível em: https://crianca.mppr.mp.br/pagina-1222.html. Acesso em: 15 ago. 2021.

FLAESCHEN, Hara; REIS, Vilma. **Sobre a violência contra crianças, adolescentes e jovens brasileiros**. Abrasco. 27 mar. 2019. Disponível em: https://www.abrasco.org.br/site/noticias/posicionamentos-oficiais-abrasco/sobre-a-violencia-contra-criancas-adolescentes-e-jovens-brasileiros/40061/. Acesso em: 15 ago. 2021.

GROOS, Caleb. ***"First 'Grooming' Child Porn Sentence: 40 Years – Sentencing – FindLaw Blotter***". Findlaw.16 jul. 2009. Disponível em: <https://blogs.findlaw.com/blotter/2009/07/first-grooming-child-porn-sentence-40-years.html>. Acesso em: 17 ago. 2021

HALLAM, Oliver Pieper Mark. ***Online child abuse investigators to get more powers***. DW. Germany, 17 jan. 2020. Disponível em: https://www.dw.com/en/germany-online-child-abuse-investigators-to-get-more-powers/a-52037583. Acesso em: 17 ago. 2021.

HOLANDA. **Código Penal Holandês**. Disponível em: https://wetten.overheid.nl/BWBR0001854/2013-09-01/#BoekTweede_TiteldeelXIV_Artikel248e. Acesso em: 18 ago. 2021.

HIDALGO, Claudia. ***Piden tipificar el "grooming" en el Código Penal del Estado de México***. Milenio. 13 mar. 2021. Toluca - México. Disponível em: <https://www.milenio.com/politica/que-es-el-grooming-diputados-piden-tipificarlo-en-edomex>. Acesso em: 18 ago. 2021.

KRUG, Etiene. G. et al. Lozano R. ***World report on violence and health***. Portal de Boas Práticas da Fiocruz, 2002. Disponível em: https://portaldeboaspraticas.iff.fiocruz.br/wp-content/uploads/2019/04/14142032-relatorio-mundial-sobre-violencia-e-saude.pdf. Acesso em: 19/08/2021.

LANDINI, Tatiana. **Vulnerabilidade e perigo potencial o processo de criminalização do assédio sexual online no Canadá e casos julgados em Ontário (2002-1014)**. Contemporânea - revista de sociologia da UFSCar. vol. 8. p. 515 - 542, 2018. Disponível em: https://www.researchgate.net/publication/330208048_Vulnerabilidade_e_perigo_potencial_o_processo_de_criminalizacao_do_assedio_sexual_online_no_Canada_e_casos_julgados_em_Ontario_2002-1014. Acesso em: 15 ago. 2021

MEIRELES, Luciano Miranda. **Revista Parquet em foco/Escola Superior do Ministério Público de Goiás**. Goiânia: ESMP-GO. v.1.n.1,set/dez, 2017. Disponível em: https://www.mpgo.mp.br/portal/arquivos/2018/02/22/16_59_09_358_Parquet_em_Foco_final.pdf. Acesso em: 12 ago. 2021.

MÉXICO. **Código Penal do Estado do México**. Disponível em: <http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf>. Acesso em: 18 ago. 2021.

MINISTÉRIO DA MULHER DA FAMÍLIA E DOS DIREITOS HUMANOS. **Canais registram mais de 105 mil denúncias de violência contra mulher em 2020**. 2020. PODER 360. Disponível em: https://static.poder360.com.br/2021/03/denuncias-disque100-ligue180-metodologia-7mar2021.pdf. Acesso em: 25 nov. 2021.

MINISTÉRIO DA SAÚDE . **Impacto na violência na saúde de crianças e adolescentes. Prevenção de violências e promoção da cultura de paz**. BVSMS. 2010. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/impacto_violencia_saude_criancas.pdf. Acesso em 15 ago. 2021.

PORTUGAL. **Convenção do Conselho da Europa para a Protecção das Crianças contra a Exploração Sexual e os Abusos Sexuais**. Série de Tratados do Conselho da Europa – N.º 201. Disponível em: https://rm.coe.int/168046e1d8. Acesso em: 19 ago. 2021.

PORTUGAL. Código penal português. **Diário da República n.º 63/1995, Série I-A de 1995-03-15**. Diário da República Eletrônico. Disponível em: <https://dre.pt/web/guest/legislacao-consolidada/-/lc/107981223/201708230200/73474088/diploma/indice>. Acesso em: 17 ago. 2021.

RELATÓRIO descritivo e analítico com os resultados da pesquisa. Governo do Brasil. Dezembro de 2019. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/agosto/201912_Relatorio_PesquisaEAtividadesConsultaBrasilViracaoRedeCS.pdf. Acesso em: 16/08/2021.

ROURE. Glacy. Q. de . **Vidas silenciadas: a violência com crianças e adolescentes na sociedade brasileira**. Campinas, SP: Editora da UNICAM. 1996.

SCHNIDRIG. Daniela. ***El delito de 'grooming' en la legislación penal actual y proyectada en argentina***. Palermo. Março de 2016. Disponível em: https://www.palermo.edu/cele/pdf/investigaciones/Informe-Anteproyecto-Codigo-Penal.pdf. Acesso em: 18 ago. 2021.

TEIXEIRA-FILHO, Fernando Silva et al. **Tipos e consequências da violência sexual sofrida por estudantes do interior paulista na infância e/ou adolescência**. Psicologia & Sociedade; 25(1): 90-102, 2013. Disponível em: https://www.scielo.br/j/psoc/a/KFZQzdpy5Y48BrRfjNj3BCP/?lang=pt. Acesso em: 19 ago. 2021.

NIKOLOVSKA, Manja. ***The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children***. Jan. 2020. Disponível em: <https://www.researchgate.net/publication/341911728_The_Internet_as_a_creator_of_a_criminal_mind_and_child_vulnerabilities_in_the_cyber_grooming_of_children>. Acesso em: 16 ago. 2021.

OS CRIMES VIRTUAIS CONTRA A MULHER E A (IN)SUFICIÊNCIA DA ATUAL LEGISLAÇÃO BRASILEIRA

VIRTUAL CRIMES AGAINST WOMEN AND THE CURRENT (IN)ADEQUACY OF THE BRAZILIAN LEGISLATION

Katiely Lemes Ribeiro
Advogada. Pós-graduanda em Direito Penal e Processual Penal pela Academia Brasileira de Direito Constitucional – ABDConst. Graduada em Direito pelo Centro Universitário Opet – UniOpet. Membra Participante da Comissão de Inovação e Gestão da OAB Paraná.
katielylemesribeiro@gmail.com.

RESUMO:
A desigualdade de gênero, muito embora permeie a sociedade há muito tempo, ainda é, infelizmente, grande problema sociocultural no Brasil, eis que não é algo natural, mas, sim, uma cultura enraizada em nosso meio social, principalmente pela continuidade, velada, do modelo patriarcal, que até o ano de 2002 (sim, século XXI) era, inclusive, positivado em nosso Código Civil. Nesse viés, apresenta-se o presente artigo, com o intuito de demonstrar que a sociedade evoluiu muito, principalmente no que tange aos avanços tecnológicos, mas, que, em paralelo, o fácil acesso à internet e o imensurável poder de disseminação rápida de informações (positivas e negativas) fez com que a violência contra a mulher também passasse a ter novas formas. Atualmente, algumas condutas virtuais perpetuam a violência contra a mulher e ante a necessidade da proteção de alguns bens jurídicas, foram tipificadas criminalmente. Assim, após a breve contextualização envolvendo a violência de gênero, analisou-se alguns dos crimes

virtuais praticados contra as mulheres, dentre eles, a *revenge porn*, o *stalking*, a sextorsão e o estupro virtual. Por fim, abordou-se um panorama com a evolução do nosso arcabouço legislativo sobre a temática e a sua (in)suficiência frente ao combate da violência contra a mulher.

Palavras-chave: Crimes Virtuais.Violência de Gênero.*Stalking. revenge porn*.Lei Maria da Penha.

ABSTRACT:
Gender inequality, although it has permeated society for a long time, is unfortunately still a major sociocultural problem in Brazil, as it is not something natural, but rather a culture rooted in our social environment, mainly due to its continuity, veiled, of the patriarchal model, which until the year 2002 (yes, 21st century) was even positive in our Civil Code. In this bias, we present this article in order to demonstrate that society has evolved a lot, especially with regard to technological advances, but that, in parallel, the easy access to the internet and its immeasurable power of rapid dissemination of information (positive and negative) made violence against women also "innovated", what we call virtual crimes, are nothing more than violence against women practiced through virtual means. Thus, after the brief contextualization of gender violence, we bring some of the virtual crimes committed against women, including revenge porn, stalking, sextorsion and virtual rape. Finally, we bring an overview of the evolution of our legislative framework on the subject and its (in)sufficiency in the

fight against violence against women.

Keywords: *Cyber Crimes.Gender Violence.Persecution. Revenge Pornography. Maria da Penha Law.*

Summary: *1. Introduction; 2. Contemporary Violence Against Women; 3. Virtual Crimes Usually Committed Against Women; 3.1. Stalking; 3.2. Revenge Porn; 3.3. Sextortion; 3.4. Virtual Rape; 4. The Evolution of Brazilian Legislation and Its (In)Sufficiency in Relation To Virtual Crimes Committed Against Women; 5. Final Remarks; 6. References.*

1. INTRODUÇÃO

É difícil imaginarmos como vivia a sociedade antes da chamada "era digital", eis que na atualidade, tudo gira em torno dos avanços tecnológicos e, principalmente, do universo da internet. Seja qual for a nossa nacionalidade ou profissão, é quase que improvável que não estejamos, de alguma forma, inseridos no meio virtual.

A facilidade oferecida seja pelo amplo acesso ou mesmo pela rapidez em disseminar qualquer conteúdo, fez com que o mundo virtual se tornasse cada vez mais presente nas relações humanas. Ocorre que ao mesmo tempo que houveram inúmeras vantagens, a tecnologia também trouxe muitos pontos negativos, sendo que um deles é a possibilidade de se praticar crimes por meio virtual.

Ao enxergarmos o passado, podemos perceber que muito antes da existência da rede mundial de computadores, a violência de gênero já existia, isso porque, a sociedade há muito, impôs – e ainda impõe – um papel de submissão e fragilidade para o sexo feminino, o que explica, mas não justifica, a violência praticada contra a mulher até hoje.

Mesmo com esses avanços, há desigualdades que continuam a se perpetuar: as mulheres conquistaram o direito ao voto graças ao movimento das sufragistas, no século XIX, mas ainda são pouco representadas nos espaços de poder político, seja no executivo, legislativo ou judiciário. Outro exemplo: elas têm garantido seu ingresso no sistema educacional, mas vivem em situação de desigualdade no trabalho, pois recebem salários mais baixos e enfrentam dificuldades maiores para galgar os postos de chefia. Por conseguinte, a sociedade humana, na qual ainda prevalece à ideologia patriarcal (que estabelece a supremacia masculina) ainda impede o pleno desenvolvimento das mulheres, discriminando-as de diferentes maneiras, conforme veremos ao longo deste artigo.

Com o surgimento da internet e dos dispositivos informáticos, a prática que já existia e perpetrava a sociedade ganhou novas formas de ação, surgindo assim, os chamados crimes virtuais, que neste artigo serão analisados sob a ótica da violência de gênero.

Ainda que as vítimas de crimes virtuais possam ser tanto homem, quanto mulher, o que se percebe, pelo conjunto histórico, social e cultural, é que as mulheres estão mais suscetíveis a serem agentes passivas dos referidos crimes, pelo simples fato de seu gênero.

Desse modo, o presente artigo abordará os principais crimes virtuais cometidos contra a mulher e trará a baila a atual legislação brasileira sobre o tema.

2. A CONTEMPORANEIDADE DA VIOLÊNCIA CONTRA A MULHER

A naturalização da violência de gênero[1] há muito tempo permeia a sociedade brasileira, eis que é transmitida de geração a geração, não só pelos homens, mas, também, pelas mulheres. É o primeiro tipo de violência apresentado ao ser humano de forma direta. Se torna assim, a violência enraizada nas relações humanas, vista como se natural fosse. Legitimada pela sociedade.

O conceito de violência de gênero, entendido como uma relação de poder e dominação do homem e de submissão da mulher, demonstra que os papéis foram impostos pela sociedade e consolidados ao longo da história, através do patriarcado e sua fiel ideologia. A indução a relações violentas entre os sexos indica o processo de socialização em que estamos inseridos. Os costumes e educação repassados por nossos ancestrais, infelizmente, preservam (até hoje) estereótipos que reforçam a ideia de que o sexo masculino tem poder sob o sexo feminino.

Num contexto mais rebuscado, temos a violência contra a mulher ganhando notoriedade a partir da realização do primeiro Dia Internacional da Mulher, movimento promovido pela Organização Mundial da Saúde em 1975. Foi a partir desse momento que as discussões sobre o referido tema conseguiram destaque na sociedade, conquistando inclusive mobilizações em prol da mudança dessa realidade (WAISELFISZ, 2015).

---

1 O termo gênero não pode ser confundido com sexo. Este na maioria das vezes, descreve características e diferenças biológicas, enfatiza aspectos da anatomia e fisiologia dos organismos pertencentes ao sexo masculino e feminino. (...) O gênero, no entanto, aborda diferenças socioculturais existentes entre os sexos masculino e feminino, que se traduzem em desigualdades econômicas e políticas, colocando as mulheres em posição inferior à dos homens nas diferentes áreas da vida humana (TELLES e MELLO, 2002)

Um dos reflexos desse sistema pode ser observado em legislação pátria, eis que o Código Civil de 1916, preceituava que o homem era o "chefe da sociedade conjugal", bem como deliberava sobre os bens particulares da mulher e até mesmo sobre o exercício de sua profissão – artigo 233, redação dada pela Lei nº 4.121, de 1962. Vejamos:

> Art. 233. O marido é o chefe da sociedade conjugal, função que exerce com a colaboração da mulher, no interesse comum do casal e dos filhos.
> Compete-lhe:
> I – a representação legal da família;
> II – a administração dos bens comuns e dos particulares da mulher que ao marido incumbir administrar, em virtude do regime matrimonial adotado, ou de pacto, antenupcial (ats. 178, § 9º, nº I, c, 274, 289, nº I e 311);
> III – o direito de fixar o domicílio da família, ressalvada a possibilidade de recorrer a mulher ao Juiz, no caso de deliberação que a prejudique;
> IV – prover a manutenção da família, guardadas as disposições dos arts. 275 e 277.

Frisa-se que o referido Código vigeu até o ano de 2002, quando publicado e sancionado o atual Código Civil brasileiro. Observa-se que a própria legislação positivava a violência de gênero, em diversas dimensões, dentre elas a patrimonial, notadamente porque ao chefe de Família incumbia administrar os bens da mulher em razão do regime matrimonial.

Pouco tempo antes da atualização da legislação civil, tivemos a realização da "Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher", que ficou conhecida como a Convenção de Belém do Pará, na assembleia geral da OEA – Organização dos Estados Americanos – em 1994. A referida Convenção definiu a violência contra a mulher como "qualquer ação ou conduta, baseada no gênero, que cause morte, dano ou sofrimento físico, sexual ou psicológico à mulher, tanto no âmbito

público como no privado" (BRASIL, 1996).
Note-se que a própria expressão "violência contra a mulher" se dá em razão de ser praticada contra pessoa do sexo feminino, tão somente pela sua condição de ser mulher. Expressão que denota a intimidação da mulher pelo homem, que desempenha o papel de seu agressor, seu dominador e seu disciplinador, conforme abordado anteriormente.

Importante destacar ainda, que o Brasil é signatário da agenda 2030 da ONU – Organização das Nações Unidas – e, entre os seus 17 (dezessete) Objetivos de Desenvolvimento Sustentável, é possível encontrar a questão de igualdade de gênero, a Desembargadora Lecine Bodstein (QUESTÃO DE ORDEM 11, 2021) comenta acerca do tema:

> Me parece que o número 8, emprego digno e crescimento econômico é indispensável, sem autonomia financeira não há igualdade de gênero, sem igualdade nós não temos o empreendedorismo e instituições fortes e sem tudo isso nós não temos boa saúde e não temos um bem-estar, evidentemente que os demais itens, como a erradicação da pobreza, energia acessível, combate as alterações climáticas, fome zero, consumo e produção responsável e redução de desigualdades, além da indústria inovação, infraestrutura e parceria em prol das metas, evidentemente que todos estão interligados e nós poderíamos dizer que as mulheres compõem cada um destes 17 objetivos, até porque, 62 ou 64% das mulheres chefes de família são hoje componentes da população rentável brasileira, então não há como sob o aspecto dos direitos fundamentais, da dignidade humana se dizer que a mulher não pode ostentar uma igualdade de direitos, uma igualdade por ser mulher, uma igualdade de trabalho de salário idêntico aos homens e também não se pode sair dessa perspectiva sempre.

Bodstein, relatou ainda que à época de seu ingresso na magistratura, foi perguntado a seu esposo se ele autorizava que ela fosse juíza. (QUESTÃO DE ORDEM 11, 2021). Nesse aspecto, reputa-se importante a percepção de que a violência contra a mulher

ocorre de diversas formas. A Lei nº 11.340/2006 (que será comentada adiante) – Lei Maria da Penha – elenca em seu artigo 7º, cinco tipos de violência, quais sejam: física; psicológica; sexual; patrimonial e; moral (BRASIL, 2006).

À vista de todo o exposto, tem-se que apesar de todos os avanços tecnológicos, a violência de gênero, em todas as suas dimensões, ainda está presente nas relações sociais atualmente.

Nesse liame e, considerando a utilização da tecnologia como meio de perpetuar a violência de gênero, passa-se a abordar alguns crimes cibernéticos em que a vítima normalmente é mulher, em razão da sua condição de mulher.

3. CRIMES VIRTUAIS EM QUE A VÍTIMA HABITUALMENTE É MULHER

Modernamente, a tecnologia ocupa um espaço fundamental em nossa sociedade, tendo modificado de forma consubstancial as relações humanas, principalmente no que tange à comunicação e divulgação de informações. Assim, temos um espaço imensurável de exercício de liberdades, que possibilita a prática de condutas criminosas, por indivíduos que acreditam estarem protegidos pelo anonimato intrínseco ao mundo virtual.

Os crimes virtuais, também conceituados como crimes cibernéticos, há algum tempo vêm ganhando espaço no mundo jurídico, e se buscarmos em nossa memória recente (em meados de 2011) foi noticiado em todas as mídias, o crime praticado contra a atriz Carolina Dieckman, ocasião em que *hackers* invadiram seus dispositivos e divulgaram diversas imagens intimas, fato que motivou a criação da Lei nº 12.737/2012, que dispõe sobre "delitos informáticos" (BRASIL, 2006).

Nesta esteira, aduz Augusto Rossini (2004):

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Muito embora em se tratando de crimes virtuais a vítima possa ser tanto a mulher, quanto o homem, comumente as vítimas são mulheres, simplesmente pela sua condição de mulher. Um dos motivos seria o tabu do corpo nu, sendo, infelizmente, ainda hoje, o corpo da mulher e a genitália dela sexualizados a todo o momento. Uma mulher "não pode", por exemplo, sair de casa sem cobrir os mamilos de seus seios, pois caso o faça, será motivo de olhares julgadores e até mesmo (quase certo de que) sofrer assédio por essa razão.

Desse modo, além de diversos outros motivos, o fato de o corpo feminino ser altamente objetificado, torna a mulher mais suscetível de se tornar vítima de crimes virtuais, como por exemplo do *stalking*, *revenge porn* e da sextorção.

3.1 STALKING

É extremamente importante entendermos o termo *stalking* para que possamos pensá-lo diante da realidade social em que vivemos. Para isso, a melhor forma de conceituar o termo é trazê-lo para a nossa língua natural.

O termo *stalking* deriva do inglês, que em sua tradução literal significa "perseguir", seria para aquele idioma, o ato de se aproximar silenciosamente daquilo ou de quem se persegue. Trazendo a

interpretação para a língua portuguesa e, especialmente, para o âmbito jurídico, stalkear seria perseguir, repetitivamente e insistentemente alguém.

De início o *stalking* somente era associado as pessoas famosas, no entanto, ao longo do tempo, a prática se tornou comum e passou a ser relacionada também a situações de violência doméstica. Como foi o caso dos Estados Unidos, que após o assassinato de cinco mulheres que sofreram perseguição por ex companheiros, originou-se um movimento de verdadeira exposição da prática do *stalking*, trazendo assim, a necessidade de se legislar acerca do assunto, com a criação de leis que criminalizavam a conduta de stalkear. (CARVALHO. 2011)

Stalking é uma das formas de violência, na qual o qual o ofensor invade a privacidade da vítima, repetindo incessantemente a mesma ação por maneiras e atos variados, utilizando-se de táticas e meios diversos, como por exemplo: ligações para o número pessoal ou profissional da vítima; mensagens de cunho sentimental e íntimo; telegramas; flores, recados em faixas; permanência na saída do trabalho, escola ou a espera da sua passagem por algum lugar; frequentar os mesmos locais de lazer, dentre outras. (JESUS, 2008)

Ao passo que existe um sujeito ativo, há também a figura da vítima, que passa a suportar demasiado constrangimento, medo, aflição, sensação de impotência, devido à invasão de sua privacidade e intimidade. Nos casos de vítimas de *stalking*, muitas precisam alterar consubstancialmente suas rotinas e modo de vida, com o fito de evitar os assédios constantes, razão pela qual, acabam, por vezes, desenvolvendo uma série de distúrbios psicoemocionais, como por exemplo, a síndrome do pânico, estresse e transtorno de ansiedade.

Atualmente no Brasil, a conduta foi tipificada como crime, por meio da Lei nº 14.132/2021, publicada em 31 de março do ano corrente. Houve a inclusão no Código Penal do artigo 147-A: "Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade".

3.2 REVENGE PORN

A *revengeporn* ou *nonconsensualpornography*, termos traduzidos para a língua portuguesa como "pornografia de vingança" e "pornografia não consentida", remete a distribuição ou publicação não consentida de imagens de nudez e vídeos que contenham sexo explícito ou a publicação de áudios com conteúdo erótico. (SYDOW; CASTRO, 2019).

Os autores atribuem a palavra vingança inserida na tradução brasileira ao fato de que "Refere-se à conduta da pessoa que, ao fim do relacionamento, dissemina as imagens por meio de websites [...], mídias sociais, chats [...], dentre outros"(SYDOW; CASTRO, 2019).

A pornografia de vingança foi popularizada no Brasil em 2010 e tem ganhado cada vez mais espaço nos índices de crimes cometidos contra a mulher, embora ainda sejam "escassas" as pesquisas de campo sobre a temática. Em 2018 foi publicado o "Projeto Vazou", realizado com o objetivo de mapear a "*cyber* violência" no Brasil. Foram realizadas enquetes com vítimas de exposição pornográfica não consentida, concluindo que 84% das vítimas são meninas e mulheres e que 81% conhecem quem divulgou os arquivos e 84% dos agressores são homens. (PASSOS; MARTINI; SEGATTO, et al., 2018).

Sendo considerada a pornografia de vingança em uma violência de gênero que afeta milhares de mulheres todos os dias. Dentre as diversas causas para a exposição não consentida, associa-se a revenge porn ao fato de que a mulher ainda é considerada objeto e deve sempre atender aos valores morais sociais, o que faz com que a vítima, além de sofrer com toda a humilhação pelo crime, também seja alvo de julgamentos sociais. (FREITAS; COSTA, 2020).

A Lei nº 13.718/2018 tipificou os crimes de importunação sexual e de divulgação de cena de estupro. Trazendo assim, na redação do artigo 218-C a conduta da *revenge porn*, vejamos:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:

A pena para o crime do art. 218-C (pornografia de vingança) é de reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constituir crime mais grave.

3.3 SEXTORSÃO E ESTUPRO VIRTUAL

Ainda em se tratando de crimes virtuais envolvendo a intimidade feminina, temos num primeiro momento a extorsão sexual, situação em que o agente exige da vítima o envio de material erótico ou à prestação de "favores sexuais" em face de ameaças de divulgação de informações confidenciais da vítima, ou até mesmo de imagens e/ou vídeos de conteúdo íntimo de que detenha posse (a obtenção do conteúdo pode ser consentida ou não).

Conforme explica Rogério Sanches Cunha (2017):

> A prática que passou a ser conhecida como sextorsão, refere-se a uma forma de exploração sexual na qual a vítima é chantageada através da ameaça de publicação de imagens e vídeos de si mesma, dotadas de cunho sexual, previamente compartilhadas mediante *sexting* ou subtraídas de seus arquivos pessoais digitais, objetivando a obtenção de alguma vantagem. Nessas situações é comum que a vítima seja constrangida a enviar mais mídias de conteúdo erótico ao agressor, constantemente sob a ameaça de divulgação tanto do conteúdo original quanto deste último obtido sob chantagem.

Surge assim uma nova forma de extorsão, conhecida como "sextorsão", que advém da palavra sexo com extorsão, sendo a extorsão praticada para receber ações. (FRANKLIN, 2014, p. 1303)

Por outro lado, em se tratando do chamado "estupro virtual" seria o cometimento do crime de estupro, tipificado no artigo 213 do Código Penal[2], em que o agente se utiliza da posse de conteúdo íntimo, ameaçando divulgá-las, para obrigar a vítima a praticar relações sexuais com o próprio agente ou com terceiros. (CUNHA, 2017)

Cruz (2018) entende que é preciso analisar o caso concreto e suas nuances para verificar a conduta:

> Se o agente simplesmente constrange a vítima a não fazer o que a lei permite ou fazer o que ela não manda, ou seja, ameaçar a divulgar as fotos caso ela não termine com o atual namorado, teremos o delito de constrangimento ilegal baseado no art. 146 do Código Penal, pois ele não buscou nenhuma vantagem econômica e nem vontade de satisfazer sua lascívia, ele simplesmente queria ver a ex terminando com o atual namorado. Já no segundo delito, se o autor constrange a vítima

2 Art. 213. Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso: Pena-reclusão, de 6 (seis) a 10 (dez) anos.

> com intuito de obter para si ou para outrem vantagem econômica, será configurado extorsão com base no art. 158 do CP; na terceira situação o sujeito constrange a ex-namorada sob pena de divulgar as fotos, em troca dela se despir e explorar seu próprio corpo se masturbando para que ele, do outro lado e pela webcam, possa satisfazer sua lascívia; neste caso, a sextorsão configura o delito de estupro.

Importante destacar aqui que, o entendimento do Superior Tribunal de Justiça em relação ao crime de estupro, é de que a prática delitiva não pressupõe contato físico.[3]

4. A EVOLUÇÃO DA LEGISLAÇÃO BRASILEIRA E A (IN)SUFICIÊNCIA EM RELAÇÃO AOS CRIMES VIRTUAIS COMETIDOS CONTRA A MULHER

Sem dúvida alguma, um dos feitos legislativos mais importantes no que diz respeito ao enfrentamento dos crimes praticados por meios virtuais, foi o Marco Civil da Internet – Lei nº 12.965/2014 -, que como a própria nomenclatura traduz, um marco. O legislador buscou estabelecer princípios, garantias, direitos e deveres para os usuários de internet no Brasil. Contudo, importante destacarmos que a Lei apresentou poucas inovações, sendo deficiente em diversos aspectos, principalmente pelo fato de que é impossível regular uma rede mundial em âmbito nacional.

Para Eduardo Tomasevicius Filho (2016) comenta sobre as deficiências técnicas da referida legislação:

---

3 A Quinta Turma do Superior Tribunal de Justiça já decidiu pela desnecessidade do contato físico para a configuração do crime de estupro. Constou no voto relator que "a maior parte da doutrina penalista pátria oriente no sentido de que a contemplação lasciva configura o ato libidinoso constitutivo dos tipos dos artigos 213 e 217-A do Código Penal, sendo irrelevante, para a consumação dos delitos, que haja contato físico entre ofensor e ofendido". (STJ. 5ª Turma. RHC 70.976-MS, Rel. Min. Joel Ilan Paciornik, julgado em 2/8/2016)

> Por outro lado, são muitas as deficiências e insuficiências do Marco Civil da Internet, mesmo depois da revisão do projeto inicial por meio da aprovação do texto substitutivo. Afinal, toda lei aprovada tem a finalidade de inovar o ordenamento jurídico, acrescentando normas necessárias à regulação dos comportamentos, eliminando aquelas que não mais atendem às necessidades sociais. O primeiro ponto a ser observado é a redundância de várias de suas disposições, que repetem, com insuficiência, o que já consta na Constituição Federal. Nenhuma "ginástica hermenêutica" é capaz de permitir ao operador do direito a obtenção de significado adicional. Por exemplo: o art.5º, X, da Constituição Federal dispõe que: "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", e o art.7°, I, do Marco Civil da Internet dispõe que é direito dos usuários da internet a: "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano moral e material decorrente de sua violação".

Acerca da temática, o Relatório apresentado em 2017 sobre "Violência contra a mulher na internet: diagnóstico, soluções e desafios" (CODING RIGTHS; INTERNETLAB, 2017) dispõe:
Lacunas:

> 1. Jurisprudência e entrevistas com atores do campo indicam que a regra do Marco Civil tem ajudado na remoção mais expedita desses conteúdos, e não há indícios de usos abusivos (para censurar conteúdos protegidos por liberdade de expressão, por exemplo). No entanto, essa avaliação será sempre parcial, pois como a remoção é privada, não temos os dados ou informações sobre número de pedidos x número de remoções, ou ainda
> justificativas para remoção ou não.
> 2. A regra, embora pareça positiva, deveria vir acompanhada de um dever de transparência, com preocupação com a privacidade das pessoas envolvidas.

Aqui, deve-se observar que, antes mesmo do advento do Marco Civil da Internet, em 2014, tivemos, na esfera legislativa, um considerável avanço no que diz respeito aos crimes virtuais, qual seja a

Lei nº 12.737/2012, mais conhecida como "Lei Carolina Dieckman"[4] que buscou combater a invasão de dispositivos informáticos alheios, conectados ou não à rede mundial de computadores.

Assim, foi incluído no Código Penal brasileiro, o artigo 154-A, considerado um dos, se não o maior avanço proporcionado pela norma. Isso porque, seu objetivo principal foi combater às principais práticas danosas a quem utiliza ou necessita dessas tecnologias, vejamos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (redação da Lei nº 12.737/2012)

O legislador, utilizou-se de inúmeras expressões ambíguas na redação do artigo, gerando inquietante violação ao princípio da legalidade estrita e trazendo a ineficácia do dispositivo. (TAVARES; RIBEIRO, 2018)

Recentemente, o Poder Legislativo inovou, mais uma vez, no que concerne ao enfrentamento dos crimes cibernéticos, com a Lei nº 13.718/2018 que tipifica os crimes de importunação sexual e de divulgação de cena de estupro, conforme citado anteriormente.

Insta salientar que antes da referida Lei, o ordenamento jurídico brasileiro não possuía um tipo penal específico que fosse capaz de punir a conduta de divulgar conteúdo íntimo sem o consentimento da vítima. Assim, o legislador – como foi no caso da Lei Carolina Dieckman – com o intuito de atender aos anseios da

4 Em meados de 2011, Carolina Dieckman foi vítima de hakcers que invadiram seus dispositivos e obtiveram acesso a informações e conteúdos pessoais e íntimos da atriz.

população, criou um tipo penal para que tais condutas pudessem ter repreensão estatal e de alguma forma fossem coibidas pelo poder público.

Merece especial destaque, o disposto no §1º do artigo 218-C, que diz: "A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação". E por que o destaque para essa redação? Conforme comentado desde a introdução desse artigo, as mulheres estão mais suscetíveis a ser vítimas dos chamados crimes virtuais contra a dignidade sexual, como é o caso da revenge porn, nesse sentido a Lei, buscou dar maior proteção às mulheres vítimas de violência doméstica.

De outro giro, nota-se que a legislação pátria caminhou mais um passo em busca de tentar proteger bens jurídicos no âmbito virtual, com a tipificação do crime de *stalking*, vide redação dada pela Lei nº 14.132/2021, que alterou o Código Penal para a inclusão do artigo 147-A. Leia-se excerto:

> Art. 147-A.Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

A referida Lei também traz disposição específica de proteção a mulher, confirmando a notoriedade de que as mulheres estão mais vulneráveis aos crimes virtuais contra a honra e dignidade sexual: II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código.

Acerca do *caput* do artigo 147-A, percebamos que para haver a subsunção do fato à norma, o tipo penal exige que a "perturbação reiterada" gere – ou seja capaz de gerar – uma das três

situações previstas no dispositivo: ameaça à integridade física ou psicológica; restrição da capacidade de locomoção ou; invasão ou perturbação da liberdade ou privacidade. Assim, mesmo que o agente não possua dolo específico de gerar essas consequências, o tipo exige sua verificação. Desse modo, deve restar caracterizado, no caso concreto, a espécie de abalo sofrido pela vítima.

Frente às críticas, de retorno a nova lei brasileira, é importante dizer que a recente tipificação acaba por corrigir uma dificuldade anterior de enquadrar formalmente a conduta prevista no artigo, que ora caminhava entre o crime de ameaça - do art. 147, do Código Penal -, ora alcançava a contravenção penal de perturbação de tranquilidade (do art. 65, do decreto-lei 3.688/41), esta última, que acabou por ser revogada pela lei 14.132/21. (PACHECO, 2021)

Outro aspecto importante, que merece destaque no que diz respeito à insuficiência das normas, é que em alguns casos, a pena base aplicável ao tipo penal é totalmente desproporcional ao dano causado à vítima.

Muito embora tenhamos legislações atuais que versam sobre crimes virtuais e que zelam pelo combate à violência contra a mulher, não há como deixar de citar a Legislação pioneira, conhecida como Lei Maria da Penha, a Lei nº 11.340/2006 já foi considerada pela ONU, como uma das melhores legislações contra a violência de gênero. (INSTITUTO BRASILEIRO DE DIREITO DE FAMÍLIA, 2009).

A Lei Maria da Penha, trouxe inovações no que diz respeito a conceituação de violência, deixando de lado a ideia primitiva de que violência contra a mulher se limita à agressão física (muito embora seja uma das mais preocupantes). Conforme já citado neste artigo, a legislação em questão trouxe em seu artigo 7º,

cinco tipos de violência, quais sejam: física; psicológica; sexual; patrimonial e; moral. Perceba-se que, dos crimes virtuais abordados neste artigo, para além da violência sexual, conseguimos verificar a presença de diversos tipos de violência.

E mesmo sob esta ótica, é possível perceber que a legislação não é suficiente para coibir, nem tampouco reparar os danos causados às vítimas.

Diz-se isto, porque apesar das tipificações realizadas pelo legislador nos últimos anos, houve aumento considerável no cometimento desses delitos nos últimos anos.

Tal constatação viabiliza afirmar que a função preventiva da norma penal – prevenção geral e especial – não atinge seu objetivo em tais crimes, nem a curto e nem a médio prazo.

Além disso, ao realizar detida análise dos projetos de Lei dos delitos anteriormente citados, nota-se que tramitaram durante anos e mesmo após diversas revisões possuem problemas dogmáticos graves, notadamente porque a redação deles vai de encontro com princípios básico de direito penal sem mencionar as afrontas a questões positivadas em cláusulas pétreas constitucionais.

Por tais razões, entre outras, é que se aponta a insuficiência da legislação brasileira atual para o enfrentamento dos crimes virtuais praticados contra a mulher.

5. CONSIDERAÇÕES FINAIS

Note-se que, apesar da "boa vontade" do Poder Legislativo, as Leis que regem a matéria dos crimes virtuais se mostram insuficientes para abarcar todos os crimes e danos cometidos na modalidade virtual contra a mulher, e quiçá, entende esta pesquisadora, haverá alguma que assim o faça. Eis que a raiz do problema não é normativo, mas sim social. Conforme trazido nesta pesquisa, a violência contra a mulher é trazida desde o seio do nascimento e passa de geração para geração, chegando a ser confundida com algo natural.

Desse modo, é possível concluir que não surgiram novos tipos de violência, mas novas formas de praticar aquelas já preexistentes e praticadas em nossa sociedade. Que até pouco tempo se encontrava positivada em Lei, como é o absurdo do teor do artigo 233, do Código Civil de 1916 (atualizado pela Lei nº 4.121 de 1962), sendo retirada do ordenamento jurídico somente no ano de 2002 – há menos de 20 anos.

No entanto, não há como negar que os esforços têm sido constantes, também pelo fato de que o Brasil é signatário da agenda 2030 (AGENDA 2030, 2018), que prevê dentre os seus principais objetivos a erradicação da desigualdade de gênero e violência contra as mulheres.

Além disso, muito embora a doutrina possua ferrenhas as críticas do ponto de vista técnica sobre as Leis que abordam a temática apresentada, devemos reconhecer que antes delas, sequer era possível punir o agente/agressor.

Por fim, ainda que existam pontos positivos e que merecem destaques, a legislação atual que versa sobre os crimes virtuais (em especial quanto a proteção das mulheres), funcionam como "tapa

buracos", amenizando, a cada nova publicação de Lei, a deficiência normativa, mas, que até o momento não são capazes de coibir e tampouco abrandar os danos causados às vítimas.

REFERÊNCIAS BIBLIOGRÁFICAS

AGENDA 2030. **Acompanhando o desenvolvimento sustentável até 2030**. 2018. Disponível em http://www.agenda2030.org.br/acompanhe Acesso em: 21 ago. 2021.

BRASIL. **Decreto nº 1.973, de 01 de agosto de 1996**. Promulga A Convenção Interamericana Para Prevenir, Punir e Erradicar A Violência Contra A Mulher, Concluída em Belém do Pará, em 9 de Junho de 1994.. Brasília, DF, 01 agosto 1996, Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1996/d1973.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 2.848, de 7 de dezembro de 1940**. Institui o Código Penal. Brasília, DF, 7 de dezembro de 1940 Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 3.071, de 1º de janeiro de 1916**. Institui o Código Civil. Brasília, DF, 1º de janeiro de 1916 Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l3071.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei 10.406, de 10 de janeiro de 2002**. Institui o Código Civil.Brasília, DF, 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 2 jun. 2021.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção

sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências. Brasília, DF, 7 de agosto de 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 21 ago. 2021.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília, DF, 24 de setembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em 21 ago. 2021.

BRASIL. **Lei nº 14.132, de 31 de março de 2021**. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais), Brasília, DF, 31 de março de 2021. Disponível

em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acesso em 21 ago. 2021.

CARVALHO, Célia Sofia de Souza. ***Ciberstalking:* prevalência na população universitária da universidade do minho**. 2011. 45 f. Dissertação (Mestrado) - Curso de Psicologia, Psicologia da Justiça, Universidade do Minho, Braga, 2011. Disponível em: http://repositorium.sdum.uminho.pt/handle/1822/18638. Acesso em: 21 ago. 2021

CODING RIGHTS; INTERNETLAB. **Violências Contra Mulher na Internet: diagnóstico, soluções e desafios**. Contribuição conjunta do Brasil para a relatora especial da ONU sobre violência contra a mulher. São Paulo, 2017.

CRUZ, Diego. RODRIGUES, Juliana. **Crimes Cibernéticos E A Falsa Sensação De Impunidade**. Garça: Faef, v. 13, jan. 2018. Semestral. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 21 ago. 2021.

CUNHA, Rogério Sanches. **Manual de Direito Penal: parte geral** (arts. 1º ao 120). 7ªEd., Salvador: JusPodivm, 2019.

DULLIUS, Aladio Anastácio. **Dos Crimes Praticados em Ambientes Virtuais**. 2012. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/30441/dos-crimes-praticados-em-ambientes-virtuais. Acesso em: 21 ago. 2021.

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: uma lei sem conteúdo normativo**. 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?l . Acesso em 21 ago. 2021.

FREITAS, Maria Victória Pasquoto. COSTA, Marli Marlene Moraes. ***Revenge Porn:* por que as mulheres sofrem mais?** Revista da 16ª Jornada da Pós-Graduação e Pesquisa – Congrega. 2020. Disponível em: http://revista.urcamp.tche.br/index.php/rcjpgp/article/view/3935/2700. Acesso em: 21 ago. 2021.

INSTITUTO BRASILEIRO DE DIREITO DE FAMÍLIA. **Para ONU, Lei Maria da Penha é uma das mais avançadas do mundo**. 2009. Disponível em: https://ibdfam.jusbrasil.com.br/noticias/2110644/para-onu-lei-maria-da-penha-e-uma-das-mais-avancadas-do-mundo. Acesso em: 21 ago. 2021.

JESUS, Damásio. ***Stalking***. 2008. Disponível em: https://jus.com.br/artigos/10846/stalking. Acesso em: 21 ago. 2021.

PACHECO, Vitor Pereira. **O crime de perseguição: breves críticas sobre o *stalking* no direito brasileiro**. 2021. Disponível em: https://www.migalhas.com.br/depeso/342950/o-crime-de-perseguicao. Acesso em: 21 ago. 2021.

SANTOS, Alice Gonçalves dos; MARTINI, Ana Maria Magnus; SEGATTO, Anderson José da Silva. **Projeto vazou: pesquisa sobre o vazamento não consentido de imagens íntimas no brasil**. 2018. Grupo de estudos em criminologias contemporâneas. Disponível em: https://www.projetovazou.com/resultado.pdf. Acesso em: 21 ago. 2021

QUESTÃO DE ORDEM 11: **O Enfrentamento da Violência Doméstica e Familiar Contra a Mulher**. Entrevistada: Lenice Bodstein. Entrevistadora: Katiely Lemes Ribeiro. ESACast. 04 mai. 2021. Podcast. Disponível em: https://open.spotify.com/episode/3BelCz5KoWCbeuO51lKzZ6?si=9CT59jrWTsK5UsdNj8aA6Q&dl_branch=1. Acesso em: 21 ago. 2021.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. 2014. Disponível em: http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 21 ago. 2021.

SYDOW, Spencer Toth; DE CASTRO, Ana Lara Camargo. **Exposição Pornográfica Não Consentida na Internet: da pornografia de vingança ao lucro** [Coleção Cybercrimes]. 2. ed. Belo Horizonte: Editora D'Plácido, 2019.

TAVARES, Jéssica Andressa Gomes; RIBEIRO, Katiely Lemes. **A (In) Eficácia do Direito Penal Como Resposta ao Clamor Público nas Redes Sociais**. Disponível em: http://abdconst.com.br/3-anais--do-xiii-simposio. Acesso em: 21 ago. 2021.

WAISELFISZ, Julio Jacobo. **Mapa Da Violência 2015: Homicídio De Mulheres No Brasil**. 1ª. Ed. Brasília: Flacso, 2015.

O MONITORAMENTO ELETRÔNICO DE PESSOAS PRESAS NA PANDEMIA DO NOVO CORONAVÍRUS

THE ELECTRONIC MONITORING OF INMATES DURING THE PANDEMIC OF THE NEW CORONAVIRUS

Fernando César Domingues da Silva
Advogado criminalista. Bacharel em Direito pela Faculdade de Direito de Curitiba (UNICURITIBA). Especialista em Direito Penal e Processo Penal pela Academia Brasileira de Direito Constitucional (ABDConst). Membro da Comissão de Defesa dos Direitos das Crianças e dos Adolescentes da OAB/PR.
fernandocesardomingues@hotmail.com

Marília Silva Scriboni
Advogada criminalista. Bacharel em Jornalismo pela Faculdade Cásper Líbero. Bacharel em Direito pela Universidade Presbiteriana Mackenzie. Especialista em Direitos Fundamentais pela Universidade de Coimbra/IBCCrim.
mascriboni@gmail.com

RESUMO:
O artigo trata do monitoramento eletrônico nos tempos de pandemia de coronavírus, analisando, por meio de pesquisa bibliográfica, o uso da tornozeleira eletrônica para reduzir a quantidade de encarcerados em tal época. Aborda também a história da pena privativa de liberdade e o cárcere, delineando como iniciou a crise do sistema penitenciário brasileiro, bem como traçando o vínculo entre o atual contexto civilizatório e o encarceramento em massa.

Palavras-Chave: Covid-19. Execução Penal. Encarceramento em massa. Monitoramento eletrônico. Tornozeleira eletrônica.

ABSTRACT:
The article analyzes the eletronic monitoring in pandemic times of coronavirus, analyzing the use of eletronic anklet to reduce the number of imprisioned at this time. It also discusses the history of penalty and the prison, outlining how the crisis in brazilian penitentiary system, as well as tracing the link between our civilizing context and mass incarceration.

Keywords: *Covid-19. Criminal Enforcement. Electronic Monitoring. Electronic Anklet. Mass Incarceration.*

1. INTRODUÇÃO

O monitoramento eletrônico de pessoas privadas de liberdade no Brasil completou 11 anos de existência com uma prova de fogo: a pandemia do novo coronavírus, ou Sars-CoV-2, causador da Covid-19.

Instituída pela Lei nº 12.258, publicada em 15 de junho de 2010, o monitoramento por meio de pulseira ou tornozeleira eletrônicas dividiu opiniões desde o princípio. De um lado, especia-

listas comentavam que esse tipo de controle estatal não tinha razão de ser, com críticas que iam desde o alto investimento nos equipamentos até o provável estigma causado ao seu usuário. De outro, estudiosos do sistema carcerário enxergavam na opção uma forma de supostamente humanizar o cárcere e de reintegrar o preso à sociedade em razão de seu caráter, ao menos aparentemente, desencarcerador.

O Brasil detém números alarmantes em se tratando do sistema carcerário: possui a terceira maior população carcerária do mundo[1], com cerca de 682,1 mil presos, e um déficit de vagas[2] conhecido inclusive por entidades internacionais de Direitos Humanos, estando 54,9% acima da capacidade (SILVA; GRANDIN; CAESAR; REIS, 2021). Desses, 31,9% consistem em presos provisórios, ou seja, que ainda aguardam pelo julgamento.

Dito de outra forma, o sistema carcerário é uma panela de pressão prestes a explodir. Soma-se a isso o racionamento de água, a escassez de produtos de limpeza e de higiene pessoal e, por último, mas não menos importante, a atuação das facções. Em um cenário pandêmico, o ambiente insalubre das unidades prisionais é propício ao alastramento rápido de qualquer agente etiológico, atingindo não só a população carcerária, como também trabalhadores terceirizados e agentes penitenciários e seus familiares.

Apenas para ilustrar como a insalubridade do ambiente prisional favorece a contaminação, em 2018 o Brasil registrou 78 mil novos casos de tuberculose, sendo que o sistema prisional concentrou

1 A população carcerária brasileira só não é menor do que a dos Estados Unidos, com 2 milhões 100 mil pessoas atrás das grades) e China (1 milhão e 700 mil pessoas encarceradas) (CONECTAS, 2020).

2 Segundo dados do Infopen, no Levantamento Nacional de Informações Penitenciárias 2019, existiam no país 442.349 vagas, ao passo em que havia 755.274 pessoas privadas de liberdade.

12% deles (O GLOBO, 2018). E mais: estima-se que o risco de contrair a doença no cárcere seja até 34 vezes maior do que fora dele.

Com a Covid-19 não poderia ser diferente. De acordo com levantamento realizado pela Agência Pública, mais de 80% das unidades prisionais brasileiras apresentaram casos de contaminação pelo novo coronavírus, o que significa um impacto em ao menos 877 unidades. Acredita-se, porém, que os números possam ser maiores em virtude da subnotificação e da ausência de testagem. Em números absolutos, foram contabilizadas oficialmente mais de 90,6 mil contaminados, além de mais de 560 mortes em decorrência da Covid-19 (BRASIL, 2021).

Em razão do potencial risco não somente no cárcere, mas também na sociedade além dos muros das prisões, o Conselho Nacional de Justiça recomendou o uso do monitoramento eletrônico para determinados casos, como será tratado mais adiante.

Assim, o presente artigo é dividido em três momentos. No primeiro, os autores discorrem sobre a evolução histórica da pena de prisão, desde as prisões eclesiásticas até os sistemas penitenciários modernos.

Em seguida, será exposta a virada punitiva, explicando a vinculação da sociedade de risco com a expansão do direito penal, concedendo destaque às características do expansionismo punitivo de acordo com a obra de SILVA SÁNCHEZ (2002), esclarecendo assim os motivos da grande inflação legislativa no âmbito criminal nas últimas décadas. Em tal contexto revela-se como se deu o encarceramento em massa na segunda metade do século XX.

Por fim, o artigo foca em tecer comentários sobre o monitoramento eletrônico em tempos de pandemia, quando apresentou um aumento considerável.

2. A PENA E O CÁRCERE

A pena privativa de liberdade não surgiu há muito tempo e inicialmente era apenas uma forma de custódia do condenado para aplicação da pena de morte ou uma simples privação de liberdade por dívidas, como havia na sociedade feudal. Na sociedade pré-industrial o cárcere como pela ainda não existia, exceto como instituição (MELOSSI; PAVARINI, 2010, p. 34). A instituição do cárcere é menos recente que o cárcere como pena, preexistindo a sua previsão nas legislações penais (FOUCAULT, 2014, p. 24).

O cárcere como reclusão, tendo por finalidade a correção, tem seu início na Inglaterra no final do século XIV, momento em que o sistema socioeconômico feudal estava começando a se desagregar. Todavia, em determinados setores da sociedade feudal, lembrando que eram estados teocráticos cristãos, já haviam formas de penas objetivando a correção e que não eram ainda encontradas nos âmbitos laicos do mundo medieval, que era a prisão eclesiástica (MELOSSI; PAVARINI, 2010, p. 34).

A Igreja Católica criou as primeiras formas de cárcere, consistindo em sanções aos clérigos e demais integrantes da comunidade religiosa que haviam cometido alguma infração disciplinar, obrigando-os a cumprir penitência em uma cela, até o momento em que se arrependesse (MELOSSI; PAVARINI, 2010, p. 23). Eis a origem do termo “penitenciária”.

A pena na prisão eclesiástica atribuiu ao tempo de internamento uma quantia de tempo necessária para “purificação”, conforme os critérios do sacramento da penitência, tendo natureza terapêutica. Dario Melossi expõe a natureza de tal pena:

> Não era tanto a privação da liberdade em si que constituía a pena, mas sim a ocasião, a oportunidade para que, no isolamento da vida social, pudesse ser alcançado aquilo que era o objetivo ideal da pena:

> o arrependimento. Essa finalidade deve ser entendida como correção, ou possibilidade de correção, diante de Deus, e não como regeneração ética e social do condenado-pecador. (MELOSSI; PAVARINI, 2010, p. 24-25)

Dessa forma, a pena eclesiástica é fundada na gravidade do delito e não na periculosidade do réu. A existência desse cárcere sempre teve um sentido religioso, apesar da possibilidade de ser utilizado com finalidades políticas (MELOSSI; PAVARINI, 2010, p. 23).

Após a dissolução da sociedade feudal na Europa ocidental, há o surgimento das casas de correções para condenados por pequenos delitos *(pettyoffenders)* na Inglaterra, onde eram colocados também pessoas integrantes de classes marginalizadas. Nessas casas ou bridwells os condenados eram corrigidos por meio do trabalho forçado (MELOSSI; PAVARINI, 2010, p. 33). Na Europa continental a primeira casa de correção foi erguida na segunda metade do século XVI, tendo por base os bridwells, sendo instalada em Amsterdã. A experiência neerlandesa, influenciada pelo calvinismo, com tais estabelecimentos serviu de inspiração para os demais países europeus ao longo do século XVII (MELOSSI; PAVARINI, 2010; p. 103).

No entanto, é importante esclarecer que, até meados do século XVIII, os delitos considerados graves eram sentenciados com penas mais severas do que o cárcere este com trabalhos forçados sendo elas o degredo, o enforcamento ou o suplício (BITTENCOURT, 2001, p. 23).

As características mais desumanas de determinadas penas passaram a ser contestadas por filósofos e juristas, fortemente influenciados pelo pensamento iluminista, entre eles Cesare Bonesana (o Marquês de Beccaria), Jean-Paul Marat, Jeremy Bentham e John Howard. Tais pensadores exigiam uma reforma no sistema penal, com fundamento nas liberdades individuais e na dignidade

humana, e este movimento teve reflexos no Brasil, apesar de tardio. A primeira Constituição do Brasil, outorgada em 1824, trouxe ao ordenamento jurídico brasileiro a reforma penitenciária ocorrida na Europa durante as últimas décadas do século XVIII, sendo determinado a partir desta carta que as edificações prisionais devam ser arejadas, limpas e seguras, regra esta corroborada pelo Código Penal de 1830, tendo esta legislação estabelecido a prisão simples ou com trabalhos compulsórios para grande maioria dos crimes (JUNIOR, 2012).

O cárcere como pena tornou-se a principal forma de punição no decorrer do século XVIII, sendo consequência do movimento pela reforma do sistema penal no período iluminista, haja vista o declínio do uso das velhas formas punitivas e da decadência das penas corporais. Entretanto, as mudanças na estrutura dos estabelecimentos prisionais também são consequências do desenvolvimento do capitalismo (MELOSSI; PAVARINI, 2010, p. 103).

A Revolução Industrial criou um vasto exército de reserva de desempregados, visto que, segundo MELOSSI e PAVARINI (2010), tornou o trabalho compulsório sub-remunerado nas casas de correção, além de obsoleto e inútil, pois nas workhouses eram realizados trabalhos com sistemas arcaicos, mesmo nas “elogiadas” casas de correção neerlandesas. O avanço tecnológico na virada do século XVIII para o XIX tornou inviável continuar produzindo por meio dos velhos sistemas a um custo competitivo. As máquinas ampliaram o exército de desocupados (MELOSSI; PAVARINI, 2010, p. 26). Os numerosos desocupados eram obrigados, para não morrer de fome, a mendigar, vagar e roubar, convertendo-se em “bandidos” (MELOSSI; PAVARINI, 2010, p. 26). Nesse contexto ocorre o advento do cárcere como a principal forma do cumprimento de pena.

MELOSSI e PAVARINI (2010) afirmam que o cárcere como pena se dá não por princípios humanitários do iluminismo ou por haver a finalidade de reabilitação do condenado, mas por ser necessária uma ferramenta para punir o criminoso e submetê-lo ao regime socioeconômico dominante, o capitalismo (MELOSSI; PAVARINI, 2010, p. 25). A prisão procura disciplinar o delinquente para torná-lo uma força de trabalho e "introduzi-lo coativamente no mundo da produção manufatureira" (BITTENCOURT, 2001, p. 23), transformando-o em um indivíduo dócil e menos provido de conhecimentos, impedindo-o de ser uma pessoa que resiste ao sistema. O condenado, inserido de maneira forçada no modo de produção capitalista, garantia à burguesia ascendente mão-de-obra barata e disciplinada (MELOSSI; PAVARINI, 2010, p. 193).

É perceptível o vínculo da disciplina e da transformação do condenado por meio do encarceramento, conforme esclarece Michel Foucault (FOUCAULT, 2014):

> Uma coisa, com efeito, é clara: a prisão não foi primeiro uma privação de liberdade a que se teria dado em seguida uma função técnica de correção; ela foi desde o início uma "detenção legal" encarregada de um suplemento corretivo, ou ainda, uma empresa de modificação dos indivíduos que a privação de liberdade permite fazer no sistema legal. Em suma, o encarceramento penal, desde o início do século XIX, recobriu ao mesmo tempo a privação de liberdade e a transformação técnica dos indivíduos (FOUCAULT, 2014, p. 225).

O cárcere, agora como forma principal e mais comum de punição legal, gerou diversos sistemas penitenciários diferentes, havendo formas distintas de cumprimento de pena privativa de liberdade, cada um de acordo com o contexto socioeconômico e político de cada Estado (JUNIOR, 2012).

Durante o final do século XVIII e início do século XIX houveram diversos sistemas penitenciários, todos inspirados nas experiên-

cias europeias e a maioria com finalidades ressocializadoras dos condenados, sendo tal ressocialização ocorrendo após o isolamento, ensino religioso, do ensino de um ofício ou mesmo pela imposição de castigos corporais (BITTENCOURT, 2001, p. 25). Dentre tais sistemas, o que predominou foi o sistema progressivo, onde o tempo de duração da pena passou a ser distribuído em períodos, havendo concessões conforme o bom comportamento e inserção do condenado nos tratamentos, podendo ele ser liberado do estabelecimento prisional antes do término da pena (JUNIOR, 2012). O sistema progressivo passou a ser aplicado no Brasil, com certas adaptações, porém é alvo de críticas e tem sua credibilidade contestada há décadas pelos mais diversos doutrinadores brasileiros.

Os Estados Unidos e alguns países europeus, que aplicam o sistema progressivo, investem em tecnologia para desenvolver ferramentas voltadas ao cumprimento de pena privativa de liberdade por meio do monitoramento eletrônico, para aqueles que foram condenados por crimes de menor potencial ofensivo (BITTENCOURT, 2001). O monitoramento eletrônico é utilizado por diversos países como um meio alternativo à execução da pena privativa de liberdade, para que o condenado que tenha a possibilidade de utilizar desta modalidade possa cumprir sua pena em local distinto do estabelecimento prisional tradicional.

3. DA VIRADA PUNITIVA

Apesar de ter havido uma modificação das penas e na instituição do cárcere, durante a virada do século XVIII para o século XIX, por influência do iluminismo, enquanto ocorria o período da primeira industrialização, na segunda metade do século XX, o mundo ocidental decidiu aplicar penas mais severas e alargar os horizontes da legislação penal, o que influencia bastante no que se refere à pena e cárcere.

Essa virada punitiva é compreendida ao analisar os atributos do contexto deste período e quem realizou minuciosamente tal análise foi o sociólogo alemão Ulrich Beck (BECK, 2011, p. 189-202).

3.1. DA SOCIEDADE DE RISCO

No mundo ocidental, do final do século XVIII até a primeira metade do século XX, havia uma confiança no futuro e uma fé no capitalismo industrial, resultantes do otimismo com relação ao desenvolvimento científico e tecnológico que começava a acelerar no referido período. Tal conjuntura – de foco no processo de aumento da produtividade industrial e avanços tecnológicos - resultou em um "superdesenvolvimento" das forças produtivas, desencadeando, paralelamente, em forças destrutivas (BECK, 2011, p. 25).

A consequência do acelerado progresso industrial foi destruição do meio ambiente, o grande fortalecimento da indústria bélica (colaborando com guerras devastadoras), a ameaça nuclear, entre outros âmbitos que no atual contexto civilizatória expõe a sociedade a um risco.

Assim, aquela confiança no desenvolvimento tecnológico existente na sociedade industrial desaparece, sendo substituído por

um pessimismo e um medo dos riscos decorrentes de tal desenvolvimento. BECK (2011) conceitua sociedade de risco da seguinte forma: "O conceito de sociedade de risco expressa a acumulação de riscos –ecológicos, financeiros, militares, terroristas, bioquímicos, informacionais–, que tem uma presença esmagadora hoje em nosso mundo" (BECK, 2011, p. 361).

Esta acumulação de riscos é bastante vinculada à revolução industrial e demanda por "superprodutividade", conforme BOTTINI (2008): "A sociedade de risco é fruto do desenvolvimento do modelo econômico que surge na Revolução Industrial, que organiza produção de bens por meio de um sistema de livre concorrência mercadológica" (BOTTINI, 2008, p. 32).

Além da revolução industrial, a sociedade de risco tem forte ligação com o fenômeno da globalização, que internacionaliza os riscos e afeta o âmbito socioeconômico e financeiro, intensificando as diferenças sociais pelo aumento da pobreza, de acordo com GUARAGNI, CHOUKR, LOUREIRO e VERVAELE (2014):

> Em resumo: a corporação produz, como sujeito central, nos marcos da sociedade de consumo e da economia globalizada de mercado, riscos objetivos profusos, apoiados em dois vetores: a intensidade de produção, distribuição e uso de tecnologias de risco de um lado; a exclusão socioeconômica, de outro (GUARAGNI; CHOUKR. LOUREIRO; VERVAELE, 2014, p. 43)

Então, quando a população percebe os resultados desastrosos do acelerado desenvolvimento industrial, havendo uma busca por atenuar os problemas causados, a sociedade passa a se perceber como uma sociedade de risco.

Todavia, o que há é uma comercialização de formas de atenuar os riscos, mas nunca de meios de evitá-los, sendo uma nova indústria. Não há exercício efetivo de prevenção de tais riscos, uma vez

que seria negativo para o sistema econômico vigente (BECK, 2011, p. 68).

Nas palavras de BOTTINI (2008): "O sistema econômico saca proveito dos riscos que produz, monetariza o risco e cria uma indústria de domínio da periculosidade à qual interessa travar a disputa pelo grau de tolerância admitido pela sociedade" (BOTTINI, 2008, p. 32).

Assim, na forma como apresentada pelas referências citadas, fica evidente que a ciência foi utilizada em prol do lucro em detrimento do desenvolvimento civilizatório que poderia ocorrer. O avanço tecnológico é sustentado pelas grandes indústrias em benefício delas mesmas (GUARAGNI, CHOUKR, LOUREIRO e VERVAELE, 2014).

Apesar do protagonismo da sociedade de risco ser da política, tal contexto é de grande desenvolvimento científico conforme já exposto e uma ciência bastante utilizada nesta época é a estatística, que é constituída por dados, e nela se analisam os danos que já aconteceram, servindo de fonte para prevenção aos riscos futuros, e conforme Beck, os riscos indicam "um futuro que precisa ser evitado" (BECK, 2011, p. 59), mas essa prevenção é muito pouco efetiva, pois tais ações preventivas visam apenas mitigar problemas e crises futuras, que já têm sua ocorrência "prognosticada" (BECK, 2011, p. 68). Na sociedade de risco não se busca algo "bom", apenas evitar o pior (BECK, 2011, p. 59-60).

A sociedade do Século XXI está repleta de incertezas e inseguranças, sem segurança jurídica e social. Os riscos existem, tanto os antigos, como a fome, quantos os novos, como os desastres ambientais, colocando as ciências e as tecnologias em uma perspectiva crítica perante a população (CABRERA, 2017).

Em tal contexto civilizatório, a população vive com medo e insegurança em níveis imensuráveis, que resulta em um clamor social por respostas fáceis e ligeiras, para, ao menos, atenuar tais sentimentos, tais riscos. Buscando atender o clamor social, o Estado utiliza do mecanismo mais violento de que dispõe: o direito penal.

3.2. O DIREITO PENAL NA SOCIEDADE DE RISCO

A sociedade de risco, em razão do sentimento de medo e insegurança intensificados, aumenta demasiadamente a utilização do direito penal como ferramenta de controle dos riscos, ou seja, o contexto civilizatório brevemente descrito anteriormente afeta diretamente a legislação penal. Corrobora tal fato BOTTINI (2008): "A compreensão do paradoxo do risco é indispensável para o estudo do direito penal na atualidade. O risco, elemento central na organização social, será fator determinante para a orientação da política criminal" (BOTTINI, 2008, p. 47).

Como consequência dessa necessidade de conter, ainda que simbolicamente, os riscos decorrentes do desenvolvimento tecnológico, temos a virada punitiva -no que se refere às penas- e a expansão do direito penal, no que tange à legislação penal (BOTTINI, 2008, p. 47-51).

SILVA SÁNCHEZ (2002) afirma que o sentimento de insegurança da sociedade de risco causou a institucionalização de tal sentimento, estando à vida social contaminada por uma grande incerteza: "estão nos 'matando', mas não conseguimos ainda saber com certeza nem quem, nem como, nem a que ritmo" (SILVA SÁNCHEZ, 2002, p. 34).

O aumento da complexidade das relações sociais, a perda da credibilidade nas ciências, a intensificação dos aparatos tecnológicos e o medo quantos aos riscos, em conjunto com a revolução

dos meios de comunicação, culminou no agravamento da crise social de insegurança, fortalecendo o anseio social por uma resposta estatal para tal demanda popular (SILVA SÁNCHEZ, 2002, p. 40-52). O Estado passou a utilizar o direito penal como forma de atender o clamor social (CABRERA, 2017).

O intenso clamor proveniente da opinião pública, que invoca o direito penal motivado pelo sentimento de insegurança, tem sido uma séria dificuldade do direito penal contemporâneo, sendo utilizado em períodos eleitorais por candidatos que prometem um aumento da quantidade e uma maior severidade das penas para aqueles que cometerem determinados crimes, caracterizando assim o intitulado "populismo penal", sendo este um dos principais produtos da "virada punitiva", deixando claro que a questão do "superencarceramento" é um fato político, bem como todo o processo de transformação dos parâmetros da justiça criminal, expondo como a sensação de insegurança é bastante explorada pelo discurso político-eleitoral (PAIVA, 2014, p. 51).

É percebido assim uma relação bem definida no contexto social atual: a globalização e pós-industrialização resultou na sociedade de riscos que, por sua vez, produziu uma grande quantidade de normas incriminadoras (CABRERA, 2017).

Prevalece na sociedade de risco um discurso no sentido de que a expansão do direito penal é imprescindível para reduzir a sensação de insegurança da população, mesmo que sacrifique os direitos e garantias individuais, de maneira que o direito penal deixe de ser a ultimaratio e se torna a prima ratio ou "única ratio" (BIANCHINI; GOMES, 2002, p. 18).

É em tal conjuntura que ocorre o encarceramento em massa.

3.3. DO GRANDE ENCARCERAMENTO

Tendo em vista o fato da prisão ter apelo político, uma vez que a adoção de uma punitividade populista satisfará considerável parcela da população, sendo esta vista apenas como um grande grupo de eleitores, comenta CARVALHO (2016):

> O objeto de consumo ofertado pelo legislador são incriminações severas, alimentando em seu público, através de forte apelo aos meios de comunicação, a sensação de que se está efetivamente buscando soluções ao problema da violência e da criminalidade (CARVALHO, 2016, p.183).

É nessa perspectiva, de possíveis legisladores ou titulares do Poder Executivo defendendo recrudescimento penal em detrimento das garantias constitucionais que o encarceramento em massa começa a se tornar realidade. É em tal contexto de virada punitiva que a prisão retomou seu protagonismo.

A narrativa midiática, a legislação penal se expandindo e as sentenças judiciais populistas, unidas contra um "inimigo", são elementos essenciais no grande encarceramento, todavia é importante destacar a guerra às drogas e a política de "lei e ordem", que foram objetos de diversos discursos eleitorais, que resultaram no recrudescimento de penas, no aumento da violência cometida por policiais e claro, no amplo aumento da população carcerária a partir dos anos 1990 (PAIVA, 2014, p. 103-109).

Sobre isso, KARAM (2012), destaca:

> Não obstante a notável expansão, pelo menos desde a década de 80 do passado século XX, do chamado direito penal econômico e a ampla criminalização de condutas voltadas contra criados bens jurídicos de natureza coletiva ou institucional, o interior das prisões no mundo inteiro não deixa nenhuma dúvida quanto a quem são os alvos primordiais do sistema penal. (KARAM, 2012, p. 55-56)

Os discursos acima citados nasceram nos Estados Unidos durante os anos 1970 e 1980, chegando ao Brasil nos anos da ditadura cívico-militar (1964-1985). Os efeitos dessa importação de política criminal antimoderna estão bem evidentes: em 1994 o Brasil tinha 110000 prisioneiros, em 2005 já eram 380000 (BATISTA, 2011). Hoje o Brasil tem a terceira maior população carcerária do mundo, de acordo com os dados do INFOPEN, sistema de informações estatísticas do DEPEN (Departamento Penitenciário Nacional), atrás somente de Estados Unidos e China, tendo tal quantidade ampliado devido às prisões decorrentes da lei de drogas (INSTITUTO HUMANISTAS UNISINOS, 2021). A população mais representativa entre os prisioneiros é a afro-brasileira, deixando bem explícito que é o alvo primordial da guerra às drogas e da expansão do direito penal.

O resultado disso são penitenciárias lotadas, decrépitas, tétricas, assemelhadas a masmorras ou prisões administradas pelas Forças Armadas dos Estados Unidos localizadas em um limbo jurídico como as prisões de *Abu Ghraib*, no Iraque, ou da base de *Guantánamo*, em Cuba (BATISTA, 2011).

Está claro, conforme o estado atual do cárcere após a virada punitiva, que cada vez mais o direito penal está distante de cumprir com seu – talvez utópico – objetivo de controle social, de intimidação via sanção penal, marchando de forma acelerada rumo ao direito penal autoritário, beligerante e ineficaz, transformando-se em uma mera alegoria, um simples símbolo.

Eis a necessidade de analisar a possibilidade de utilização de equipamento de monitoramento indireto do encarcerado via tornozeleira eletrônica, através do crivo das garantias constitucionais, com destaque ao princípio da dignidade humana, ao passo que "ninguém será submetido a tortura nem a tratamento desumano ou degradante" (BRASIL, 1988), conforme dita o art. 5º, III,

da nossa Constituição.

4. A REINTEGRAÇÃO E O MONITORAMENTO ELETRÔNICO DA PESSOA PRESA

Quem estuda o sistema prisional ou possui o mínimo de proximidade com a temática já deve ter lido ou ouvido as expressões ressocialização, reeducação, reinserção, reabilitação ou recuperação, apenas para citar algumas, em referência aos presos. Em sua tese de doutorado, BRAGA (2012, p. 29) critica as chamadas ideologias "res" pois, no seu entendimento, tais abordagens tratariam a pessoa presa como objeto de intervenção penal, por meio das quais caberia ao sistema moldar o modo de ser do apenado.

Como contraponto às ideologias "res", BRAGA (2012, p. 29-30) defende a reintegração do preso à sociedade. Para tanto, ela considera três pressupostos: (i) o preso somente se diferencia dos demais indivíduos da sociedade pelo fato de estar preso, devendo ser enxergado como uma pessoa "normal"; (ii) ao contrário do que ocorre daquilo que chama "as antigas ideologias 'res'", o preso não é objeto de intervenção penal, mas, sim, sujeito da Execução Penal, tendo a capacidade de manifestar tanto sua vontade quanto sua autonomia nas atividades desenvolvidas e (iii) a sociedade passa a ser também responsável pela reintegração da pessoa presa, devendo oportunizar o diálogo.

Nas palavras de BRAGA (2012):

> Um dos sentidos da reintegração social – que considero de suma importância – diz respeito à volta do egresso à sociedade, de forma a lhe possibilitar o exercício de seus direitos individuais, políticos e sociais. (BRAGA, 2012, p. 32)

A pesquisadora lembra que:

> A privação de liberdade não converge para a construção de um sujeito mais autônomo e integrado. Se não temos condições, no momento, de prescindir das prisões, também não podemos reforçar a falácia apresentada pelas ideologias e reeducação e ressocialização. (BRAGA, 2012, p. 33)

Nesse sentido, muitas vezes, a progressão de regime, prevista na Lei nº 7.210, de 1984, a Lei de Execução Penal, acaba sendo uma das únicas maneiras pelas quais o Estado ensaia reintegrar o preso à sociedade, ainda que de forma insuficiente e passível de críticas.

A Lei de Execução Penal prevê, em seu artigo 112, que a pena privativa de liberdade deve ser executada de forma progressiva com a transferência para regime menos gravoso, ou seja, do fechado para o semiaberto para o aberto. Com isso, espera-se que a pessoa presa seja reintegrada à sociedade de forma gradual e adequada[3].

Uma vez que o monitoramento eletrônico, seja por meio da pulseira ou da tornozeleira, permite controlar a localização da pessoa investigada, presa ou condenada, é permitida sua aplicação em duas hipóteses, segundo a Lei nº 12.258, de 2010, que alterou dispositivos da Lei de Execução Penal: quando o juiz autoriza a

3 Nesse ponto, vale dizer que a Súmula 491 do Superior Tribunal de Justiça determina que "é inadmissível a chamada progressão per saltum de regime prisional", baseada em interpretação do antigo artigo 112 da Lei de Execução Penal, segundo o qual o preso deve cumprir pelo menos um sexto da pena no regime original antes de poder passar para o próximo. No entanto, com a entrada em vigor da Lei nº 13.964, de 2019, a chamada Lei Anticrime [sic] não houve vedação expressa quanto à possibilidade da aplicação da progressão por salto, razão pela qual poderia a defesa alegar referida tese por restar configurado o constrangimento ilegal.

saída temporária no regime semiaberto (artigo 146-B, inciso II) ou quando determina a prisão domiciliar (artigo 146-B, inciso IV). É válido dizer, em tempo, que alguns dispositivos do diploma legal foram vetados – os que previam, por exemplo, monitoramento eletrônico na hipótese de livramento condicional ou de suspensão condicional da pena ou de pena restritiva de direitos – por contrariarem o ordenamento jurídico na medida em que maculam, dentre outros aspectos, as necessárias individualização e proporcionalidade da pena.

No ano seguinte, em 4 de maio de 2011, foi aprovada a Lei nº 12.403, que passou a prever a possibilidade de utilização do monitoramento eletrônico como medida cautelar diversa da prisão (artigo 319, inciso IX, do Código de Processo Penal).

Por fim, com a edição da Súmula Vinculante nº 56[4], o Supremo Tribunal Federal, considerando a insuficiência de vagas, acatou a possibilidade de cumprimento de prisão domiciliar com uso da tornozeleira eletrônica tanto para pessoas que progrediram para o regime semiaberto quanto para aquelas que iniciavam o cumprimento nesse regime.

BOTTINI (2008) lembra que esse tipo de equipamento:

> reduz a autonomia do indivíduo, afetando seu direito fundamental à intimidade e à privacidade (art. 5º, X, da CF), motivo pelo qual sua aplicação deve sempre ocorrer apenas em casos, de fato, necessários. Ainda, embora o equipamento possa ser utilizado como pena ou como medida assecuratória, sua natureza penal será sempre a de "restrição de direitos" (BOTTINI, 2008, p.170).

4 Determina a Súmula Vinculante nº 56 que "A falta de estabelecimento penal adequado não autoriza a manutenção do condenado em regime prisional mais gravoso, devendo-se observar, nessa hipótese, os parâmetros fixados no RE 641.320/RS.

Em sua tese de doutorado, JUNIOR (2012), por seu turno, elenca os limites que devem ser observados relativamente a essa espécie de monitoração:

> Tratando-se de restrição de direitos fundamentais, o monitoramento eletrônico de penas e alternativas penais deve observar os seguintes limites e garantias: respeito ao princípio da legalidade, vigilância das obrigações e restrições impostas e não de imagens e sensações da pessoa, sigilo das informações coletadas, informações prévias, detalhadas e claras ao monitorado, aplicação e controle através de decisão judicial, menor visibilidade possível do equipamento e acesso independente de condição econômica. (JUNIOR, 2012, p. 271)

Já LANCELLOTTI (2018, p. 166), ao realizar pesquisa etnográfica juntamente aos usuários de tornozeleiras eletrônicas, aponta que a gestão desses equipamentos está "envolta com paradoxos", elencando dois deles. De acordo com a pesquisadora, o primeiro paradoxo consiste "na ideia de reinserção que a tornozeleira eletrônica permite", uma vez que:

> Ao mesmo tempo em que é possível cumprir a pena dentro de um âmbito doméstico e também se reinserir no mundo do trabalho, algumas atividades que não conseguem ser mapeadas pela tornozeleira podem gerar um castigo. (LANCELLOTTI, 2018, p. 166)

Em seguida, aponta que o segundo paradoxo é que:

> Apesar da confiança que os profissionais da segurança têm no aparelho, ele pode ser burlado, pode apresentar defeitos e o cumprimento das suas regras não significa uma reinserção por um caminho que não seja considerado um delito. (LANCELLOTTI, 2018, p. 166)

Por tais razões, para LANCELLOTI (2018), a tornozeleira eletrônica deve ser considerada como um "objeto fluido" (LANCELLOTTI, 2018, p. 167), mudando, assim, a percepção geral sobre o instrumento.

4.1. A PANDEMIA DO NOVO CORONAVÍRUS E O SISTEMA PRISIONAL

Em meados de março de 2020, o Brasil entrava naquela que seria sua maior crise sanitária: a pandemia causada pelo novo coronavírus, ou Sars-CoV-2, causador da Covid-19. Até a data de fechamento do presente artigo, morreram no Brasil mais de 573 mil pessoas em decorrência de complicações causadas pelo vírus.
É conhecido pela sociedade como um todo – e não só pela comunidade jurídica – que o ambiente das unidades prisionais é extremamente insalubre também em virtude da superlotação carcerária.

Tanto é verdade que, em 2015, o próprio Supremo Tribunal Federal reconheceu a existência de um "Estado de Coisas Inconstitucional"[5] no julgamento da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 347. Em seu voto, o ministro Marco Aurélio escreveu que:

> SISTEMA PENITENCIÁRIO NACIONAL – SUPERLOTAÇÃO CARCERÁRIA – CONDIÇÕES DESUMANAS DE CUSTÓDIA – VIOLAÇÃO MASSIVA DE DIREITOS FUNDAMENTAIS – FALHAS ESTRUTURAIS – ESTADO DE COISAS INCONSTITUCIONAL – CONFIGURAÇÃO. Presente quadro de violação massiva e persistente de direitos fundamentais, decorrente de falhas estruturais e falência de políticas públicas e cuja modificação depende de medidas abrangentes de natureza normativa, administrativa e orçamentária, deve o sistema penitenciário nacional ser caracterizado como 'estado de coisas inconstitucional (BRASIL, 2021).

O conceito de "Estado de Coisas Inconstitucional" foi emprestado da Corte Constitucional da Colômbia, segundo a qual, para que reste caracterizado, é necessário que (i) haja uma situação de violação generalizada de direitos fundamentais; (ii) exista inércia ou incapacidade reiterada e persistente das autoridades públicas

5 A definição foi emprestada da Corte Constitucional da Alemanha.

em modificar a situação e (iii) para que haja superação das transgressões, é necessária atuação conjunta de uma pluralidade de autoridades. (BRASIL, 2021).

Ora, é indiscutível que o sistema penitenciário brasileiro padece dos três pontos supramencionados. No entanto, vale também dizer que o reconhecimento desse estado de coisas inconstitucional muito pouco ou quase nada mudou relativamente às mazelas do sistema prisional.

Ciente disso e frente ao cenário desolador que se desenhava em virtude da pandemia da Covid-19, o Conselho Nacional de Justiça editou a Recomendação nº 62, de 17 de março de 2020 (BRASIL, 2021), por meio da qual pretendeu incentivar que tribunais e magistrados adotassem medidas objetivando amenizar a incidência do novo coronavírus nos ambientes prisionais por meio da concessão de liberdade ou, ainda, pela substituição da prisão preventiva por domiciliar.

Quase um mês depois, o Conselho Nacional de Justiça publicou Orientação Técnica (BRASIL, 2020) tratando sobre a monitoração eletrônica de pessoas no contexto da Recomendação nº 62, o que de certa forma poderia, ainda que sacrificando outros direitos fundamentais, constituir uma possibilidade de diminuição da superpopulação prisional.

Nesse ponto, vale dizer que o Conselho Nacional de Justiça indicou, na referida Orientação Técnica, como necessária a análise, pela autoridade judicial, das condições individuais da pessoa monitorada, devendo ser asseguradas atividades relacionadas, por exemplo, à aquisição de medicamentos, ao cuidado com filhos, familiares ou dependentes e ao atendimento à saúde.

Também ressaltou o Conselho Nacional de Justiça que fossem adotadas outras medidas alternativas que não a monitoração eletrônica, como nos casos de pessoas idosas com deficiência, transtorno mental ou portadora de doença grave, pessoas em situação de rua ou com outra condição socioeconômica que inviabilizasse o funcionamento do equipamento ou, ainda, sendo gestante, lactante ou pessoa responsável por criança ou por pessoa com deficiência, dentre outras hipóteses.

Ainda, o Conselho Nacional de Justiça frisou, dentre outros aspectos, a importância da "progressiva substituição das tornozeleiras como medida cautelar" (BRASIL, 2020) por medida menos gravosa, sobretudo nos casos nos quais o monitoramento já tenha se desenrolado por período superior a 90 dias, além da não adoção do monitoramento eletrônico para o cumprimento de pena no regime aberto.

Já as Centrais de Monitoração foram orientadas a adotar medidas de higienização dos equipamentos de monitoração, bem como a tratar os incidentes de forma remota. (BRASIL, 2020)

Fato é que, apesar do Conselho Nacional de Justiça ter se manifestado pela concessão de liberdade e pela substituição da prisão preventiva por domiciliar nos casos em que o preso integra grupo de risco (pessoas idosas, gestantes e com comorbidades), em São Paulo, por exemplo, apenas 25% das pessoas que poderiam ter saído de trás das grades foram efetivamente postas em liberdade, segundo levantamento do Instituto de Defesa do Direito de Defesa (IDDD, 2021, p. 62).

Com a publicação do relatório "Justiça e Negacionismo: Como os Magistrados Fecharam os Olhos para a Pandemia nas Prisões" (IDDD, 2021), a entidade revelou os dados originados pelo mutirão carcerário organizado ao longo do ano de 2020 em parceria com

a Defensoria Pública do Estado de São Paulo visando efetivar a aplicação da Recomendação nº 62, do Conselho Nacional de Justiça (BRASIL, 2020).

Durante o tempo de duração do mutirão carcerário, foram realizados ao todo 448 pedidos de liberdade, tendo sido colocadas em liberdade 118 presos. Dito de outra forma, de cada quatro presos cuja Recomendação nº 62 poderia contemplar, três continuaram nas mesmas – péssimas, diga-se de passagem – condições pré-pandêmicas. É como se a pandemia nunca tivesse existido, a não ser pelo agravamento das condições desumanas às quais os presos foram submetidos.

Os pesquisadores CASTRO e MORI (2021), ao conduzirem estudo de caso que analisou a incidência da Recomendação nº 62 no âmbito do Tribunal de Justiça do Rio Grande do Sul, lembram que, no Brasil, "o enfrentamento da violência tem ocorrido no Brasil com a afronta aos valores mais comezinhos dos indivíduos" (CASTRO; MORI, 2021, p. 33).

Nas palavras dos pesquisadores, "poder-se-ia dizer, aliás, que o fundante direito à vida se encontra sob ameaça entre os muros, atrás das grades e dentro das celas das penitenciárias" (CASTRO; MORI, 2021, p. 33).

De acordo com CASTRO e MORI (2021):

> É como se a restrição de liberdade, seja como medida cautelar, seja como medida sancionatória, retirasse o status de ser humano e, logo, a titularidade de sujeito de direitos humanos. Nesse sentido, as falhas estruturais constitutivas, historicamente, do sistema prisional brasileiro vêm à tona no curso da crise sanitária da Sars-CoV-2 e revelam a nudez de homens e mulheres, despidos de sua dignidade, obstados de condições básicas de (sobre)vivência. (CASTRO e MORI, 2021, p. 33).

Para os pesquisadores, apesar de o monitoramento eletrônico possuir um viés que não pode ser desconsiderado, que consiste na possibilidade de ampliar o controle penal sobre o indivíduo – o que caracterizaria um fenômeno de dilatação do sistema penal brasileiro –, também não se pode negar suas potencialidades em tempos de pandemia, sobretudo para evitar violações ainda maiores dos Direitos Humanos além das já usuais e típicas do cárcere.

Portanto, CASTRO e MORI (2021) argumentam que:

> A tornozeleira eletrônica exibe-se como mecanismo direcionado a reduzir os índices de enclausuramento, não obstante mantenha ou acresça a vigilância sobre os seres humanos. No atual cenário, aliás, a aludida ferramenta evidencia-se como relevante, de um lado, à continuação do controle securitário e, de outro lado, à viabilidade do controle sanitário. (CASTRO e MORI, 2021, p. 34).

Das 120 decisões no âmbito do Tribunal de Justiça do Rio Grande do Sul analisadas pelos pesquisadores, 17 foram favoráveis e 80 foram desfavoráveis ao acusado ou condenado, não tendo o monitoramento eletrônico recebido grandes menções.

Por outro lado, no período de outubro de 2019 a julho de 2020, houve um aumento de 20,4% no quantitativo total de pessoas monitoradas.

5. CONSIDERAÇÕES FINAIS

O presente artigo buscou inicialmente delinear, ainda que brevemente, as origens da pena privativa de liberdade e de seu cumprimento no cárcere, expondo o desenvolvimento da instituição penitenciária conforme as mudanças socioeconômicas e políticas, além do grande crescimento das prisões e da quantidade de internos a partir da segunda metade do século XX.

Diante do que foi apresentado neste artigo, é perceptível a relação entre o advento do atual contexto civilizatório (sociedade de risco) e o populismo penal, que está consistindo em um excessivo alargamento dos limites para a atividade punitiva, contribuindo para a desestruturação dos princípios e garantias do direito penal, tendo como consequência o encarceramento em massa.

O grande encarceramento, este sendo produto da virada punitiva, e indiretamente da sociedade de risco, é insustentável em um Estado dito democrático. É imprescindível que o legislador não atenda o clamor popular e não trate mais o direito penal como uma solução para os problemas sociais, visto que está evidente o quão ineficaz é contra a criminalidade, ou seja, o direito penal se torna meramente um instrumento simbólico e nocivo.

Todavia, é importante tratar da situação mais explícita, que consiste no Brasil tendo a 3ª maior população carcerária do mundo, com pessoas empilhadas dentro de estabelecimentos degradados, insalubres e violentos, em completa desconformidade com a Constituição de 1988 e legislações internacionais no que se refere aos Direitos Humanos.

Um início de solução para as prisões superlotadas seria por meio do avanço tecnológico na área da execução penal, que é a vigilância remota dos condenados, via monitoramento eletrônico por

pulseiras ou tornozeleiras. Como ficou demonstrado no presente artigo, tal tecnologia não é unânime entre acadêmicos e juristas, pois reduz a já afetada liberdade do condenado, além de atingir o seu direito à intimidade e à privacidade, bem como não ser um aparelho à prova de defeitos.

Se já haviam muitos motivos para desinternar condenados devido à superlotação e os vários direitos fundamentais violados na penitenciária, em 2020 tivemos o começo da pandemia de coronavírus, sendo um dos fatores de contaminação pelo vírus Sars--Cov-2 a aglomeração, uma vez que esse vírus se propaga pelo ar, afetando o sistema respiratório, ou seja, há mais um forte motivo para reduzir o encarceramento.

O Conselho Nacional de Justiça emitiu orientação para que os magistrados buscassem tomar medidas para mitigar os danos que a pandemia causaria nos estabelecimentos prisionais, podendo substituir a pena sendo cumprida na penitenciária por prisão domiciliar, utilizando, por exemplo, monitoramento eletrônico.

No entanto, tais recomendações não foram consideradas pelos magistrados, visto que a maior parte dos pedidos de inserção em regime alternativo ao internamento em estabelecimento prisional foram negados, mantendo os encarcerados em condições piores do que as anteriores, visto que agora há um vírus letal circulando livremente, podendo contaminar todos os aprisionados, aglomerados em celas apertadas e com péssimas condições sanitárias.

Entretanto, houve magistrados que seguiram as recomendações do CNJ e inseriram condenados em monitoração eletrônica, uma vez que houve aumento percentual na quantidade de monitorados de 2019 para 2020.

Enfim, o monitoramento eletrônico de presos tem condições de amenizar o sistema carcerário brasileiro, o que já é referendado pelo CNJ, ainda mais quando se trata de uma crise sanitária mundial, não esquecendo que as penitenciárias brasileiras estão em uma crise humanitária há décadas.

Conforme visto no decorrer do artigo, os encarcerados têm direito ao tratamento digno e nossa Constituição tem de ser respeitada, senão tal país não merece ser considerado um Estado Democrático de Direito.

REFERÊNCIAS BIBLIOGRÁFICAS

BATISTA, Vera Malaguti. **Introdução crítica à criminologia brasileira**. 2ª ed. Rio de Janeiro; Revan, 2011.

BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade**. Trad. Sebastião Nascimento. 2. ed. São Paulo: Editora 34, 2011.

BIANCHINI, Alice, GOMES, Luiz Flávio. O direito penal na era da globalização. São Paulo: Revista dos Tribunais, 2002.

BITENCOURT, Cezar Roberto. **Falência da pena de prisão: causas e alternativas**. 2 ed. São Paulo: Saraiva, 2001.

BLOWER, Ana Paula; PAINS, Clarissa. **INCIDÊNCIA de tuberculose em presos é 30 vezes maior do que na população geral**. 2018. Disponível em: https://oglobo.globo.com/saude/incidencia-de-tuberculose-em-presos-30-vezes-maior-do-que-na-populacao-geral-22540362. Acesso em: 21 nov. 2021.

BOTTINI, Pierpaolo Cruz. **Aspectos pragmáticos e dogmáticos do monitoramento eletrônico**. In: JAPIASSÚ, Carlos Eduardo Adriano (Org.). Monitoramento eletrônico: uma alternativa à prisão? Brasília: Conselho Nacional de Política Criminal e Penitenciária, 2008.

BOTTINI, Pierpaolo Cruz. **Crimes de perigo abstrato e princípio da precaução na sociedade de risco**. São Paulo: Editora Revista dos Tribunais, 2007.

BOTTINI, Pierpaolo Cruz. **O paradoxo do risco e a política criminal contemporânea**. In: MENDES, Gilmar Ferreira; BOTTINI, Pierpaolo Cruz; PACELLI, Eugênio (Org.) Direito penal contemporâneo, São Paulo: Saraiva Jur, 2011.
BRAGA, Ana Gabriela Mendes. **Reintegração social: discursos e práticas nas prisões**. 371 f. Tese [Doutorado em Direito]. - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

BRASIL. Conselho Nacional de Justiça. **Recomendação nº 62 de 17 mar. 2020**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3246, Acesso em 25 ago. 2021.

BRASIL. Conselho Nacional de Justiça. **Registros de Contágios e Óbitos**. Disponível em: https://www.cnj.jus.br/sistema-carcerario/covid-19/registros-de-contagios-obitos/ Acesso em 25 ago. 2021.

BRASIL. Conselho Nacional de Justiça. **Orientações técnicas sobre a monitoração eletrônica de pessoas no âmbito da adoção de medidas preventivas à propagação da infecção pelo novo coronavírus (covid-19)**. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2020/04/Monitorac%CC%A7a%CC%83o-Eletro%CC%82nica-CNJ.pdf Acesso em 25 ago. 2021.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

SINAN. **Sistema de informação de agravos de notificação**. Disponível em: https://portalsinan.saude.gov.br/ Acesso em 25 ago. 2021.

BRASIL. Supremo Tribunal Federal (STF). **ADPF nº 347**. Rel. Min. Marco Aurélio Mello, j. 9 set. 2015.

CABRERA, Michelle Gironda. A sociologia do risco como suporte político criminal dos delitos culposos e seu impacto no direito penal contemporâneo. In: BACH, Marion; GUARAGNI, Fábio André (coord.); SOBRINHO, Fernando Martins Maria. **Direito penal econômico: administrativização do direito penal, criminal compliance e outros temas contemporâneos**. Londrina: Thoth, 2017.

CARVALHO, Salo de. **A política criminal das drogas no Brasil: estudo criminológico e dogmático da Lei 11.343/06**. 8ª ed. rev. e atual. São Paulo: Saraiva, 2016.

CASTRO, André Giovane de, MORI, Emanuelle Dallabrida. **Pandemia de covid-19 e monitoramento eletrônico: um estudo de caso sobre a atuação do Tribunal de Justiça do Rio Grande do Sul**. Revista de direito penal, processo penal e constituição. Florianópolis, v. 7, n. 1, p. 17-38, jan/jun. 2021. Disponível em: https://www.indexlaw.org/index.php/direitopenal/article/view/7595/pdf Acesso em 25ago. 2021.

CÍCERO, José, OLIVEIRA, Rafael, RIBEIRO, Raphaela, SCOFIELD, Laura. **Levantamento inédito revela que pelo menos 877 unidades prisionais registraram infecções no país**. Agência Pública. 10 mai. 2021. Disponível em: https://apublica.org/2021/05/covid-19-atingiu-mais-de-80-das-prisoes-em-14-estados/ Acesso em 25 ago. 2021.

CONECTAS. **Brasil se mantém como 3º país com maior população carcerária do mundo**. 2020. Disponível em: https://www.conectas.org/noticias/brasil-se-mantem-como-3o-pais-com-a-maior-populacao-carceraria-do-mundo/. Acesso em: 25 ago. 2021.

COVID nas prisões. Disponível em: https://www.covidnasprisoes.com/ Acesso em 25 ago. 2021.

FOUCAULT, Michel. **Vigiar e punir: o nascimento da prisão**. 42ª ed. Trad. de Raquel Ramalhete. Petrópolis: Vozes, 2014.

FUNDAÇÃO OSWALDO CRUZ. **Boletim extraordinário do Observatório Covid-19 aponta maior colapso sanitário e hospitalar da história do Brasil**. Rio de Janeiro, 16 mar. 2021. Disponível em: https://portal.fiocruz.br/documento/boletim-extraordinario-do-observatorio-covid-19-aponta-maior-colapso-sanitario-e Acesso em 25 ago. 2021.

GUARAGNI, Fábio André. **Responsabilidade penal do ente coletivo: pilastras político-criminais derivadas das noções de sociedade de risco e alteridade**. In: CHOUKR, Fauzi Hassan; LOUREIRO, Maria Fernanda; VERVAELE, John (org.). Aspectos contemporâneos da responsabilidade penal da pessoa jurídica. v. 2. São Paulo: Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo, 2014.

INSTITUTO HUMANITAS UNISINOS. **Brasil se mantém como 3º país com maior população carcerária do mundo**. Disponível em: http://www.ihu.unisinos.br/78-noticias/596466-brasil-se-mantem-como-3-pais-com-maior-populacao-carceraria-do-mundo. Acesso em 25. ago. 2021.

JUNIOR, Alceu Corrêa. **Monitoramento eletrônico das penas e alternativas penais**. 285f. Tese [Doutorado em Direito]. - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

IDDD. **JUSTIÇA e negacionismo: como os magistrados fecharam os olhos para a pandemia nas prisões**. São Paulo: IDDD, 2021. Disponível em: https://iddd.org.br/wp-content/uploads/2021/08/iddd-relatorio-negacionismo-final-2.pdf Acesso em 25 ago. 2021.

KARAM, Maria Lucia. **"Guerra às drogas" e criminalização da pobreza**. In: BOZZA, Fábio da Silva; ZILIO, Jacson Luiz. Estudos críticos sobre o sistema penal: homenagem ao Professor Doutor Juarez Cirino dos Santos por seu 70º aniversário. Curitiba: LedZe Editora, 2012.

LANCELLOTTI, Helena Patini. **Tecnologias de governo, vigilância e transgressão: um estudo etnográfico sobre as tornozeleiras eletrônicas**. Mediações: Revista de Ciências Sociais, Londrina, v. 23, n. 1, p. 141-169, abr. 2018. Quadrimestral. Disponível em: https://www.uel.br/revistas/uel/index.php/mediacoes/article/view/32346. Acesso em: 21 nov. 2021.

MELOSSI, Dario, PAVARINI, Massimo. **Cárcere e Fábrica: As origens do sistema penitenciário (século XVI-XIX)**. Trad. de Sérgio Lamarão. Rio de Janeiro: Revan, 2010.

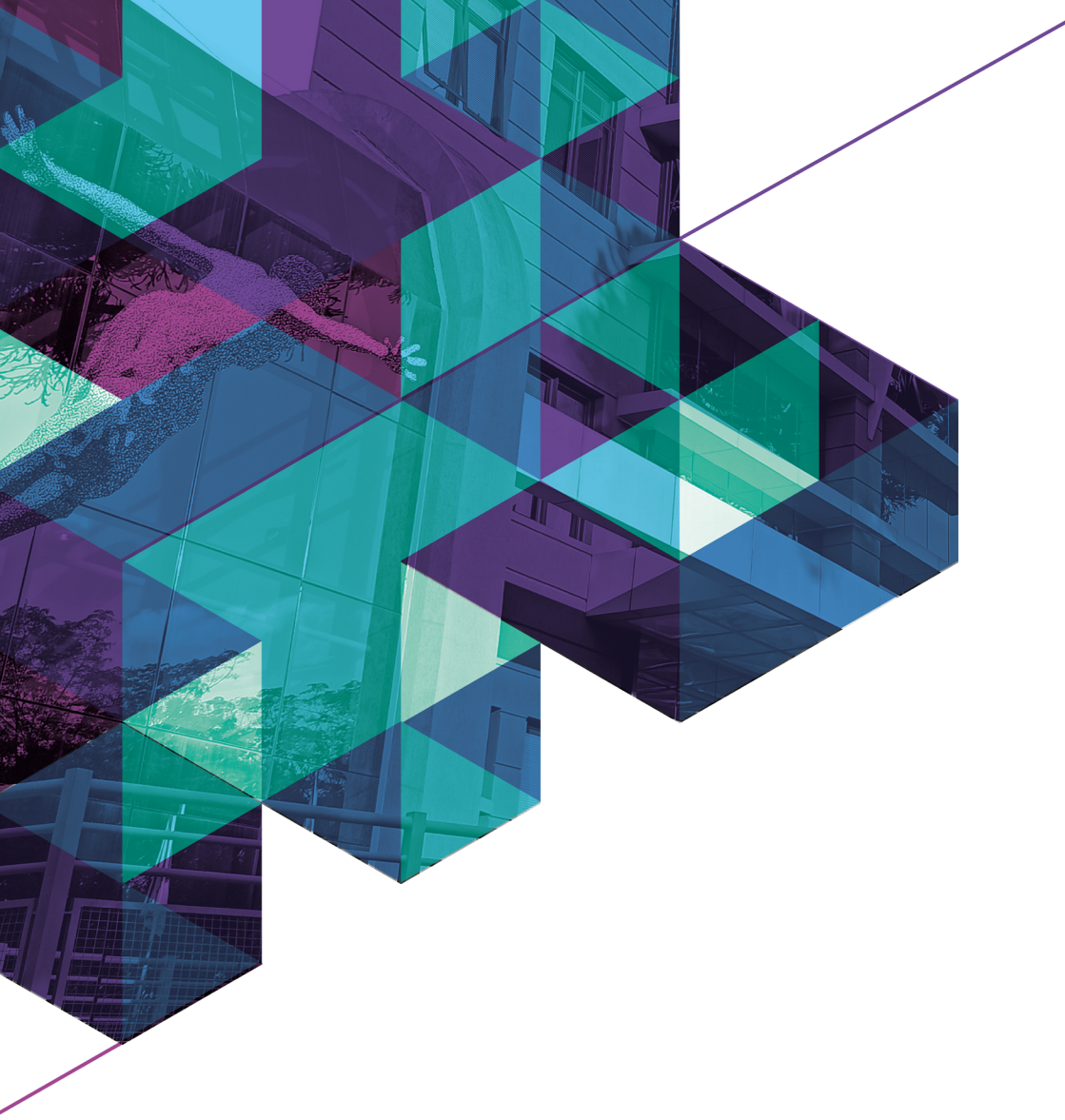
PAIVA, Luiz Guilherme Mendes de. **Populismo penal no Brasil: do modernismo ao antimodernismo penal, 1984 – 1990**. 178 f. Tese [Doutorado em Direito]. – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

SCRIBONI, Marília Silva. **Monitoramento eletrônico: Tornozeleira e pulseira eletrônica dividem opiniões**. Consultor Jurídico. 1 ago. 2010. Disponível em: https://www.conjur.com.br/2010-ago-01/monitoramento-eletronico-mal-saiu-papel-divide-opinoes Acesso em 25 ago. 2021.

SILVA, Camila Rodrigues, GRANDIN, Felipe, CAESAR, Gabriela, REIS, Thiago. **POPULAÇÃO carcerária diminui, mas Brasil ainda registra superlotação nos presídios em meio à pandemia**. G1. 15 mai. 2021. 2021. Disponível em: https://g1.globo.com/monitor-da-violencia/noticia/2021/05/17/populacao-carceraria-diminui-mas-brasil-ainda-registra-superlotacao-nos-presidios-em-meio-a-pandemia.ghtml Acesso em 25 ago. 2021.

SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais**. Tradução Luiz Otávio de Oliveira Rocha. São Paulo: Editora Revista dos Tribunais, 2002.

SINAN. **Sistema de informação de agravos de notificação**. Disponível em: https://portalsinan.saude.gov.br/ Acesso em 25 ago. 2021.



OAB 90 ANOS PARANÁ

OAB PARANÁ

COMISSÃO DE INOVAÇÃO E GESTÃO

COMISSÃO DE DIREITO DIGITAL E PROTEÇÃO DE DADOS

COMISSÃO DE GESTÃO E EMPREENDEDORISMO

ESA ESCOLA SUPERIOR DE ADVOCACIA