XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO II

CAIO AUGUSTO SOUZA LARA

RICARDO STANZIOLA VIEIRA

JOANA STELZER

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

D597

Direito, globalização e responsabilidade nas relações de consumo II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Caio Augusto Souza Lara; Joana Stelzer; Ricardo Stanziola Vieira.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-628-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Globalização e responsabilidade nas relações de consumo. XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO II

Apresentação

Superadas as emoções da Copa do Mundo de Futebol (2022), justamente após a derrota da seleção brasileira para a Croácia, era momento para se reunir e discutir as excelentes pesquisas desenvolvidas no GT 'Direito, Globalização E Responsabilidade Nas Relações De Consumo II', que ocorreu em Balneário Camboriú (SC), no período de 7 a 9 de dezembro de 2022, na Universidade do Vale do Itajaí (UNIVALI). E, de fato, brilhantes investigações envolveram os congressistas em contínuas discussões sobre as relações consumeristas e demonstraram (mais suma vez), a qualidade do evento.

De plano, foi apresentado o trabalho denominado 'O Fenômeno do Greenwashing no Mercado de Consumo', na qual se descreveu a utilização indevida da lavagem verde para a venda de produtos e serviços. Concluiu-se que, na realidade, o mercado oferece ao consumidor um produto aparentemente sustentável, pretendendo fidelizar suas escolhas, mas, que muitas vezes não 'entrega' o que promete ao consumidor.

Após, houve a discussão do artigo 'Globalização, responsabilidade de consumo e cultura de honestidade: um comparativo da quantidade de execuções cíveis e morosidade no Brasil e Inglaterra considerando o Índice de Percepção de Corrupção de 2021', no qual as autoras evidenciaram a relação existente entre cultura de honestidade e a relação do índice com a execução cível nos países. No caso do Brasil, ocupa-se o 96º lugar no índice e há 3.715.669 de execuções que demoram 5 anos e 1 mês para serem julgados. A Inglaterra, por sua vez, está em 11º lugar no ranking e julga em média 1.442.000 casos em 1 ano e 2 meses.

Em 'Sociedade de consumo e superendividamento: a eventual necessidade de políticas públicas para prevenção e tratamento do superendividamento e preservação do mínimo existencial do consumidor' foi possível verificar a relação existente entre as políticas públicas e o superendividamento. Para os autores, em que pese existirem normas para evitar as práticas abusivas, o fato é que se percebem práticas reiteradas nesse sentido. Assim, evidenciou-se a necessidade do Estado atuar para evitar os excessos, ao invés de jogar para o sistema financeiro a problemática.

Na pesquisa ‘O direito de dano e a proteção de dados pessoais em perspectiva comparada’ foram apresentadas as legislações de EUA e China, em que a primeira superpotência tecnológica dá ainda pequenos passos em prol da proteção, enquanto a segunda potência, há anos se movimenta em legislação considerada avançada. De qualquer forma, apela-se à disseminação da cultura de proteção de dados para que se torne possível um mínimo equilíbrio na balança dessa economia global fundada em dados.

Em ‘O Greenwashing diante do Direito: uma análise conceitual e casuística’ os autores defenderam que é preciso positivar expressamente o Greenwashing, conceituando-o e caracterizando-o para além das relações de consumo, a fim de que se alcance, verdadeiramente, sua ampla reparação, bem como sua coibição, inclusive, no âmbito social da produção simbólica. Nesse sentido, foi citado o exemplo do bioplástico que, apesar de não possuir uma definição, viabiliza supostas ‘sacolinhas plásticas sustentáveis’. Uma pesquisa que faz alerta importante.

Na pesquisa ‘O Princípio da Precaução e o tratamento jurídico dos riscos ambientais nas relações de consumo’ as autoras entendem como coerente a aplicação do Princípio da Precaução contra riscos ambientais nas relações de consumo, especialmente em lógica distinta da lógica do Direito-Dever que, normalmente, anima os operadores do Direito. Com isso, foi possível realizar um enquadramento no atual contexto constitucional e uma melhor compreensão sobre o Princípio da Precaução e o tratamento jurídico dos riscos, em uma análise convergente entre as relações de consumo e a proteção ambiental.

Na investigação sobre ‘Privacidade dos dados pessoais sensíveis na área da saúde através da lei geral de proteção de dados e do compliance’ a pesquisa discorreu sobre os dados pessoais considerados sensíveis pela Lei Geral de Proteção de Dados; e, o Compliance, como instrumento empresarial para garantir a proteção à privacidade e cumprimento da norma legal por empresas que atuam na área da saúde. Assim, os autores se empenharam em analisar o instituto do Compliance como estrutura administrativa de gestão, que possui como objetivo as medidas de prevenção, a fim de evitar atos de desvio de condutas no âmbito empresarial.

No artigo ‘Teoria da “Maçã Mordida” - uma leitura sobre a venda casada como influência no comportamento do consumidor’ foi trazido à baila as diferenciações e classificações comportamentais do consumidor, o conceito de relação de consumo, a contextualização da venda casada, além da pesquisa empírica das jurisprudências regionais sobre o tema em comento, tudo com o escopo de adentrar as correntes ainda conflitantes. Perguntavam-se os

pesquisadores: o consumidor compraria uma “maça mordida”, com perda substancial do seu conteúdo? Ou ele busca uma compra que o vincule ao produto [marca] independente se o complemento/acessório lhe está apartado?.

Em relação à temática dita ‘Tratamento ao consumidor superendividado para a preservação do mínimo existencial: diálogo entre a lei 14.181/2021 e a lei de falências’ investigaram-se os impactos causados pelo superendividamento, enquanto fenômeno global, no homo economicus e os instrumentos para a preservação do mínimo existencial ante o cenário de sua instauração. Com isso, foi feita a análise de coincidência entre a Ciência do Direito e a defesa do consumidor, e, mais especificamente, entre a tutela do consumidor superendividado e a preservação do mínimo existencial. A questão do superendividamento mais uma vez aparece nesse GT como questão essencial a ser enfrentada.

Na pesquisa ‘O modelo de greve política em Walter Benjamin e o falso empoderamento do consumidor: um estudo sobre a violência institucionalizada nas relações de consumo’ os pesquisadores tinham como objetivo realizar a análise do consumo em e-commerce e do estudo das ferramentas da teologia política, em específico as ferramentas utilizadas no consumismo, para uma análise dos modelos de greve descritas por Walter Benjamin e os sistemas de avaliação de serviços e produtos no consumo digital. Concluiu-se que o sistema de avaliação dentro das próprias plataformas é um instrumento intimamente ligado à teologia política e que ocasiona uma fé no consumidor, mesmo com sua ineficácia.

Na discussão sobre ‘Due Diligence em Comércio Justo: adensamento da responsabilidade corporativa e os efeitos no consumo sustentável’ foi momento de avaliar a orientação dos pequenos produtores de Comércio Justo no que concerne à Due Diligence. Afinal, se há aumento da consciência na responsabilidade corporativa, o compromisso e a vontade dos consumidores de pagar por um consumo justo tende a aumentar. Sob tal escopo, defendeu-se que o Comércio Justo e a Due Diligence aumentam a consciência, o compromisso e a vontade dos consumidores de pagar por um consumo sustentável.

Na pesquisa sobre ‘Neocolonialismo climático: a métrica do carbono sob o olhar da justiça intergeracional’ os autores estudaram sobre a justiça ou não de atuais imposições transnacionais das métricas de carbono. Assim, procuraram identificar as características da norma de direito intergeracional climático que impõe sanções e prêmios conforme a economia de carbono de cada Estado membro, bem como a análise da justiça histórica intergeracional, uma vez que gerações futuras sofrerão o impacto das ações de gerações passadas (e, ao que indica, não se passará diferente com a questão dos créditos de carbono).

Deste modo, na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, com artigos rigorosamente selecionados, por meio de dupla avaliação cega por pares (double blind peer review). Assim, todos os artigos ora publicados guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

Caio Augusto Souza Lara

Joana Stelzer

Ricardo Stanziola Vieira

O DIREITO DE DANO E A PROTEÇÃO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA

THE RIGHT TO DAMAGE AND THE PROTECTION OF PERSONAL DATA IN COMPARATIVE PERSPECTIVE

Caitlin Mulholland
Andressa Guerra Felippe dos Santos
Carolina Peçanha de Souza

Resumo

A pesquisa tem como principal objetivo identificar parâmetros que vêm sendo aplicados pela doutrina pátria e pelos tribunais brasileiros e estrangeiros que poderão ser adotados para melhor direcionar a atividade jurisdicional e administrativa brasileira na formulação de critérios para determinar a obrigação de indenizar. A pesquisa se sustenta em três etapas. Na primeira, compreendeu-se como a evolução de tecnologias pode trazer impactos para a sociedade e de como as atuais práticas do Direito são modificadas por ela. Em um segundo momento, foram analisadas decisões dos principais tribunais brasileiros, tais como STJ, TJRJ e TJSP, - com recorte temporal de 2018 em diante - acerca dos parâmetros adotados pela jurisprudência brasileira na aplicação da Lei Geral de Produção de Dados e de leis correlatas, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965/2014) e a Lei do Cadastro Positivo (Lei 12.414/2011). A terceira etapa consiste na atualização das decisões dos tribunais brasileiros e na análise preliminar da legislação, doutrina e decisões das cortes estadunidenses (foco no Estado da Califórnia) e chinesas para identificar parâmetros utilizados nos países na determinação do tipo de dano causado pela infração de dados pessoais.

Palavras-chave: Responsabilidade civil, Danos, Proteção de dados pessoais, Lgpd, Pipl

Abstract/Resumen/Résumé

The main objective of the research is to identify parameters that have been applied by the national doctrine and by Brazilian and foreign courts that may be adopted to better direct Brazilian jurisdictional and administrative activity in the formulation of criteria to determine the obligation to repay. The research is based on three stages. In the first one, it was understood how the evolution of technologies can impact society and how current legal practices are modified by it. In a second moment, decisions of the leading Brazilian courts, such as STJ, TJRJ and TJSP, were analyzed - with a time frame from 2018 onwards - about the parameters adopted by Brazilian jurisprudence in the application of the General Data Production Law and related laws, such as the Consumer Protection Code, the Civil Rights Framework for the Internet (Law 12,965/2014) and the Positive Registry Law (Law 12,414 /2011). The third step consists of updating the decisions of the Brazilian courts and the

preliminary analysis of the legislation, doctrine and decisions of the US (focus on the State of California) and Chinese courts to identify parameters used in the countries to determine the type of damage caused by data infringement.

Keywords/Palabras-claves/Mots-clés: Civil liability, Damages, Data protection, Lgpd, Pipl

1. Introdução:

Um levantamento feito pelo CETIC.br em 2021 publicado no Painel TIC COVID-19 esclarece que cerca de 94% dos usuários da Internet fizeram uso de redes sociais naquele ano, demonstrando o exponencial crescimento da economia digital e uma sociedade moldada pela Informação, que armazenada em *bits* permite um tratamento de dados pessoais de forma quantitativa e qualitativa em escalas altíssimas sem precedentes no globo.

Neste contexto, quem tem dados tem poder, seja para interferir ocultamente nos desejos das pessoas ou até manipular decisões políticas dos Estados ameaçando diretamente a democracia, tão logo, o estudo sobre a regulação de dados, direito de dano e responsabilização civil dos agentes de tratamento que exploram e coletam dados tornou-se mandatório.

A entrada em vigor da Lei Geral de Proteção de Dados no Brasil que regula, fiscaliza e protege os dados da pessoa humana atingiu um judiciário em retrocesso com a interpretação de caracterização de danos morais, tal qual, em sua maioria, seria a qualificação do dano por violação empresariais dos dados pessoais o que pode resultar na mitigação da cultura de proteção de dados e a ideia errônea de despriorização dos investimentos em adequações e engajamento de colaboradores.

Considerando que Internet, como rede propulsora de conexão mundial, não se limita às fronteiras territoriais dos Estados, notou-se a necessidade de expansão da presente análise sobre parâmetros e perfil dos países detentores majoritários das *Big Techs* - Estados Unidos da América e China - tais como Alphabet (Google), Microsoft, Amazon, Alibaba, Tencent e Huawei que, como multinacionais, exercem suas atividades quase sem barreiras regionais e é vasta as suas influências nos países subdesenvolvidos.

Observada a evolução da conectividade, este artigo busca analisar as normas do Brasil, Estados Unidos e China sobre o Direito de Dano e a responsabilização dos agentes de tratamento pela violação de dados pessoais, que, muitas vezes, tratam com negligência e discriminação, dados pessoais de bilhões de indivíduos.

2. O Direito de Dano e Responsabilidade Civil no Brasil na Lei Geral de Proteção de Dados.

Diante da epidemia do olho eletrônico[1] vivenciada na contemporaneidade, os usuários tornam-se *hipervulneráveis*, as empresas estão cada vez mais especializadas em métodos de

[1] Conceito criado por Umberto Eco que trata sobre a postagem em massa feita pelas pessoas em relação a tudo que fazem no seu dia-a-dia.

conversão de dados em dinheiro. Esta monetização já introduz técnicas de inteligência artificial como *perfilização (profiling)*, onde algoritmos conseguem projetar cada indivíduo com seus gostos e preferências para direcionamento de produtos ou serviços compatíveis, todavia, todo esse poder concentrado em uma indústria também permite o enviesamento para manipulação do pensamento em massa, como o famoso caso *Cambridge Analytica*.

A captura de dados pessoais, ou seja, as projeções digitais da pessoa humana, tornou-se um instrumento de poder extremamente útil para o capitalismo, abrindo margem para manipulação a nível mundial.

Diversos países consolidaram em regulamentos as suas discussões sobre proteção dos dados, conceituando direitos aos titulares e instituindo deveres às empresas - em destaque às *Big Techs*, como referência nota-se a União Europeia com a *General Data Protection Regulation* (GDPR), que inspirou e acelerou a promulgação da Lei Geral de Proteção de Dados (nº 13.709/2019 - LGPD) do Brasil, pois havia um desejo claro de ingresso na OCDE - Organização para Cooperação e Desenvolvimento Econômico - intenção esta que não foi consolidada.

Após diversas modificações no texto do Projeto Lei, a LGPD, foi sancionada no dia 14/08/2018, com objetivo de esclarecer conceitos, fixar direitos e obrigações e definir mecanismos de prestação de contas e fiscalização. Não foi um nascimento de um vazio regulatório, pois diversas leis já regulavam o tratamento de dados pessoais de forma direta ou indireta, dentre estas: a Lei de Cadastro Positivo; o Marco Civil da Internet; o Código de Defesa do Consumidor; e a Lei de Acesso à Informação.

Inclusive, mesmo antes da inserção expressa do Direito à Proteção de Dados Pessoais no rol de direitos fundamentais da Constituição pela EC115/22, entendia-se que uma interpretação contemporânea do direito à privacidade já garantiria sua tutela, uma vez que a esfera negativa nascida sob a ótica de Warren e Brandeis como um *direito de ser deixado só* não é mais suficientemente satisfatório, pois há também uma perspectiva positiva enquanto controle dos próprios dados dados - autonomia informativa.

Há que se falar na relevância da legislação para fortalecimento dos institutos, destaque da gravidade do tema, criação da Autoridade Nacional de Proteção de Dados - ANPD - hoje autônoma e independente, disseminação da cultura de proteção de dados e centralização da definição política do que é lícito e ilícito para incentivo da conduta legal e repressão do ilícito.

Nessa seara, emerge o direito do titular por danos decorrentes da violação da Lei que busca a reparação de prejuízos e restabelecimento do *status quo ante*. Isto porque a LGPD estabelece os parâmetros e as regras para garantir que o tratamento de dados respeitará os

direitos fundamentais do titular e, em complemento, prescreve o regime de responsabilidade civil que será aplicado àqueles que sofram danos durante o tratamento de dados pessoais.

Contudo, restou omisso o texto legal quanto ao regime de responsabilidade, se objetiva - baseada no risco e independente de culpa, caracterizando-se pelo dano, nexo causal e ato ilícito - ou subjetiva - fundamentando-se na atitude culposa do agente, tal fato resultou em um riquíssimo debate doutrinário quanto à aplicabilidade pelos Tribunais.

Em razão da teoria do diálogo das fontes e a força gravitacional das normas consumeristas, impera a caracterização da responsabilidade objetiva pois a maioria esmagadora dos litígios levados ao judiciário decorrerem de uma relação de consumo (artigo 12 e 14 do Código de Defesa do Consumidor), como ver-se-á nos próximos dois subitens.

3. As correntes doutrinárias sobre Responsabilidade Civil dos agentes de tratamento.

O advento da LGPD criou duas figuras para distinção das suas obrigações enquanto tratam dados pessoais: o controlador e operador. Ambos os agentes de tratamento para legislação, contudo, o operador somente responde pelos danos causados por seu descumprimento da lei ou quando não seguir as orientações do controlador (artigo 42, §1º, I, LGPD). Hipótese expressa de configuração da solidariedade passiva.

A antijuridicidade capaz de acarretar a responsabilização não surge somente pela violação à norma, mas também pelo não fornecimento da segurança necessária e adequada, como parâmetro, espera-se dos agentes as medidas razoáveis enquanto atualização do estado da arte da respectiva tecnologia.

Outro pressuposto normativo que merece menção é o nexo de causalidade, Dantas Bisneto (2020), contudo, faz uma crítica à omissão da legislação relacionada aos critérios objetivos para a imputação do dano que, em consequência, gerará a adoção de presunções totalmente subjetivas pelo Poder Judiciário para saneamento desta lacuna.

O artigo 42 da LGPD que trata da responsabilização dos agentes entrou em vigor com um texto lamentavelmente silente em relação ao regime, o que chama atenção é que outrora o Projeto Lei que deu origem a legislação foi construído sob a perspectiva da responsabilidade objetiva. Frisa-se trecho do Deputado Orlando Silva analisando o PL 4.060/2012 em 2018:

> A atividade de tratamento de dados pessoais constitui atividade de risco, o que atrai a incidência da responsabilidade objetiva ao agente de tratamento, ou seja, aquela segundo a qual não há necessidade de perquirir a existência de culpa para obrigar o causador do dano a repará-lo.

Contudo, no decorrer do processo legislativo houve a deliberada remoção do regime, sem considerar a clareza sobre qual responsabilidade seria então aplicável, sendo certo que nas

relações de consumo, observada a teoria do diálogo entre as fontes, adotar-se-ia a responsabilidade objetiva.

Para a corrente da doutrina que entende pela responsabilização subjetiva, a remoção de todas as menções à objetividade é um dos fundamentos que demonstraria a opção do legislador em alterar o regime previsto anteriormente no PL e a orientação pelo regime de *accountability*, frisando que a prestação de contas e adoção das medidas legais de segurança demandam ausência de culpa, consequentemente, de responsabilidade.

Gisela Sampaio da Cruz e Rose Meireles (SAMPAIO DA CRUZ; MEIRELES, 2019) afirmam que não há sequer sentido na adoção da responsabilidade objetiva, uma vez que a Lei impõe diversos deveres e obrigações, logo, responsabilizá-los mesmo do cumprimento integral de todo rol determinado iriam contra a própria lógica da estrutura. Em harmonia, Dantas Bisneto (2020) reforça que o Código Civil estatui como regra a responsabilidade fundada na culpa, logo, o risco apenas caberia em regulamentos que expressamente o previssem.

Ademais, o artigo 43 da LGPD, das excludentes de responsabilidade, expõe em um dos seus incisos que não haverá responsabilidade quando não houver violação à legislação de proteção de dados, isto é, quando o agente tomar as medidas de segurança e governança necessárias.

Sob outra perspectiva, entende-se pela adoção da responsabilidade objetiva em razão do risco da atividade (artigo 927, parágrafo único, do Código Civil):

> (...) A atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental. Ademais, tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves, ao atingirem direitos difusos, o que, por si só, já justificaria a adoção da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo (MULHOLLAND, 2020).

Outra corrente doutrinária, composta, dentre outros, por Anderson Schreiber (SCHREIBER, 2020) e Bruno Bioni, Daniel Dias (BIONI; DIAS, 2020) inova na adoção de uma interpretação híbrida de responsabilidade, assim como ocorre no CDC - os fornecedores respondem objetivamente pelos danos causados e os profissionais liberais, mediante a presença de culpa. Explica-se do destrinchamento do artigo 44 da LGPD que define a responsabilização:

> (1) "*quando deixar de observar a legislação*" (caput);
> (2) "*quando não fornecer a segurança que o titular dele pode esperar*" (I, II e III);
> (3) quando os agentes de tratamento não adotarem as medidas de segurança previstas no art. 46 e seguintes da LGPD (parágrafo único).

No 1 e 3 nota-se a responsabilidade subjetiva, no 2, objetiva. Isto porque observou-se a conexão do trecho com o artigo 14 §1º, do CDC cujo objeto é o defeito do serviço, logo, a

segurança esperada é a de um titular de dados médio, como um padrão de conduta que legitimamente é esperada dos agentes.

Superado os três regimes mencionados, Maria Celina Bodin de Moraes (BODIN DE MORAES, 2019), baseando-se na interpretação do artigo 6º, X[2] da LGPD, caracteriza o sistema de responsabilização especialíssimo - *sui generis*, nomeando-o como proativo, já que o artigo, além de determinar o ressarcimento de danos, buscou prevenir e evitar a ocorrência desses danos.

Por fim, como último requisito: o dano, que será patrimonial, moral, individual ou coletivo. Das duas primeiras classificações, a caracterização da extrapatrimonialidade está gerando notada recusa jurisprudencial, que se verá com maior profundidade no item abaixo. Esta peculiaridade restou presente após entrada em vigor da legislação, pois, mesmo com vasta menção em brilhantes doutrinas há algumas décadas e forte tentativa de definições objetivos, o conceito não é restrito e uniforme, o que possibilita alterações de postura dos tribunais, mesmo que retrógradas.

4. As tendências da jurisprudência sobre o Direito de Dano e Responsabilidade Civil.

No período de outubro de 2021 a abril de 2022, estudamos o inteiro teor das sentenças ou acórdãos de 75 processos, nestes, em sua maioria, na competência do Tribunal de São Paulo. Cabe destacar a publicação do Painel da LGPD nos Tribunais[3] pelo CEDIS-IDP, IDP e Jusbrasil em que conseguiram mapear com muita qualidade as decisões em escala maior (274 decisões) e, para nossa felicidade, nossos levantamentos foram compatíveis com esse material.

Nesses primeiros anos de legislação chama atenção a ausência do seu protagonismo nas decisões, é constante a fundamentação a reboque de outras, isto porque as relações consumeristas são as maiores razões de lide que pôde-se notar. Não se viu o assentamento da discussão doutrinária sobre a natureza da responsabilidade civil, já que a esfera gravitacional do Código de Defesa do Consumidor em seus artigos 12 e 14 definem a objetividade de seu sistema.

Outra reflexão importante é manifestação ainda rasa da fundamentação judiciária nos temas que atingem dados pessoais, por isso, restringem-se aos fundamentos da lei (artigo 2º da

[2] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[3] PAINEL DA LGPD NOS TRIBUNAIS. Acesso em 10.08.2022. https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html

LGPD) e aos conceitos (artigo 5º da LGPD), o Painel da LGPD pelo IDP demonstra que a segunda maior incidência (28,6%) percebida pela pesquisa das decisões versam sobre o Capítulo I - Das disposições preliminares da LGPD[4].

A despeito dessas menções, há forte dificuldade de caracterização da vulnerabilidade do titular de dados diante da violação da lei pelas empresas - como nos casos de incidentes de segurança. Afunilando esta concepção, destaca-se as decisões que surgiram do pleito por direito à reparação por danos morais dos titulares que tiveram seus dados expostos no incidente de segurança ocorrido na empresa ENEL - concessionária de serviço público de energia elétrica - em São Paulo no ano de 2020, foram cerca de 290 mil clientes e o teor dos dados foram: nome, CPF, celular, data de nascimento, endereço completo, e-mail, índices de leitura e histórico de pagamentos.

Dentre diversos processos no Tribunal de São Paulo, inclusive com infundados pedidos de segredo de justiça pela empresa, alguns acolhidos, levantamos 16 casos. Em nenhum destes o titular mereceu tutela, mesmo caracterizada a responsabilidade objetiva pelo CDC, a interpretação restou pela ausência de caracterização de dano, mesmo com a juntada de *prints* de diversas tentativas de contato de terceiros com a informação da numeração dos índices de leitura de energia.

Este caso merece alerta pois podemos traçar duas características relevantes da postura dos juízes frente às tendências geradas pelas novas tecnologias: (I) a violação da proteção de dados não configura dano moral *in re ipsa*[5], devendo o titular [hipervulnerável] demonstrar prova robusta do dano; (II) demonstração de um entendimento *extra legis* que distingue dados pessoais cadastrais e definem que estes não merecem tutela pelo rotineiro uso.

É emblemática a referida distinção porque a legislação no seu rol de conceitos e no decorrer do seu texto identifica 5 tipos de classificações, quais são: os dados pessoais, dados pessoais sensíveis, dados anonimizados, dados pessoais manifestamente públicos e dados de acesso público. Ainda, define expressamente que apenas no caso de dados anonimizados a legislação não será aplicável.

Ora, vê-se no judiciário uma inovação fundada na ausência de dano quando a exposição de dados for limitada aos dados pessoais cadastrais e na interpretação restritiva de

---

[4] Ressalta-se que está abaixo apenas dos 35,7% dos casos que foram fundamentados no Capítulo II - Do Tratamento de Dados Pessoais. Acesso em 15/08/2022. https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html

[5] A despeito disso, o uso indevido da imagem gera dano moral in re ipsa, ou seja, dano do próprio registro de fato inexistente, bastando a constatação de ato ilícito para concretizar o direito à reparação. Entendimento já consolidado pelo Superior Tribunal de Justiça na Súmula 403.

dano apenas quando o dado "vazado" for de natureza sensível. Dada a característica atual de direito fundamental da proteção de dados pessoais, como já mencionado neste relatório, despertamos uma vulnerabilidade, pois das 16 decisões, 11 fizeram esta menção. Para elucidar o posicionamento, destaca-se o próprio trecho de um dos acórdãos:

> Analisando referidos dados, a maioria envolve qualificação do consumidor (nome, RG, CPF), que não é acobertado por mínimo sigilo e o conhecimento por terceiro em nada macularia qualquer direito da personalidade da parte autora. Os demais dados não são considerados sensíveis ou violadores de qualquer privacidade ou intimidade [telefones fixo e celular, endereço eletrônico, carga instalada no imóvel e consumo estimado, tipo de instalação, leitura e endereço residencial]. Referidos dados são costumeiramente fornecidos por todos, seja em estabelecimento comercial (físico ou virtual), portarias de acesso a imóveis, aplicativos e sites de compras, muitas vezes até com autorização para sua cessão posterior a terceiros. (Processo nº 1025226-41.2020.8.26.0405. o Des. João Camillo Costa)

Nos parece conceito próximo ao que a lei quis chamar de "dados pessoais manifestamente públicos", mas dada peculiaridade, preferimos optar pela autonomia deste conceito ainda não apresentado pela doutrina pátria ou discussões do tema. Remonta-se então ao alerta feito por Bruno Bioni e Daniel Dias (BIONI; DIAS, 2019) sobre uma construção dogmática falha que vincula a proteção de dados pessoais à dicotomia entre o público e o privado, já que os desembargadores fizeram uma ligação direta ao direito de dano pela violação de dados com o direito à privacidade no seu aspecto mais íntimo e não como um direito autônomo, como deve ser.

Por fim, faz-se necessário a criação de critérios objetivos e conectado à cultura de proteção de dados para caracterização do dano, olhando para Europa, nota-se o critério da gravidade da ofensa como importante parâmetro até para quantificação monetária da indenização que, dependendo da extensão, poderá ser reduzida.

5. A análise transfronteiriça sobre legislações de Proteção de Dados Pessoais e o Direito de Dano: um enfoque nos Estados Unidos da América e na República Popular da China.

A tecnologia, ao mesmo tempo que permite o surgimento de novas tendências, a conexão de pessoas, otimização de tempo e geração de novas oportunidades no mercado, também acarreta a manipulação dos indivíduos, restrição dos interesses e gostos, impulsão de formatos para criação de "bolhas" e variados mecanismos de vigilância.

Jaron Lanier (LANIER, 2018) lembra que o tratamento de dados pessoais pelas companhias, em especial as redes sociais, usam técnicas behavioristas - lógica perde e ganha, *like* e *dislike* - amplamente limitadoras da capacidade cognitiva humana, permitindo a analogia dessa relação com a de animal de estimação - cachorro - e seu dono. Os bits são utilizados

como iscas para armazenamento de informações em massa, que entrega, na maioria das vezes, gratuitamente, a "coleira" repleta de dados aos terceiros, estes passam a ter quase que um poder de deus - absoluto - pois entendem o perfil único e completo de cada indivíduo.

As grandes empresas, numa nova conjuntura do capitalismo global cada vez mais ligada à automação, inteligência artificial, robotização e sistemas de infraestrutura em nuvem, identificaram valor nos investimentos efusivos em produtos e serviços voltados à tecnologia da informação, especialmente em comunicações e dados digitais. Esses investimentos emergiram de modo a configurar as empresas detentoras da tecnologia como protagonistas na competição global pela posse de plataformas durante a transição e manutenção das atividades na quarta revolução industrial.

Entre as companhias pioneiras nessa moderna e automatizada arquitetura de mercado, sempre estiveram as empresas estadunidenses, lideradas pela Alphabet (Google), Meta (anteriormente reconhecida apenas como Facebook), Apple, Microsoft e Amazon. Empresas como IBM, Uber, Tesla, Intel, Twitter, Qualcomm, entre muitas outras, também não podem ser esquecidas. Tais companhias têm a maior capitalização de mercado, obtendo a maior porcentagem de seus lucros a partir dos seus direitos de propriedade intelectual (referentes aos seus softwares e suas invenções patenteadas, por exemplo). Além disso, seus fluxos de receita e suas importantes atividades, que são hoje rotineiras dos indivíduos em todo o planeta, lhes conferem um poder estruturante. Por outro lado, desde a abertura do comércio e a investimentos e implementação de reformas de livre mercado por volta do final dos anos 70/início dos anos 80, a China vem se tornando gradativamente uma das maiores potências mundiais, em especial porque o governo passou a adotar a inovação como prioridade. O país se tornou um grande fabricante, comerciante, parceiro comercial e ainda lar para uma população com alto poder de compra. Tudo isso fortaleceu a atuação de suas grandes empresas com o decorrer dos anos. Tencent, Alibaba, Baidu, Didi e ByteDance (TikTok) centralizam o poder tecnológico e as plataformas digitais que circundam as diferentes dinâmicas da população. Não deixando de fora outras grandes companhias chinesas de tecnologia, tais como Xiaomi, Huawei, Shein, Meiyuan, Weibo, ZTE, etc.

Esse poder das Big Techs supramencionadas se explica não somente pelo produto, pela inovação ou pela facilidade e caráter intuitivo dos formatos de suas plataformas, mas também pelo volume e valor da informação que milhares de usuários produzem ao utilizá-las. Essas empresas têm muito em comum, embora o que as unam mais fortemente em um só desafio seja a capacidade de armazenamento de dados pessoais de suas ferramentas e sistemas operacionais. Outro desafio, então, surge para as nações neste contexto: o de regular e legislar

com o objetivo de prever o dever de indenizar pelas violações aos indivíduos que confiam seus dados e informações pessoais na atividade das grandes companhias visando a facilitar e otimizar seus trabalhos, seu lazer e suas vidas em geral. Ambos os países trazidos no presente capítulo ainda experienciam grandes reestruturações jurídicas para manter no mercado plataformas que atuam de forma comprometida com a segurança de seus usuários.

Naturalmente, o rápido crescimento econômico da China nas últimas décadas acarretou o aumento dos laços comerciais com os Estados Unidos. Contudo, as divergências políticas, econômico-sociais e culturais fizeram com que houvesse uma certa obscuridade na manutenção da cooperação comercial entre os países. Resquícios dessa rivalidade influem no restante do mundo.

A exemplo dos dissensos entre as nações, em 2018, uma revista de notícias ligada ao Partido Comunista Chinês destacou os "Oito Guerreiros Guardiões"*:* Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle e Qualcomm em um relatório crítico que dizia que as empresas tinham conseguido entrar diretamente no mercado, enquanto, por outro lado, a Huawei e a ZTE foram mantidas de fora dos Estados Unidos. Diante disso, o Estado chinês aumentou o escopo das restrições tecnológicas e os requisitos de compartilhamento de tecnologia para regular mais incisivamente as transnacionais estrangeiras, especialmente as norte-americanas.

Mais recentemente, um sinal vermelho acendeu bem acima da Big Tech chinesa ByteDance, com relação ao seu principal produto, o aplicativo "TikTok", e sua vigência nos EUA. Uma reportagem do canal de informações Buzzfeed afirmou que alguns dados de usuários dos EUA estariam sendo acessados repetidamente da China. Em sequência, em uma carta aberta, um membro da Federal Communications Commission (FCC), órgão regulador da área de telecomunicações e radiodifusão dos EUA, solicitou ao Google e à Apple, empresas locais, que excluíssem imediatamente o aplicativo de suas respectivas lojas virtuais, sob pena de terem que se justificar perante a autoridade reguladora. O comissário afirmou que a ByteDance estaria "em dívida" com o governo chinês e que, por conta disso, seria exigida por lei a cumprir exigências de vigilância de Pequim. Desde 2019, o Comitê de Investimento Estrangeiro nos Estados Unidos está de olho no "TikTok" e atrás de implicações de segurança nacional através da coleta de dados pessoais dos cidadãos do país. Alguns políticos expõem publicamente seu medo do risco de espionagem por parte do partido comunista chinês, como era o caso do ex-presidente Donald Trump. Atualmente, parlamentares do Congresso americano continuam a requerer que o governo de Joe Biden tome medidas contra o "TikTok", citando as mesmas preocupações com segurança nacional e privacidade de dados.

Em resposta ao incidente noticiado, além de prometer oferecer aos pesquisadores e investigadores mais transparência sobre a atividade na plataforma, incluindo acesso de um grupo seleto à sua interface de programação de aplicativos, o "TikTok" anunciou a transferência dos dados de usuários estadunidenses para a plataforma de nuvem "Oracle", Big Tech local, com base em uma aparente maior segurança. Certo é que o clima de tensão e rivalidade entre os países, configurando uma nova guerra fria, só tende a crescer ao passo que suas empresas se tornam cada vez mais influentes no mercado. Com isso, se abre, por óbvio, um caminho árduo para regular, legislar e observar profundos impactos na economia global, que atinge em muito o Brasil e a América Latina, por exemplo.

Assim, observado a amplitude de atingimento, a presença das referidas instituições multinacionais difundidas pelo mundo e a possível influência normativa sobre dados das duas maiores superpotências do mundo, elaboramos breves reflexões sobre qual postura estão adotando, se é possível notar alguma cultura em proteção de dados e se há solidez na responsabilização por violação aos dados pessoais.

Cumpre, contudo, advertir que os próximos itens não possuem uma análise aprofundada do direito comparado, trabalho dos mais difíceis e interessantes, mas tão somente um levantamento atual sobre a possibilidade de reparação extrapatrimonial e regulação no âmbito da proteção de dados pessoais.

6. A descentralização das leis norte-americanas: a ausência de uma legislação geral e um destaque às influências do *California Consumer Privacy Act* (CCPA).

Das primeiras manifestações regulatórias sobre proteção de dados pessoais, tem-se os *Fair Information Practice Principles/FIPP* quando os Estados Unidos, pelo seu Departamento de Saúde, Educação e Bem-estar social, reconheceram os clássicos princípios do acesso, da qualidade, da finalidade, da transparência, do *accountability*, da segurança, entre outros. Desenvolvidos na década de 70, estes valores perpetuaram-se ao longo dos anos pela Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais até à consolidação regulamentar europeia, a *GDPR* de 2018, que atualmente é a maior referência internacional na matéria.

Os FIPP tornaram-se o *backbone* (espinha dorsal) das leis proteção de dados e privacidade, direito que alcançou status de fundamental em constituições de diferentes países, mas não na realidade norte-americana. Informações pessoais são constitucionalmente protegidas apenas contra ações de invasão à intimidade pelo governo, mesmo assim há um teste

de balanceamento multifatorial que pesa o dano potencial de tratamento e divulgação contra adequação de salvaguardas aos dados sensíveis.

O que chama atenção é o fato dos EUA e Europa tomarem como base os FIPPs, mas seguirem por caminhos completamente distintos. As discussões europeias reforçam a autonomia do direito à proteção de dados pessoais, enquanto as norte-americanas, não formalizam com clareza a diferença entre *data protection* e *data privacy*.

A *Bill of Rights* americana, que emendou a Constituição, baseia-se em uma gama de restrições ao governo pela liberdade individual. Ressalta-se, porém, que a característica constitucional é sintética entendida pelo contexto histórico que buscava limitar o poder central do Estado em 1787 e desde esta data permanece em vigor, o que resulta em um rol de direitos negativos, muito conectados à ideia de propriedade, reforçando também a basilar e fortíssima defesa à liberdade de discurso e expressão. Um traço claro da cultura norte-americana.

Ademais, é necessário destacar o sistema jurídico como *Common Law*, em resumo, a jurisprudência e os costumes (direito consuetudinário) aplicam as normas e regras. Apesar de atualmente não existir uma completa rigidez quanto ao tema, dada a flexibilização e promulgação de legislações importantes, é de suma relevância interpretar os contextos e definições refletindo sobre a postura dos tribunais norte-americanos que têm o papel central de construção de direitos.

O conceito de direito à privacidade ganhou forma doutrinariamente pela visão norte-americana com Warren e Brandeis em 1890, fixou-se nos seus estudos um direito de ser deixado só - *the right to be alone*. Todavia, como mencionado outrora, houve dificuldade inicial para consolidação deste no formato regulatório pois os limites legais eram definidos de forma mais rígida pela jurisprudência, traço da *Common Law*. Depreende-se, contudo, que a força deste direito tomou proporções relevantes que se tornou aceitável nas decisões dos juízes e consolidou-se no direito norte-americano.

Frisa que a gênese deste direito tem um viés muito elitista, uma vez que ambos os doutrinadores eram socioeconomicamente favorecidos e estabeleceram uma perspectiva muito vinculada à noção de propriedade, que é um dos direitos fundamentais expressamente previstos na Constituição. Assim, o *right to privacy* foi associado à ideia de casa, moradia, protegendo a vida privada das pessoas dentro de seu próprio lar, restrita então ao direito negativo.

Setorialmente, estatutos foram promulgados e iniciativas surgiram para garantir maiores proteções e direitos, como o *Privacy Act* para impedir repleta arbitrariedade e vigilância do governo e *Fair Credit Reporting Act* para evitar o uso indiscriminado de relatórios de crédito dos consumidores pelas entidades privadas. Todavia, não é possível notar uma

harmonização e uniformização regulatória nos Estados Unidos quanto ao tema, pois a confusão com o direito à privacidade, a concepção do consentimento como base legal protagonista e exclusiva para efeitos regulatórios, o receio de um controle absoluto dos dados pelo próprio titular que poderia estagnar a cultura da inovação tão cara para economia e desenvolvimento do país, podem ser fatores impeditivos de um desenvolvimento regulatório e geram engano com tentativas de legislações americanas de privacidade de dados que falharam ou foram ineficientes.

Para um país que pouco limita a liberdade de expressão quando ponderada com outros direitos, estabiliza a cultura da inovação, a promulgação de uma legislação geral torna-se um grande desafio. Kaminsky (KAMINSKY, 2021), uma professora norte-americana, em seu texto *An American's Guide to GDPR*, aprofunda-se nos principais equívocos sobre a interpretação do seu país quanto aos parâmetros normativos e ressalta que pensar na privacidade e proteção de dados como um mesmo direito é um erro, mesmo pela estrutura e fundamentos da defesa do direito à privacidade contra o governo, por isso, leis de proteção de dados que focam na transparência, prestação de contas e direito de acesso para responsabilização civil das companhias, é mais compatível com a proteção à liberdade de expressão pelo *Freedom of Information Act* (FOIA) garantindo ao titular uma maior autonomia, que não é absoluta, reforça com afinco Kaminsky, na Era dos Dados.

São 5 estados com legislação assinada, destes, o *California Consumer Privacy Act*, em vigor desde 2020, já em Colorado, Connecticut, Virginia e Utah, as leis entrarão em vigor apenas em 2023. Há mais 8 Projetos de Lei que constam em azul sobre proteção de dados tramitando no Comitê para aprovação (Michigan, Nova Jersey, Ohio e Pensilvânia [alguns estados com mais de um projeto em tramitação]) e, em cinza escuro, algumas iniciativas ainda não ativas. É possível que essas ações não virem leis, porém, já demonstra o crescimento da relevância e a pauta sobre o tema.

Um traço que merece destaque é a setorialização dos projetos, mesmo os que já entraram em vigor, pois apresentam-se muito voltados ao âmbito consumerista e obrigações comerciais. No âmbito federal, por exemplo, o *Federal Trade Comission* buscando a proteção dos consumidores e em prol de um comércio justo e não enganoso pode defender os titulares de dados nos casos de falsas promessas comerciais e injustas políticas de privacidade. Assim, os parâmetros da proteção de dados se consolidam através de situações e instituições particulares, como em dados de consumidores, dados de crianças (*COPPA*), dados relacionados à saúde (*HIPAA*), à crédito (*FCRA*), à família (*FERPA*) etc.

Mesmo muito tímida, há alguma ideia de legislação única: a ADPPA (American Data Privacy and Protection Act) é uma proposta de Lei bi-partidária que se encontra atualmente em debate no Congresso Americano. Pretende unificar a legislação sobre proteção de dados no território americano, constituindo também uma autoridade nacional central para a regulação da atividade de tratamento de dados pessoais.

Contudo, a sensação de liberalidade e o uso indiscriminado de dados das pessoas é uma sensação constante para muitos norte-americanos. Um artigo do The New York Times, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)* escrito por Thorin Klosowski (KLOSOWSKI, 2020), que em tradução livre, aborda alguns acontecimentos preocupantes que ficaram sem quaisquer sanções ou condenações:

> Vimos um meio de comunicação usar dados de aplicativos pseudônimos supostamente vazados de um anunciante associado ao aplicativo de namoro Grindr, que identificou um padre utilizando os serviços. Lemos sobre o governo dos EUA comprando dados de localização de um aplicativo de oração. Pesquisadores descobriram aplicativos de tratamento de dependência de opióides compartilhando dados sensíveis. E a T-Mobile sofreu recentemente uma violação de dados que afetou pelo menos 40 milhões de pessoas, algumas que nunca tiveram uma conta T-Mobile.

Kate Ruane (*apud* KLOSOWSKI, 2020), conselheira sênior da *ACLU - American Civil Liberties Union*, afirma que os dados das pessoas estão sendo usados e tomados de forma muito danosa e para construção de uma internet melhor, um mundo melhor, precisa de maior proteção à privacidade. Inclusive, faz dura crítica à legislação aprovada da Virgínia, pois considera um *lobby* ostensivo da Amazon na aprovação, por isso, restou-se numa legislação fraca de proteção dos direitos civis e repleta de disposições afirmativas ao modelo de negócio.

Como influência positiva para supressão deste vácuo regulatório, destaca-se a legislação aplicável aos consumidores da Califórnia (*CCPA*), já em vigor, pois apesar de não ser uma lei geral, fixou importantes direitos aos titulares, dentre estes: o direito de acesso; o direito de remoção; o direito à portabilidade; o direito de *opt-out* para venda de dados; direito à transparência; não discriminação; entre outros.

Frisa-se que diferente da opção do legislador brasileiro em ampliar o conceito e proteção dos dados pessoais, já que protege inclusive aqueles manifestamente públicos, para fins da CCPA não é considerado dado pessoal as informações publicamente disponíveis de registros do governo federal, estadual ou local, como licenças profissionais e registros públicos de imóveis[6].

---

[6] DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA. BONTA, Rob. Advogado Geral. https://www.oag.ca.gov/privacy/ccpa Acesso em 28/08/2022

A despeito disso, o CCPA inova na criação do "*private right of action*"[7] que consiste na possibilidade do titular de dados a processar (*to sue*) a empresa que está tratando os seus próprios dados em caso de incidente de segurança ou *data breach,* todavia, há um rol taxativo dos dados que cumprem os requisitos para a possibilidade de execução deste direito, tais como:

> - O número de segurança social;
> - O número da carteira de motorista, número de identificação fiscal, número do passaporte, número de identificação militar ou outro número de identificação exclusivo emitido em um documento do governo comumente usado para identificar a identidade de uma pessoa;
> - O número da conta financeira, número do cartão de crédito ou número do cartão de débito, se combinado com qualquer código de segurança, código de acesso ou senha necessários que permitiriam que alguém acesse sua conta;
> - As informações médicas ou de seguro de saúde;
> - Impressão digital, imagem de retina ou íris ou outros dados biométricos exclusivos usados para identificar a identidade de uma pessoa (mas não incluindo fotografias, a menos que sejam usadas ou armazenadas para fins de reconhecimento facial)[8]

Há uma ressalva sobre a forma como ocorreu o incidente pois somente caberá ao titular a possibilidade de ação e execução do direito de dano se as informações pessoais forem roubadas de forma não criptografada e não editada, o que demonstra a necessidade minimamente técnica de avaliação da forma do vazamento que não parece uma tarefa tão fácil para o indivíduo.

Em uma investigação do *National Law Review* sobre o ajuizamento das ações vinculadas às reclamações dos titulares fundadas no direito de ação do CCPA em 2021[9], tem-se 125 casos, destes 91,2% foram propostas nos tribunais federais e, em cada trimestre, a média foi de 30 a 35, mas, diante de um judiciário norte americano ainda muito conservador, 60% desses casos foram arquivados. Notavelmente, quase 40% destes casos se referiam ao incidente de segurança da empresa T-Mobile que envolveu hackeamento do número de segurança social, nome, endereço, data de nascimento e carteira de motorista e, das empresas que figuram no polo passivo do total dessas ações majoritariamente foram das indústrias de comunicações e serviços financeiros.

Ademais, da fixação de parâmetros jurisprudenciais, destacam-se 3 casos:

Lavarious Gardiner v. Walmart Inc., trata-se de demanda sobre violação de dados pessoais por incidente de segurança notada pelo titular ao encontrar seus dados na dark web,

---

[7] Projetos de Lei de Connecticut, Florida, Oklahoma, Washington e Dakota do Norte falharam na tentativa de promulgação por tentarem prever o "*private right of action*".

[8] DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA.BONTA, Rob. Advogado Geral. https://www.oag.ca.gov/privacy/ccpa. Acesso em 28/08/2022.

[9] THE NATIONAL LAW REVIEW, 2021 Year in Review: CCPA Litigation https://www.natlawreview.com/article/2021-year-review-ccpa-litigation. Acesso em 28/08/2022.

em defesa a Walmart alegou que não houve prova do autor quanto a data do "vazamento", logo, não sendo a CCPA retroativa, não lograria ao titular o direito de dano, tese que prevaleceu no tribunal, que, em tradução livre, afirma que a "*ausência de alegações estabelecendo que a suposta violação da CCPA pelo Walmart ocorreu após sua entrada em vigor, a reivindicação da CCPA do Autor não é viável.",* além disso, também considerou que o autor não alegou suficientemente o dano e divulgação de seus dados pessoais[10].

Sob alegação de programas de segurança deficiente e descumprimento dos padrões regulatórios da Blackbaud[11], no litígio multidistrital de privacidade (MDL[12] Nº 2972 [DSC 12/08/2021]), o Tribunal considerou que a empresa tem um modelo de negócio tutelado pelo CCPA, esta, por outro lado, alegou que qualificar-se-ia como uma "corretora de dados", contudo, fixou-se a caracterização como "prestador de serviços" para fins de responsabilização da lei da Califórnia.

No que tange às ações coletivas, o caso TransUnion LLC v. Ramirez chegou à Suprema Corte norte-americana, que decidiu pela ausência de "lesão de fato" que seria um interesse concreto e particularizado ou real ou iminente, isto é, no caso em questão, os autores não conseguiram comprovar um dano concreto.

Ademais, mesmo a Corte reconhecendo que danos intangíveis poderão ser concretos, entendeu que o autor não "satisfaz automaticamente o requisito de dano de fato sempre que uma lei concede a uma pessoa um direito estatutário e pretende autorizar essa pessoa a processar para reivindicar esse direito".[13]

O que chama atenção é que a demanda proposta pela TransUnion, uma classe composta por 8.185 consumidores, reivindicava um dano extrapatrimonial pois os Estados Unidos os consideravam como potenciais ameaças terroristas, quando na verdade apenas

---

[10] DYADKINA, Raisa, Data Breach Litigation Without a Data Breach? Not So Fast Walmart Says…. 2020. https://www.consumerprivacyworld.com/2020/12/data-breach-litigation-without-a-data-breach-not-so-fast-walmart-says/. Acesso em 28/08/2022.

[11] BRYAN, Kristin e LAMOUREUX, Christina. IT'S ON! Federal Court Orders Creation of Two Massive Data Privacy MDLs This Week Involving Clearview and Blackbaud. 2020. https://www.consumerprivacyworld.com/2020/12/its-on-federal-court-orders-creation-of-two-massive-data-privacy-mdls-this-week-involving-clearview-and-blackbaud/. Acesso em 28/08/2022.

[12] Os MDLs (ações multidistritais) são uma forma de lidar com várias ações civis de uma só vez e podem ser formados quando ações separadas em diferentes tribunais distritais compartilham uma questão de fato comum, normalmente utilizada no âmbito consumerista dos EUA. Vale ressaltar que os MDLs diferem das ações coletivas porque, enquanto uma ação coletiva é uma ação movida em nome de um grupo de demandantes, aquela permanecerá mantendo os processos separados que são tratados em conjunto para maior eficiência.

[13] CATTANACH, Robert. SCHMIDT, Kent. JORDAN, Melonie. "No Concrete Harm, No Standing" – Supreme Court's TransUnion v. Ramirez Decision Clarifies Federal Court Standing Requirements for CCPA and BIPA Class Actions. 2021 https://www.dorsey.com/newsresources/publications/client-alerts/2021/06/supreme-courts-transunion-v-ramirez-decision. Acesso em 30/08/2022.

tinham nomes similares àqueles que porventura seriam supostos criminosos, logo, a sinalização da administração norte-americana era um falso positivo quanto aos autores.

De todo modo, ao curso do processo, notou-se que 1.853 dos 8.185 efetivamente tiveram seus relatórios compartilhados com terceiros, o que resultou no entendimento da Corte que a violação por si só da CCPA não gera dano indenizável, tão somente se houver materialização a comprovação do dano, ou seja, apenas no caso dos 1.853, "*No Concrete Harm, No Standing*"[14], destaca-se da tradução livre, trecho da decisão:

> Para fins permanentes, portanto, existe uma diferença importante entre (i) a causa legal de ação de um autor para processar um réu por violação da lei federal pelo réu e (ii) o dano concreto de um autor devido à violação da lei federal pelo réu. O Congresso pode criar causas de ação para que os queixosos processem os réus que violam essas proibições ou obrigações legais. Mas, de acordo com o Artigo III, uma lesão de direito não é uma lesão de fato. Somente aqueles queixosos que foram concretamente prejudicados pela violação estatutária de um réu podem processar esse réu privado por essa violação em um tribunal federal.

Nesse sentido, conclui-se que a Corte torna ainda mais difícil a comprovação de dano pelos demandantes das ações, cria um impeditivo para a tutela de proteção de dados pessoais e mantém o desequilíbrio entre o autor (titular de dados) e empresas detentoras de dados pois a legitimidade só será entendida para fins de propositura da ação com a comprovação da concretude de um dano, não apenas da violação da CCPA, fato que torna ainda mais árdua a busca pela privacidade em sentido latu sensu, isto é, não somente vinculada à intimidade e a proteção de dados, já que a cultura norte-americana tem um viés decisório mais conservador e em prol dos negócios e inovações, o que gera uma sensação de abuso e insegurança para os cidadãos.

7. Conclusão.

Objetivou-se neste artigo apresentar os debates atuais doutrinários sobre a Responsabilidade Civil na LGPD, bem como a postura dos tribunais após a sua entrada em vigor, salientando aspectos importantes que demonstram uma adaptação ainda prematura aos conceitos, tendências e complexidades, um viés mais conservador quanto à caracterização do dano moral em decorrência de incidentes de segurança, uma estratégia judiciária que pode-se vincular indiretamente a evitar a proliferação em massa de processos judiciários com demandas reparatórias.

---

[14] CATTANACH, Robert. SCHMIDT, Kent. JORDAN, Melonie. "No Concrete Harm, No Standing" – Supreme Court's TransUnion v. Ramirez Decision Clarifies Federal Court Standing Requirements for CCPA and BIPA Class Actions. 2021 https://www.dorsey.com/newsresources/publications/client-alerts/2021/06/supreme-courts-transunion-v-ramirez-decision. Acesso em 28/08/2022.

Contudo, faz-se necessário mencionar que a LGPD tem apenas 4 anos, entre idas e vindas até a entrada em vigor em sua integralidade.

Em paralelo, apresenta-se EUA e China e suas legislações, em que a primeira superpotência tecnológica dá ainda pequenos passos em prol de uma unidade com relação à privacidade e à proteção de dados pessoais de seus cidadãos frente às grandes companhias locais, utilizando-se do tema, contudo, como fundamento político para sobrepor seus interesses à nível global. A segunda potência, por sua vez, há anos se movimenta não apenas pela proteção dos indivíduos em sua particularidade, mas também pela segurança e pelos interesses nacionais relacionados a eventuais danos decorrentes do tratamento inadequado de informações da população, isso para supostamente resguardar a estabilidade social do país e conduzi-lo à "prosperidade comum" tão almejada.

Por fim, apela-se à disseminação da cultura de proteção de dados para que torne possível um mínimo equilíbrio na balança dessa economia global fundada em dados. Nota-se que, para que isto ocorra, o papel da sociedade civil, do Estado e das empresas são fundamentais, inclusive na participação dos debates multissetoriais para construção de um ambiente mais justo, criativo e igualitário. Por isso, "*precisamos fomentar alegria, desafio intelectual, individualidade, curiosidade e outras qualidades que não se encontram em um gráfico organizado*" (LANIER, 2018), isto é, na lógica computacional resumidamente restrita a 0101, não nas especificidades e multipotenciais próprios da pessoa humana.

5. Referências Bibliográficas:

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: <http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/>.

BRASIL. *Lei 13.709 de 14 de agosto de 2018* – Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

BODIN DE MORAES, Maria Celina e QUINELATO DE QUEIROZ, João. Artigo: LGPD: um novo regime de responsabilização civil dito proativo. Civilistica. 2019.

BRYAN, Kristin e LAMOUREUX, Christina. IT'S ON! Federal Court Orders Creation of Two Massive Data Privacy MDLs This Week Involving Clearview and Blackbaud. 2020. https://www.consumerprivacyworld.com/2020/12/its-on-federal-court-orders-creation-of-two-massive-data-privacy-mdls-this-week-involving-clearview-and-blackbaud/. Acesso em 28/08/2022.

CATTANACH, Robert. SCHMIDT, Kent. JORDAN, Melonie. “No Concrete Harm, No Standing” – Supreme Court’s TransUnion v. Ramirez Decision Clarifies Federal Court Standing Requirements for CCPA and BIPA Class Actions. 2021 https://www.dorsey.com/newsresources/publications/client-alerts/2021/06/supreme-courts-transunion-v-ramirez-decision. Acesso em 30/08/2022.

DANTAS BISNETO, Cícero. Reparação por danos morais pela violação à LGPD e ao RGPD: Uma abordagem de Direito Comparado. Civilistica, 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados.* São Paulo: Thomson Reuters Brasil, 2019.

DYADKINA, Raisa, Data Breach Litigation Without a Data Breach? Not So Fast Walmart Says…. 2020. https://www.consumerprivacyworld.com/2020/12/data-breach-litigation-without-a-data-breach-not-so-fast-walmart-says/. Acesso em 28/08/2022.

KAMINSKY, Margot, JONES, Meg Leta. An American’s Guide to the GDPR. 2021. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620198*

KLOSOWSKI, Thorin. The State of Consumer Data Privacy Laws in the US (And Why It Matters). The New York Times. 2021 https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ Acesso em 27.08.2022

LANIER, Jaron. Dez argumentos para você deletar agora suas redes sociais. Rio de Janeiro, 2018. Ed. Intrínseca.

LEE, Michelle. “*Beyond Big Brother: Implications of China's Social Credit System for Global Credit and Governance”*. Thesis Presented to the Committee on Global Thought at Columbia University, 2022.

MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Editora Arquipélago.

SAMPAIO DA CRUZ, Gisela; MEIRELES, Rose M. V. Término do Tratamento de Dados. In: Gustavo Tepedino; Ana Frazão; Milena Donato Oliva. (Org.). Lei Geral de Proteção de Dados Pessoais. 1ed.São Paulo: Thomson Reuters / Revista dos Tribunais, 2019, v. 1, p. 219-241.

SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais. Tratado de Proteção de Dados Pessoais. Editora Forense, 2020. pgs. 331-334.