DIEGO COÊLHO

REGIME JURÍDICO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A REAFIRMAÇÃO DE DIREITOS HUMANOS E CONSTITUCIONAIS

editora itacaiúnas

DIEGO COÊLHO

REGIME JURÍDICO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

a reafirmação de direitos humanos e constitucionais

1º edição

Editora Itacaiúnas
Ananindeua - Pará
2020

1ª edição

Editoração eletrônica/ diagramação: Walter Rodrigues
Organização e preparação de originais: Deividy Edson
Projeto de capa: Os organizadores
Bibliotecário: Vagner Rodolfo da Silva - CRB-8/9410

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

C672r Coêlho, Diego Henrique Damasceno

Regime jurídico da proteção de dados pessoais no Brasil [recurso eletrônico] : a reafirmação de direitos humanos e constitucionais / Diego Henrique Damasceno Coêlho. – Ananindeua, PA : Itacaiúnas, 2020.
168 p. : il. ; PDF ; 6,60 MB.

Inclui bibliografia e índice.
ISBN: 978-65-88347-33-1 (Ebook)
DOI: 10.36599/itac-ed1.032
1. Direito. 2. Proteção de dados pessoais. 3. Direitos humanos e constitucionais. I. Título.

CDD 340
2020-2485 CDU 34

Elaborado por Vagner Rodolfo da Silva - CRB-8/9410

Índice para catálogo sistemático:
1. Direito 340
2. Direito 34

Esta obra foi publicada pela Editora Itacaiúnas em outubro de 2020.

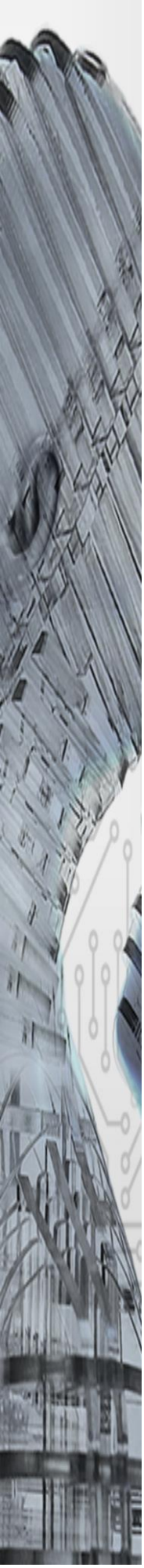
Dedico aos meus pais, os meus primeiros professores, sempre doadores de seus conhecimentos, sabedoria e generosidade, investindo amor, tempo e capital, como incentivos para a minha caminhada e com a confiança da superação de tempos os mais difíceis – sempre avante.

Muito obrigado!

APRESENTAÇÃO

A criação e a distribuição de tecnologias da informação e da comunicação (TICs), além de mecanismos eletroeletrônicos, de modo geral, proporcionaram às pessoas, empresas e governos novas condições de interoperabilidade e a expansão de mercados e economias em nível global, de modo que as relações entre indivíduos e máquinas ocorrendo cotidianamente, oportunizaram novas formas de comércio, produtos e serviços transcorridos no ciberespaço, através da internet - como uma rede aberta e democrática - um fenômeno socioeconômico que transformou o modo de vida, de pensamento e de produção, bem como oportunizou o surgimento de conflitos em decorrência da má utilização de tecnologias, em especial análise voltada para a coleta, o tratamento e o armazenamento de dados pessoais realizados por empresas físicas e virtuais ou pela Administração Pública. Para tutelar tais conflitos, os Estados têm desenvolvido Leis de Proteção de Dados Pessoais, em um panorama de possível concorrência entre normas de direito doméstico, estrangeiro e internacional, sobre demandas envolvendo violações a proteção. Assim sendo, a presente pesquisa, desenvolvida em sede de dissertação de mestrado, tem como objetivo identificar e compreender os aspectos, contextuais, geracionais e normativos mais relevantes para a conformação do Regime Jurídico da Lei de Proteção de Dados Pessoais – LGPD, no Brasil à luz da implementação da Lei nº 13.709/2018, com especial atenção voltada para os Direitos Humanos, o princípio da dignidade da pessoa humana, o direito constitucional fundamental à privacidade e os direitos à proteção de dados pessoais, à segurança digital e à autodeterminação informativa, através do método hipotético-dedutivo, em caráter predominantemente qualitativo, contemplando as taxonomias advindas da Ciência da Computação e da Informática, da Economia Digital, do Direito Constitucional em perspectiva comparada, o Direito Internacional Público e Privado e o Direito Administrativo, para verificar possíveis modalidades de exercício jurisdicional no Brasil em demandas envolvendo violação à proteção de dados pessoais, considerando possíveis conflitos de competência e o exercício da jurisdicional transnacional (*cross-border*), quando da entrada em vigor da LGPD, com o intuito de corresponder a uma necessidade coletiva de saber e aprender, visando à consolidação de uma infraestrutura social mais ética e capaz de fortalecer o Estado Constitucional Democrático, a dignidade da pessoa humana, a privacidade e a proteção de dados como direitos fundamentais e inalienáveis.

SUMÁRIO



INTRODUÇÃO

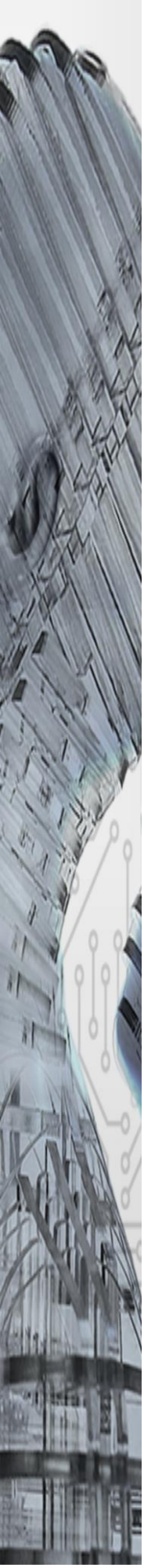
O desenvolvimento de um novo campo para a economia, com a utilização de ferramentas de comunicação digital sendo aperfeiçoadas e oferecidas em massa à população, desde meados dos anos 70 do século XX, oportunizou o estabelecimento de novas formas de comércio e de circulação mercantil, fortemente relacionadas à globalização e fundamentadas numa rede aberta e democrática - um fenômeno socioeconômico que transformou o modo de vida, de pensamento e de produção. Neste novo cenário, "a fluidez do consumo e a ausência de limites para a inovação são as principais características" (BAUMAN, 2001, p.18). Segundo Meadows:

> [...] na década de 1980, o desenvolvimento da tecnologia da informação e comunicação alcançara a etapa em que podia começar a competir com a impressão em papel, como meio universal para difundir informações científicas. Nos últimos anos, portanto, passou a ser razoável examinar a possibilidade de se transferir informações científicas do meio impresso para o meio eletrônico. (MEADOWS, 1999, p. 35)

O Direito, como ciência viva e dinâmica, também busca se adaptar às novidades tecnológicas, para atender às demandas judiciais sobre questões dos campos virtuais e eletrônicos, se adequando às configurações exigidas por setores sociais e empresariais do momento histórico mais recente (BOBBIO, 2007, 206-208). Por consequência, o Judiciário tem sido nas últimas duas décadas e, a cada ano mais, conforme demonstram as pesquisas realizadas pelo Supremo Tribunal Federal – STF, através dos anuários "Justiça em Números" (CNJ, 2017; CNJ, 2018), provocado a decidir questões disciplinadas pelo termo guarda-chuva do Direito Eletrônico[1], mas dentro do microambiente virtual, como uma seara jurídica em construção de suas legislações específicas.

Um dos reflexos decorrentes da utilização da Internet e das Tecnologias da Informação e da Comunicação (TICs) por governos, empresas e indivíduos é a necessidade de compreensão das dimensões sobre a proteção de dados pessoais no ambiente virtual. Tal como nas relações sociais, "o mercado e a economia virtuais, através da Internet, propiciaram

[1] O Direito Eletrônico, como doutrina de relativa juventude e em franco desenvolvimento no panorama jurídico-literário brasileiro, tem interconexão com o Direito Digital, o Direito Virtual e o Direito da Internet, por vezes sendo confundidos entre si, além de terem acrescentado novos contornos aos Direitos Humanos, ao Direito Constitucional, de Propriedade Industrial e Intelectual, do Consumidor, Contratual, Empresarial, Civil, Penal e seus Processos, ao Processual Eletrônico, aos Direitos Mercantil, Industrial, Econômico, Financeiro, Eleitoral, e Desportivo, dentre outras áreas, revelando a sua autonomia para fundamentar pedidos e decisões judiciais, complementando e fortalecendo searas normativas até então desprotegidas.



a ampliação da circulação de produtos, bens e serviços, mediante comércio eletrônico e a troca de informações" (ANGHERN, 1997, p. 362), também conhecido como "E-*commerce*". O crescimento "exponencial do comércio eletrônico tem levado analistas, economistas e consumidores a estudarem as adequações de mercados *on-line*, prevendo a paulatina redução de lojas físicas do varejo tradicional" (MISTRY; DHAVALE, 2011, p. 94), podendo ser atualmente comercializados bens, produtos e serviços pela Internet, em moedas nacionais, cartões bancários, carteiras digitais, ou através das chamadas "criptomoedas" ou *webcoins*.

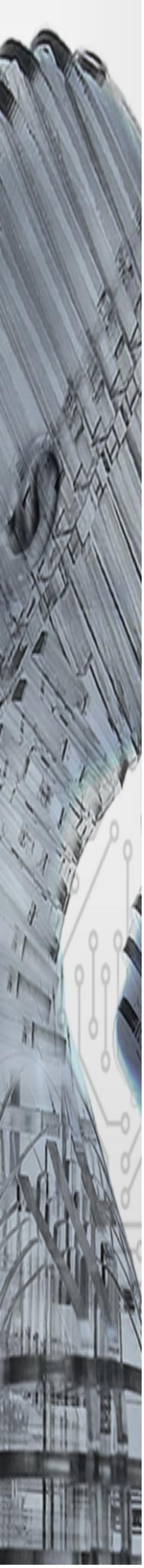
De forma semelhante, a Administração Pública e os órgãos dos governos, seja no Brasil seja em países estrangeiros, também têm adequado as suas estruturas administrativas para adquirirem equipamentos eletrônicos que utilizem o processamento de dados coletados de contribuintes, cidadãos, partes (autoras e rés) em processos judiciais e residentes de forma geral, usuários da rede pública de saúde e de ensino, dos sistemas financeiro e fiscal e em demais fontes de informação, a fim de aprimorarem a execução de políticas e garantirem maior eficiência, controle social e boa governança, a partir do conhecimento mais detalhado de setores específicos, por via do cruzamento e sobreposição de dados nacionais e internacionais. Assim sendo, empresas públicas e privadas e entidades governamentais passaram a realizar diariamente a coleta e o tratamento de dados pessoais[2].

Os dados pessoais são informações transcritas em documentos individuais em vias físicas ou virtuais, capazes de individualizar uma pessoa, fornecer formas de contato, endereçamento, idade e renda, por exemplo, compreendendo tanto dados públicos como também as informações provenientes de atos tidos como privados, tais como a reprodução de imagens capturadas por câmeras de vigilância[3], informações bancárias (como locais e valores de saques), o geoposicionamento de aparelhos eletroeletrônicos (como *smartphones, tablets* e computadores, através de rastreamento do endereço de IP[4]) e o conteúdo de e-mails e mensagens de aplicativos.

[2] A "coleta" e o "tratamento de dados" são conceitos que, junto aos demais abarcados pelas legislações sobre Direito Virtual e Eletrônico e de Proteção de Dados, encontram-se explicados de modo mais aprofundado no presente estudo, com a leitura da seção de número 2: Globalização da Informação: Perfis de Proteção de Dados e Economia Virtual, a partir da página 30.

[3] Após as revelações de Edward Snowden sobre a espionagem realizada pelos serviços de Inteligência dos Estados Unidos da América, corroboradas pelos documentos vazados por Julian Assange e o *site* Wikileaks, o termo "*mass surveillance",* ou monitoramento de massa, alçou maior amplitude e popularizou-se, significando a utilização de câmeras de vigilância – públicas e privadas, incluindo captação de áudio e vídeo mediante invasão ilegal de aparelhos eletroeletrônicos e apropriação de informações e dados pessoais, de maneira *contra legem*, mas com o apoio e o fomento do Estado, destacando a facilidade de se realizarem interceptações, sem o aval judicial e em completo desrespeito aos Direitos Humanos e Constitucionais.

[4] Segundo a definição trazida pelo Marco Civil da Internet (BRASIL, 2014), IP é "o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais" (BRASIL, 2014).

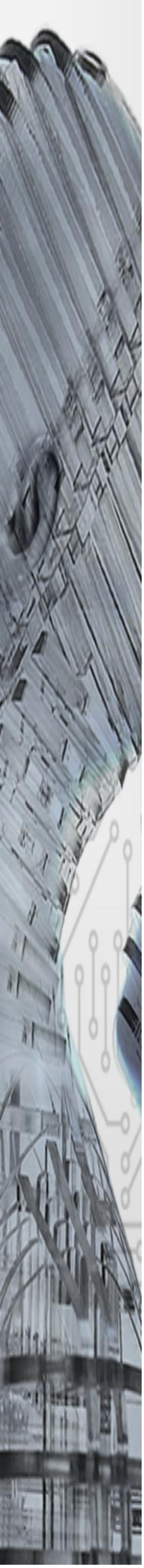


Como os dados pessoais de natureza pública ou privada são conteúdos de fácil violação, estes se tornaram temas de discussão, análise e pesquisa voltados para a criação de leis à luz da privacidade, da segurança digital e da proteção. Como Direitos Humanos inalienáveis e constitucionais fundamentais, sobretudo em sede de investigação policial, na maioria vezes sem a específica autorização judicial prévia, ou por parte de empresas de crédito e cobranças, tais manipulações de dados pessoais configuram abusos e desrespeitos à intimidade do indivíduo, que se encontra em relação de desigualdade, desvantagem e hipossuficiência frente às possibilidades de danos por incidentes envolvendo dados pessoais ou à capacidade obter sucesso em um eventual processo judicial, frente à capacidade de defesa por parte de autoridades governamentais e de agentes empresariais e corporativos.

Para compreender a necessidade da proteção de dados pessoais como um direito previsto em leis específicas, as seguintes hipóteses podem levar a uma reflexão crítica, questionando se: caso um indivíduo revisasse toda a sua atividade envolvendo produção e compartilhamento de informações em ambiente físico e virtual nas últimas 24 horas, possivelmente contendo nomes e números de identificação pessoal (Identidade, CPF, Passaporte), números de cartões de créditos, endereços eletrônicos (*e-mails*), endereços residenciais, fotos e vídeos em redes sociais, conversas em aplicativos de mensagens, além de informações públicas e dados sobre quais sítios eletrônicos foram acessados, trafegando e permanecendo visíveis *online*, ou armazenados em *caches* e *cookies* ou em "nuvens", com quem tal indivíduo se sentiria plenamente seguro para confidenciar e guardar todas estas referências? Com os pais, irmãos, o melhor amigo, o patrão, um colega de trabalho, o cônjuge ou companheiro, em alguma nuvem de dados em um país distante, ou com o Governo de seu país?

Todo este tráfego de valores e informações, reduzidas a dados, feitas tanto por pessoas físicas, quanto jurídicas privadas ou jurídicas de direito público, através de seus agentes, podem parecer irrelevantes, mas quando esses pequenos fragmentos de vidas e personalidades são reunidos, eles têm a capacidade de serem usados para integrar uma imagem detalhada (perfilamento social) a respeito de um indivíduo: suas crenças, identidade, gostos, desgostos, localização, movimentos, associações e muito mais.

Esta reunião de fragmentos de cada ser humano possui potenciais econômicos, resultando em um fenômeno de precificação sobre os dados pessoais, como uma consequência natural à circulação de informações por meio eletrônico. Outras violações podem sobrevir, causando problemas à vida de seus respectivos titulares de dados pessoais, tal como a pirataria



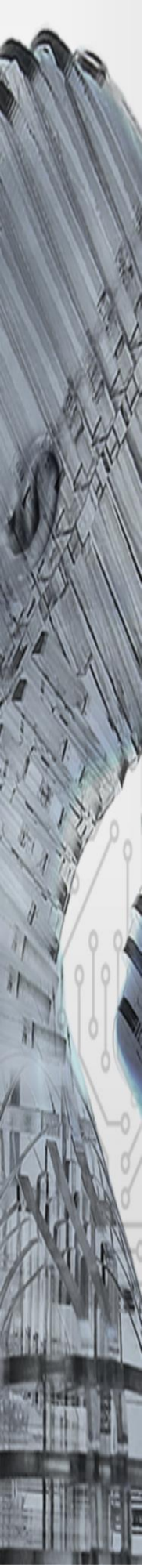
virtual, realizadas por *hackers* que roubam, alteram e vendem tais dados obtidos de maneira aberta ou ilegal, utilizando técnicas conhecidas como o *phishing*[5], por exemplo, dentre outros estratagemas maliciosos, os quais revelam um comércio não regulado dos dados pessoais, contas particulares e públicas, além de dados armazenados por governos e empresas.

Neste cenário de avanços e desafios, têm-se os Direitos Humanos e Constitucionais como estabelecidos, mas as formas pelas quais são compreendidos vêm sendo gradualmente modificadas pela presença da tecnologia e os seus desdobramentos práticos, que ao invés de estarem disponibilizados como ferramentas da era moderna, capazes de assegurar maior proteção à dignidade da pessoa humana, têm demonstrado falhas como o predomínio de interesses privados da indústria e de Governos, por sobre a proteção e o respeito à privacidade e à intimidade de pessoas - as quais não poderiam ter suas intimidades compreendidas como ativos financeiros ou possíveis fontes de lucro. Tais fatores, portanto, requerem uma mais aprofundada compreensão a respeito da exigência de um nível adequado à proteção de dados pessoais na Era Digital e a sua função precípua de manutenção dos espectros da chamada "liberdade", tais como a privacidade e a autodeterminação informativa, que vêm sendo paulatinamente mitigadas pela ubiquidade do monitoramento e da vivência no ciberespaço.

Neste sentido, a "liberdade" e o "monitoramento" encontram-se intimamente atrelados às formas como são utilizadas as Tecnologias de Informação e Comunicação, que compõem um setor em expansão e aprimoramento de equipamentos, aplicações, serviços e tecnologias básicas, enquadradas em três categorias, quais sejam: computadores, telecomunicações e dados multimídia. As tecnologias estão em constante evolução e são desenvolvidas de maneira independente ou interdependente, implicando em ajustes a cada nova versão dos aparelhos, *softwares* e aplicativos, bem como em questões relativas à interoperabilidade e à preservação da intimidade, na busca por eficiência e ampliação dos direitos fundamentais. Nas palavras de Ingo Wolfgang Sarlet:

> Todavia, em que pese este inquestionável progresso na esfera da sua positivação e toda a evolução ocorrida no que tange ao conteúdo dos direitos fundamentais, representado pelo esquema das diversas dimensões (ou gerações) de direitos, que atua como indicativo seguro de sua mutabilidade histórica, percebe-se que, mesmo hoje, no limiar do terceiro milênio e em plena era tecnológica, longe estamos de ter solucionado a miríade de problemas e desafios que a matéria suscita. (SARLET, 2018, p. 22).

[5] *Phishing* é a tentativa fraudulenta de obter informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito, muitas vezes por motivos maliciosos, disfarçando-se como uma entidade confiável em uma comunicação eletrônica. A palavra é um neologismo criado como um homófono do verbo em inglês *to fish*, cuja a tradução é "pescar", devido à semelhança de usar uma isca na tentativa de capturar uma vítima.



Dentre as várias lacunas peculiares ao processo natural e contínuo do aperfeiçoamento dos sistemas políticos, legislativos e sociais, os aparatos tecnológicos despontam também como mecanismos capazes de expandir as possibilidades de atuação humana e suas necessidades conexas, quando os seus valores de utilidade são empregados com o escopo de dar maior amplitude às ciências e à eficiência dos Estados, excluindo motivações econômicas sazonais ou ideológicas, oscilações e competições no mercado global e desmistificando paradigmas e preconceitos nos formalismos e rigores técnicos do estudo científico, os quais impõem, por vezes, barreiras ao acesso e à absorção de novos conteúdos. Nas palavras de Tefko Saracevicz:

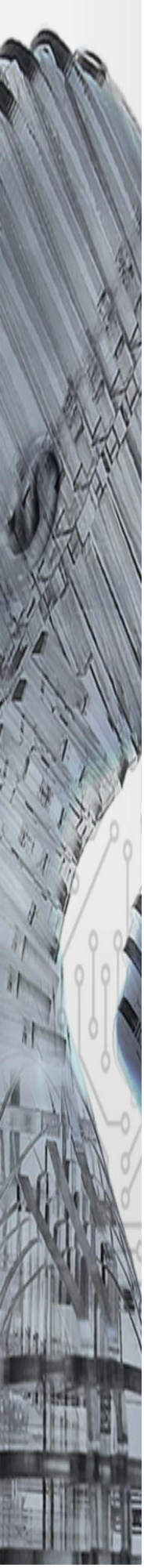
> A importância crítica de se buscar o equilíbrio da relação homem-tecnologia na problemática estudada pela CI[6] reside no simples e incontroverso truísmo de que, toda e qualquer aplicação da tecnologia e das técnicas, sem objetivos claros, com conceitos indefinidos ou uma filosofia nebulosa, introduzirão a barbárie. Gostaria de sugerir que os objetivos, a filosofia e os conceitos determinantes para o equilíbrio homem- tecnologia precisam originar-se do seu lado humano. (SARACEVICZ, 1996, p. 56)

Esta valorização do "lado humano" (SARACEVICZ, 1996, p. 56) da tecnologia também pode ser percebida no aprofundamento pelo qual a ciência jurídica passou a buscar a concretização da jurisdição, empregando o modelo democrático como base de transformação isonômica e protetiva do cidadão, de forma a buscar evitar excessos ou predominância exagerada dos interesses do Estado. Seguindo essa linha crítica, Cândido Rangel Dinamarco aponta, *in verbis*:

> A manutenção de dispositivos antiisonômicos no vigente Código de Processo Civil explica-se pelo fato de ele ser mera continuação do estatuto de 1939, em relação ao qual muito pouco se inovou substancialmente. Apoiados no falso dogma da indisponibilidade dos bens do Estado, os privilégios concedidos pela lei e pelos tribunais aos entes estatais alimentam a litigiosidade irresponsável que estes vêm praticando, mediante a propositura de demandas temerárias, oposição de resistências que da parte de um litigante comum seriam sancionadas como litigância de má-fé, excessiva interposição de recursos etc. - tudo concorrendo ainda para o congestionamento da tutela jurisdicional aos membros da população. (DINAMARCO, 2017, p. 233)

Como a expansão das Tecnologias de Informação e Comunicação (TICs) ocorre de modo acelerado, o ambiente virtual ainda apresenta mecanismos de segurança não tão eficientes quanto à atuação de agentes mal-intencionados, sobretudo para a parcela da população menos consciente quanto aos riscos presentes no mundo virtual e na (má) utilização de dispositivos conectados à Internet. Desta forma, muitos países tem buscado, pela

[6] CI como abreviatura para a Ciência da Informação.



via legislativa, criar mecanismos mais eficazes e seguros de controle, regulação, prevenção de crimes e punição, para fatos, negócios e atos jurídicos realizados através do ambiente virtual.

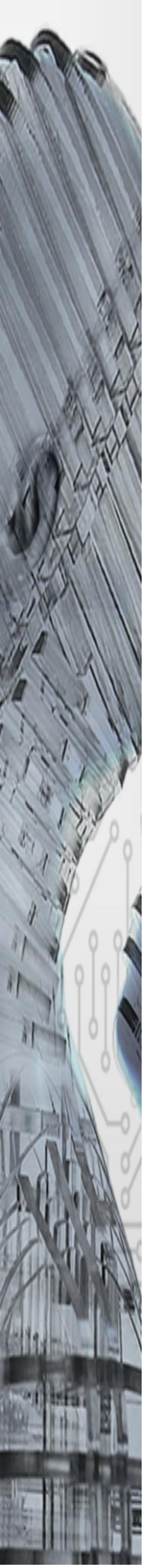
A atual configuração do direito à segurança e proteção de dados pessoais advém de construtos jurídicos históricos, cujas bases pavimentaram-se no direito fundamental à privacidade, insculpido em documentos internacionais lastreados nos Direitos Humanos, tais como na Declaração dos Direitos do Homem e do Cidadão, de 1789 (JELLINEK, 2015, 107 - 112), no art. 12 da Declaração Universal dos Direitos do Homem, de 1948 (ONU, 1948), no art. 5º da Declaração Americana dos Direitos e Deveres do Homem (CIDH, 1948), no art. 8º da Convenção Europeia dos Direitos do Homem (COMISSÃO DA EUROPA, 1950), bem como em constituições e normas de direito interno em diversos países[7]. O direito à privacidade está inserido no art. 5º, inciso X, da Constituição da República Federativa do Brasil (BRASIL, 2018), determinando que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação", bem como nos artigos do 11 ao 21 do Código Civil (BRASIL, 2002).

No Brasil, como um dos países com maior número de utilizadores do *cyberespaço* (ITU, 2018, p. 7), o instrumento de regulação específico para a proteção de dados pessoais foi incorporado no dia 14 de agosto de 2018, seguindo os passos do bloco europeu, quando adentrou no ordenamento jurídico nacional a Lei nº 13.709, também conhecida como Lei Geral de Proteção de Dados Pessoais - LGPD, a qual instituiu um Regime Jurídico formado pela consociação de direitos, deveres, garantias e penalidades aplicáveis a determinadas relações qualificadas tanto pelo Direito Público, quanto pelo Direito Privado.

A referida lei representa também o diálogo normativo e a aproximação do Brasil com os sistemas jurídico-econômicos de muitos de seus principais parceiros comerciais, bem como confere maior proteção, autodeterminação e segurança às relações governamentais e empresariais envolvendo a coleta e o tratamento de dados pessoais, em níveis nacional e transnacional.

Junto à Lei nº 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação e à Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, a LGPD visa ao aumento da proteção das informações pessoais, da

[7] *Exempli gratia:* As Constituições Constituição da República Portuguesa (1976); *Datenschutzgesetz* (ÁUSTRIA, 2000); Constituição de Espanha de (ESPANHA, 1978); Constituição Política da Colômbia, de 06 de julho de 1991; a Constituição da República do Paraguai, de 20 de junho de 1992, a Constituição Política da República do Peru: 31 de outubro de 1993, na Constituição da Nação Argentina, de 22 de agosto de 1994 e na Constituição da República do Equador, de 11 de agosto de 1998, dentre outras.



autodeterminação, da autogestão de dados e à promoção de maior segurança jurídica dentro e fora da Internet, estabelecendo limites entre a responsabilização pública, privada e pessoal.

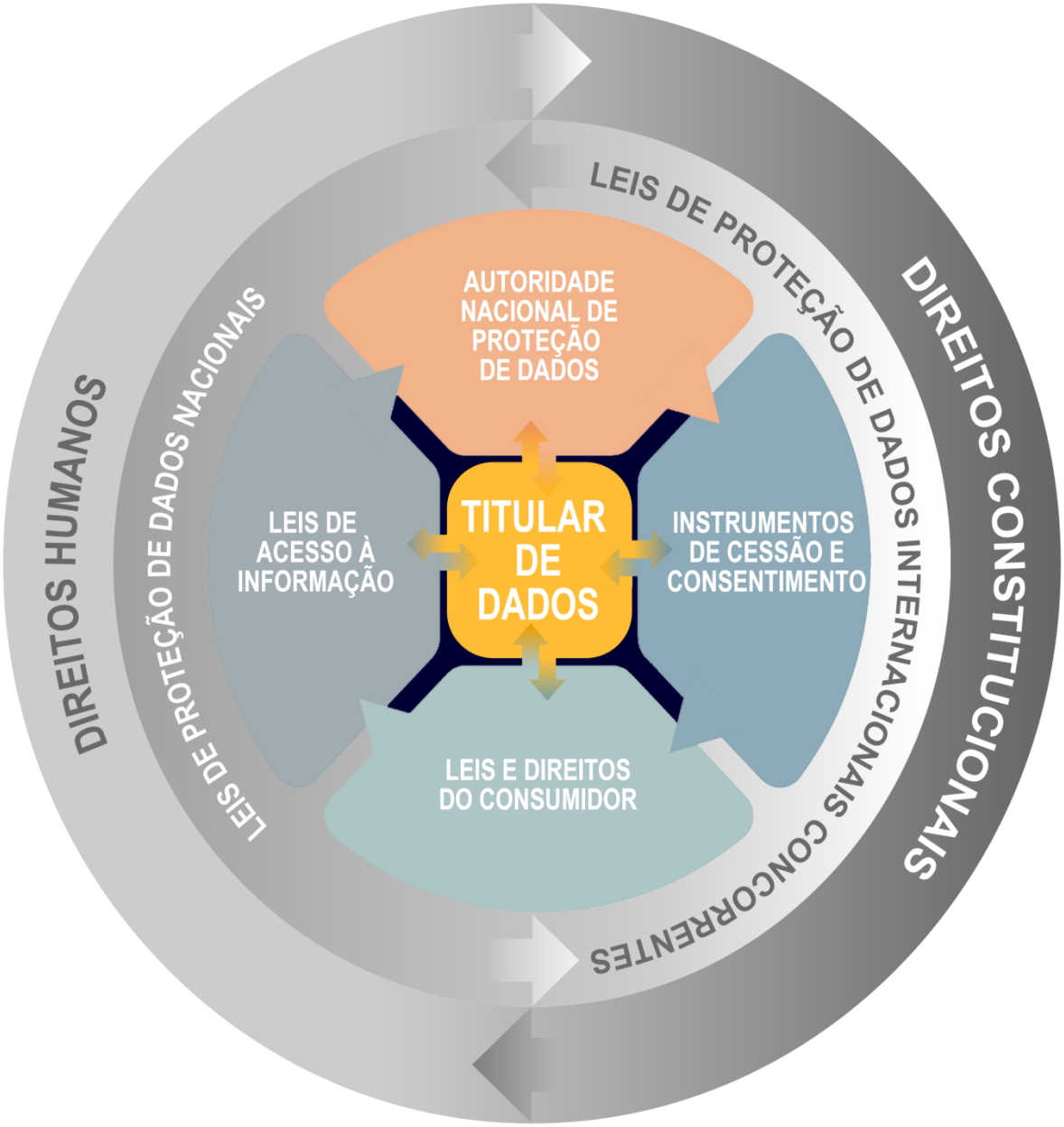
A LGPD possui caráter intersetorial e multidisciplinar, tendo em vista que afeta os setores público, privado, misto com o terceiro setor e as legislações a elas conexas, em decorrência de sua natureza constitucional proveniente do direito fundamental à privacidade, o que positiva este preceito constitucional e fortalece o princípio da Dignidade da Pessoa Humana e demais bases dos Direitos Humanos.

Na medida em que a economia global se torna interconectada e a Internet está amplamente disponibilizada - em dispositivos fixos ou portáteis e mediante provedores distribuídos por cabeamento ou por via satelitária, conflitos jurisdicionais envolvendo Estados, atores privados e agências reguladoras estão se tornando cada vez mais comuns. Neste passo, os Estados passam a frequentemente buscar a afirmação de sua jurisdição sobre as condutas que ocorrem fora de seus territórios, particularmente no que diz respeito às ocorrências em ambiente virtual. Dadas as especificidades pretendidas pela entrada em vigência da LGPD, é possível prever um cenário onde muitas questões sofrerão judicialização, por não estarem em conformidade com as novas regras.

Embora os princípios fundamentais e de alto nível das leis de proteção de dados sejam semelhantes entre regiões e sistemas jurídicos, neste espaço onde o virtual e o real colidem, as questões jurisdicionais, cujas competências tradicionais são geograficamente baseadas, poderão enfrentar dificuldades em determinar a jurisdição suficientemente competente para julgamento, tendo em vista que a comunicação eletrônica atravessa fronteiras sem ter qualquer ligação específica com o território onde a tecnologia está localizada e os usuários se envolvem em atividades globais sem a necessidade de presença física dentro do Estado onde ocorre negócio, ato ou fato jurídico capaz de ensejar análise em sede judicial.

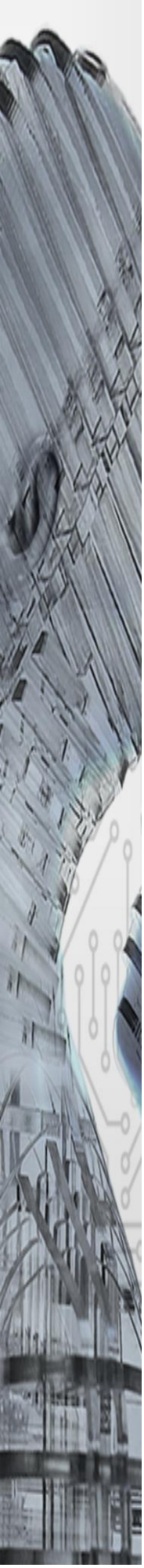
Deste modo, os impactos acarretados pela LGPD descortinam a introdução de novos direitos infraconstitucionais ao ordenamento jurídico brasileiro, bem como aduzem a uma reformulação nos comportamentos de todos os indivíduos, cidadãos, residentes, administradores empresariais e agentes públicos, em vistas a estarem em conformidade com os ditames da referida lei, ao passo que também dialogam com as leis de proteção de dados estrangeiras, nos casos de parcerias governamentais, empresariais e em operações de coleta e tratamento de dados realizados em outros Estados. Esta constelação normativa interdisciplinar permite compreender o Regime Jurídico da Proteção de Dados Pessoais conforme a proposição dos conteúdos presentes no seguinte diagrama:

FIGURA 1: Diagrama do Regime Jurídico da Proteção de Dados Pessoais.



Fonte: Elaboração própria.

Enquanto a utilização da Internet tem se tornado parte da vida diária para muitas pessoas, setores governamentais e segmentos empresariais, ao invés de representar um lugar – conhecido como "ciberespaço", que merece visita ocasional, os tribunais de diferentes países começam a tomar ações positivas visando à adaptação dos sistemas jurídicos existentes a ciber-réus, cujas identidades podem ser nebulosas ou residirem fora do Estado. Por conseguinte, os critérios de competência, de jurisdição e a escolha de legislação aplicável a cada caso, despontam como anátema a ser discutido, para a criação de posturas mais próximas



entre tribunais e suas jurisprudências, de modo que a proteção de dados pessoais como direito fundamental à privacidade, tenha também a segurança jurídica garantida pela atuação do Poder Judiciário.

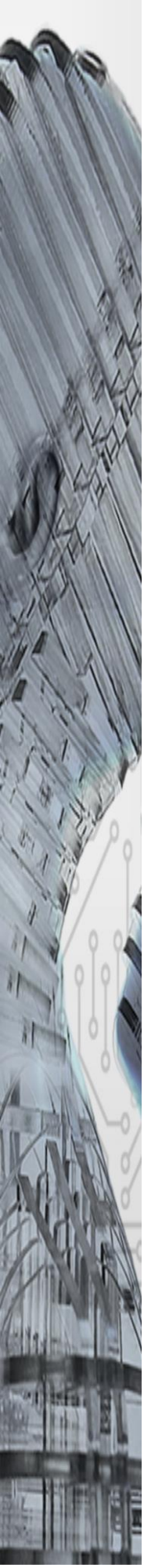
Na perspectiva das formas como a jurisdição pode ser exercida em proteção aos dados, o conhecimento acerca das legislações de direito público, as normas de direito privado, os tratados internacionais e as legislações já desenvolvidas sobre a temática em Estados estrangeiros, são componentes fundamentais do exercício jurisdicional realizado de forma interdisciplinar, também contemplando o macroambiente socioeconômico e geopolítico onde as relações, contratos e ilícitos possam envolver o desrespeito ao direito fundamental à privacidade e a proteção a dados pessoais, a fim de que toda a sistemática procedimental ocorra da forma mais aproximada à realidade o possível e, consequentemente, garanta o fortalecimento das instituições democráticas, do acesso à informação, da dignidade da pessoa humana e viabilize o aperfeiçoamento de leis e do próprio Estado Constitucional de Direito, com a garantia e a satisfação dos Direitos Humanos, de modo pleno.

À vista de tais componentes fundamentais, a literatura objetivamente trabalhada em sede de pesquisa, até o presente momento buscou situar o problema frente às diversas obras existentes sobre a proteção de dados pessoais, nos aspectos teóricos, filosóficos, legislativos e processuais, bem como a valoração das escolhas ante o interesse público, a economia e a ética, com o fito de compreender a moldura normativa, os contextos correlacionados e os possíveis impactos socioadministrativos da prestação jurisdicional estatal de forma eficaz.

Desta feita, a caracterização do recorte temático analisa a proteção de dados pessoais prioritariamente pelas perspectivas do Direito Constitucional e dos Direitos Humanos, considerando a amplitude da natureza interdisciplinar do tema, que abarca árvores científicas tais como a Ciência da Computação e da Informática, as Tecnologias da Informação e Comunicação, Economia Digital e Economia Ambiental Virtual, Direito Constitucional Brasileiro e Internacional, Direito e Processo Eletrônico Brasileiro e Internacional, Direito Administrativo, Direito Público, Direito Privado, Direito e Processo Civil, Ciências Políticas, Teoria Geral do Estado e demais fontes conexas de conhecimentos, com o escopo de localizar e interpretar os conteúdos delimitados em sede de pesquisa.

A partir de então, a coleta de informações, bibliografias e literaturas científicas, *prima facie,* buscou realizar uma investigação transversal[8] (LAMY, 2011) das bases

[8] Como técnica para análise e comparação e dados, o estudo investigativo transversal levanta e analisa dados, em um período de tempo definido como observacional, para estudar uma população em um momento, delimitado ou



conceituais e terminologias da Ciência da Computação envolvendo o processamento de dados, para então compreender sua aplicabilidade nos campos da Economia, da Administração Pública e do Direito Constitucional, sobretudo à luz da jurisdição aplicável à Lei Geral de Proteção de Dados brasileira e suas compatibilidades e lacunas na moldura jurídica proposta pelo Código de Processo Civil de 2015, cuja vigência se iniciou em abril de 2016 e pela Constituição Federal (BRASIL, 2018), analisando as possibilidades de atuação do Poder Judiciário, representado por seus magistrados, na aplicação prática da lei às regras específicas processuais, para soluções dos problemas envolvendo as ações judiciais que podem requerer análise de legislações internacionais para a fixação de critérios de competência e admissibilidade, assim como a garantia do acesso à Justiça, inserido no propugnado modelo do Regime Jurídico da Proteção de Dados Pessoais.

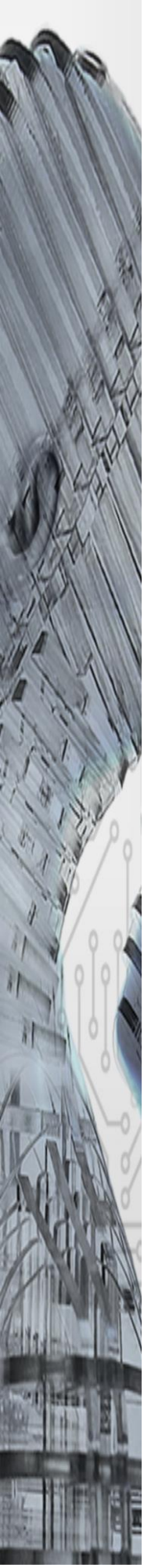
Desta análise inicial, buscou-se compreender o atual momento jurídico-normativo brasileiro na perspectiva da proteção de dados pessoais, donde emergiram os seguintes questionamentos:

- Quais são o(s) sentido[9] (s) e significado[10] (s) taxonômicos de terminologias importadas das Ciências da Computação e da Informática, à luz das Leis de Proteção de Dados Pessoais?
- Quais são os objetos jurídicos tutelados pela proteção à privacidade, à segurança e aos dados pessoais, na perspectiva dos Direitos Humanos e Constitucionais Fundamentais?
- Em quais ambientes (onde e por que) ocorrem a coleta de dados, quais são as finalidades de sua utilização e como podem ocorrer as principais violações a dados pessoais?
- Em quais contextos (quando) as Leis de Proteção de Dados Pessoais se desenvolveram e quais são as legislações mais relevantes sobre tal Regime Jurídico?
- De quais formas (como) as violações à privacidade e à proteção de dados pessoais poderão requerer a tutela jurisdicional, considerando a sobreposição de leis nacionais e internacionais?
- Quais são os critérios necessários para acolhimento e fixação de competência para julgar, tendo em vista a territorialidade como princípio presente nos instrumentos de cessão de dados pessoais?

não. Além disso, é importante para examinar a relação entre variáveis de interesse, como as socioeconômicas, normativas, geopolíticas, dentre outras funcionalidades.

[9] Sentido: forma de percepção subjetiva de cada sujeito a respeito de determinado objeto ou fato, envolvendo os aspectos sociais, políticos, econômicos, religiosos, culturais, éticos e jurídicos, dentre outros (LAMY, 2011).

[10] Significado: definição perene e objetiva de uma realidade socialmente construída e amplamente integrada ao senso comportamental comum (LAKATOS, MARCONI, 2003).



- Quais são os limites estabelecidos no novo CPC e nas legislações brasileiras para a adjudicação e processamento de pedidos lastreados em violações à proteção a dados pessoais, conforme a moldura normativa do ordenamento jurídico nacional?
- De quais maneiras a LGPD pode se tornar um mecanismo de cooperação internacional e de fortalecimento dos Direitos Humanos e Constitucionais Fundamentais, no ambiente virtual?

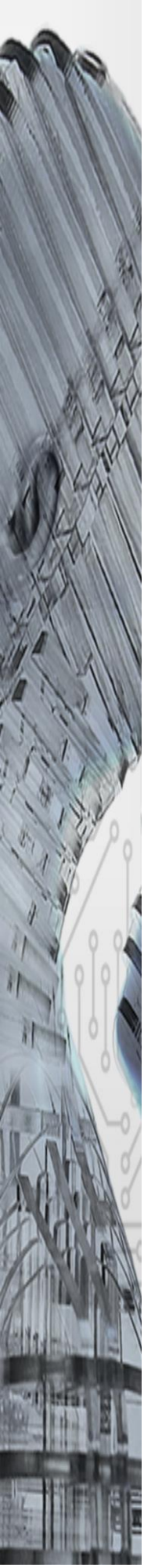
No escopo de obter respostas cientificamente viáveis a tais indagações, os seguintes objetivos foram delimitados:

- Objetivo geral:

- Identificar e compreender os aspectos, contextuais, geracionais e normativos mais relevantes para a conformação do Regime Jurídico da Proteção de Dados Pessoais no Brasil à luz da implementação da Lei nº 13.709/2018.

- Objetivos específicos:

- Conhecer e depreender os conceitos, princípios, tutelas, regras e sentidos jurídicos das nomenclaturas de natureza informática apresentadas nas leis de proteção de dados;
- Compreender dados e indicadores em economia virtual, seus impactos nos direitos à privacidade, à segurança digital, à proteção de dados pessoais e na manutenção da dignidade da vida humana;
- Localizar semelhanças e diferenças entre as legislações estrangeiras sobre proteção de dados pessoais e a LGPD, verificando aspectos geracionais e comuns.
- Diferenciar as formas de atuação jurisdicional previstas no Código de Processo Civil brasileiro em relação à Lei Geral de Proteção de Dados Pessoais e demais legislações internacionais;
- Verificar aspectos do exercício da jurisdição transfronteiriça (jurisdição *cross-border*), da Jurisdição Exorbitante e da Doutrina dos Efeitos, na sobreposição das Leis de Proteção de Dados Pessoais;
- Mapear os parâmetros legais e subjetivos que devem ser observados antes do acolhimento de pedidos sobre proteção de dados pessoais envolvendo empresas ou ente da Administração Pública como polo passivo do contexto jurídico-processual;



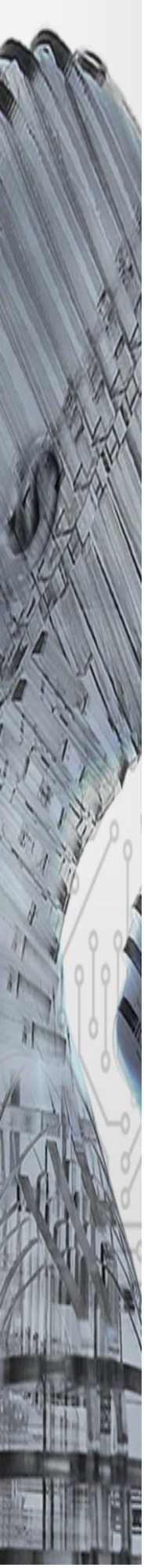
- Localizar leis, normas e princípios legais já estabelecidos que fixem os critérios de competência jurisdicional no Brasil e;
- Reforçar a necessidade de desenvolvimento da consciência individual e transpessoal sobre a proteção de dados pessoais, como um exercício de cidadania e de reafirmação dos direitos humanos e constitucionais.

Para tanto, a pesquisa empregou o método hipotético-dedutivo (LAKATOS; MARCONI, 2003, p. 48) na estruturação dos quesitos a serem analisados e verificados com o devido rigor metodológico para, na continuidade, perfazer uma profunda e esquadrinhada seleção literária qualitativa, com o escopo de pavimentar conceitos e paradigmas por meio de uma interpretação comparativa (LAMY, 2011, p. 67). Também foram trazidos à revisão alguns construtos normativos e jurídicos, os quais possibilitam a compreensão dos critérios de fixação para a competência em questões nacionais e internacionais envolvendo a proteção de dados pessoais, com enfoque em sua aclimação à jurisdição do Brasil, com base na moldura normativa da LGPD. Posto isto, o presente estudo também primou por examinar normas e leis internacionais e brasileiras, a fim de tecer um embasamento mais sólido para os quesitos perquiridos durante o desenvolvimento textual e complementar a abordagem qualitativa.

A pesquisa bibliográfica (BUCCI, 2008, p. 34 - 38) elaborada sobre os objetos do estudo, ocorreu através da triagem, separação, leitura e fichamento de legislações, livros, artigos científicos e textos, primordialmente, bem como utilizou estudos oficiais publicados por organizações de relevância nacional e internacional como fontes secundárias, estando estes, mormente disponibilizados em plataformas e sítios eletrônicos das respectivas instituições. O material contemplado correlaciona uma reflexão de rigor teórico-metodológico (LAKATOS; MARCONI, 2003, p. 38 - 42), selecionando e editando as informações específicas cabíveis no contexto do recorte temático (com inclusão e exclusão), extraídas mediante leitura atenta e sistemática, por via de fichamentos das informações contidas nas obras literárias, textos, publicações e demais materiais científicos levantados, visando a posterior ordenação e análise dos conteúdos em íntimo diálogo com o referencial teórico.

Desta forma, a presente pesquisa contemplou um desenvolvimento proposto em três seções[11], sendo a primeira delas a de número 2, intitulada “Globalização da Informação:

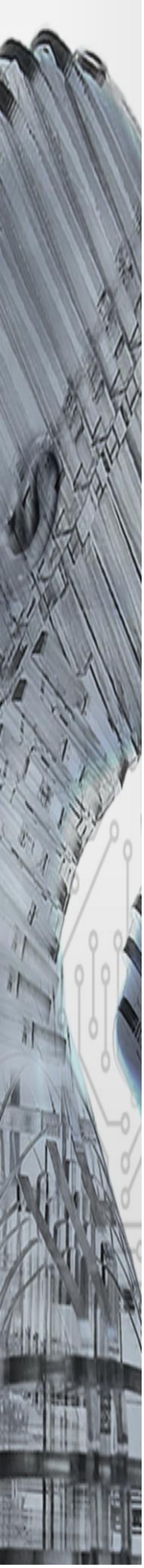
[11] Conforme a norma ABNT NBR 6024 (2012), a nomenclatura correta a ser utilizada é “seção”, para definir as divisões temáticas textuais. As nomenclaturas “item” ou “capítulo” não aparecem em nenhuma das normas em vigor da ABNT. No manual “Apresentação de trabalhos monográficos de conclusão de curso (TCC)” da Universidade Federal Fluminense - UFF (2013) também é adotada a nomenclatura “seção” para definir as divisões temáticas textuais.



Perfis de Proteção de Dados e a Economia Digital", objetivando inicialmente alicerçar a compreensão das terminologias advindas da linguagem computacional, como peças-chave para o estudo e melhor interpretação dos ambientes virtuais e reais, onde tem início a necessidade de promoção da privacidade e da segurança em dados. Deste modo, é apresentado um levantamento histórico acerca do advento da Ciência da Computação e da Informática, levando à consequente absorção de dispositivos e aparelhos capazes de produzir e armazenar dados; propiciando também a formação da sociedade da comunicação e a globalização em decorrência do desenvolvimento conexo das Tecnologias da Informação e da Comunicação. Nas seções secundárias são apresentadas as taxonomias de maior relevância para a compreensão de conceitos-chave, posteriormente empregados nas Leis de Proteção de Dados Pessoais, sendo os de maior destaque o tratamento de dados, a segurança (conjuntamente à confidencialidade, integridade e disponibilidade de dados), a transferência e o armazenamento de dados, não somente pessoais, como também os advindos pela captação de informações sobre valores do comércio eletrônico e das demais ocorrências no ambiente virtual, informações em nuvens de dados, a captação de dados meteorológicos, registros históricos, geográficos e financeiros, dentre outros, os quais produzem *Big Data*, como um grande conglomerado de dados que podem estar abertos e disponibilizados a setores públicos e privados, para análise de informações e dados em massa ou em larga escala.

Na continuidade, é analisada a Economia Virtual, contemplando principalmente informações e dados sobre a migração de setores da economia tradicional para o ambiente virtual, através de fatores como o fortalecimento do comércio eletrônico, a criação de moedas virtuais, a precificação de produtos eletrônicos, como os aplicativos e programas de *software*, a publicidade virtual, a tributação no ambiente da Internet, a circulação de mercadorias internacionalmente e o planejamento econômico de governos e empresas, tendo em vista a realização crescente das operações financeiras e comerciais mundiais em ambiente virtual. Neste ponto, a sustentabilidade econômica e sustentabilidade ambiental (leia-se: do meio ambiente natural e do ambiente virtual), representam duas perspectivas de atenção para os planejamentos em *e-commerce*, os quais devem coexistir a fim de promoverem a segurança jurídica esperada por consumidores, tanto no recebimento de produtos adquiridos, quanto no momento de coleta de seus dados, envolvendo números de documentos pessoais, cartões de crédito, endereços, dentre outros.

Todavia, sua utilização pode estar relacionada a situações onde a privacidade e a proteção a dados pessoais correm risco de ameaça, motivadas pela reciclagem e a reutilização

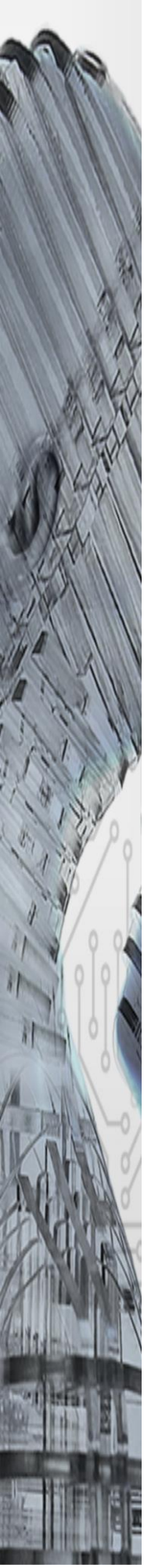


de informações, tendo estas também valor econômico e comercial, de modo que o precificação realizada sobre os mesmos e sua possível perda e a reprodução indevida ou não autorizada representam atividades ilícitas, em um ambiente pouco regulamentado de modo específico. Assim, a seção é encerrada perfazendo uma análise sobre a segurança em dados e a privacidade à luz dos Direitos Humanos e Constitucionais Fundamentais, como oportunidade de conscientização através da educação taxonômica, econômica, normativa e sobre riscos quanto à gerência de dados pessoais e a autodeterminação informativa[12], como formas de reafirmar a liberdade de expressão, pensamento e a dignidade da pessoa humana na Era Digital.

A seguinte seção, de número 3 e intitulada "A proteção de dados pessoais como um direito em positivação", traz a comento o desenvolvimento e o exercício jurisdicional sobre dados na perspectiva internacional, mediante o mapeamento das normas constitucionais e infraconstitucionais sobre a proteção de dados e o acesso à informação em países ordenados juridicamente pelos modelos de *Civil Law* e de *Commom Law*. Para tanto, as análises realizadas nas subseções de mesma origem também abordam os países com legislações mais modernas, conscientes e eficientes sobre a proteção de dados pessoais, principalmente sob o enfoque dos Direitos Humanos e Constitucionais Fundamentais, de forma a serem apresentados dispositivos constitucionais e infraconstitucionais, além dos regulamentos em proteção de dados pessoais, nas realidades jurídicas de alguns países da Ásia, África, América Latina, como também nos Estados Unidos da América e no Canadá e, em caráter pormenorizado, no âmbito da União Europeia, tendo em vista o advento do Regime Geral sobre Proteção de Dados – RGPD, sendo comentados os princípios envolvendo o RGPD, suas limitações na ambientação às leis nacionais, nos contextos de aplicação internacionais e os direitos por ele tutelados, além da privacidade, da segurança e da proteção de dados, em decorrência de seu aspecto geracional para com a LGPD brasileira.

Em seguida, é estudado o panorama das legislações digitais, virtuais e eletrônicas brasileiras, perfazendo uma conceituação acerca destas subáreas do Direito como disciplinas em construção e sua transversalidade com os demais ramos das Ciências Jurídicas. Desta forma, foi realizado um levantamento das legislações brasileiras mais relevantes que regulamentam a utilização de mecanismos eletroeletrônicos, como o telefone, o *fac-símile (fax),* computadores e o advento do processo judicial eletrônico, em normas que recepcionam a utilização de equipamentos na Administração Pública e nos órgãos provenientes dos

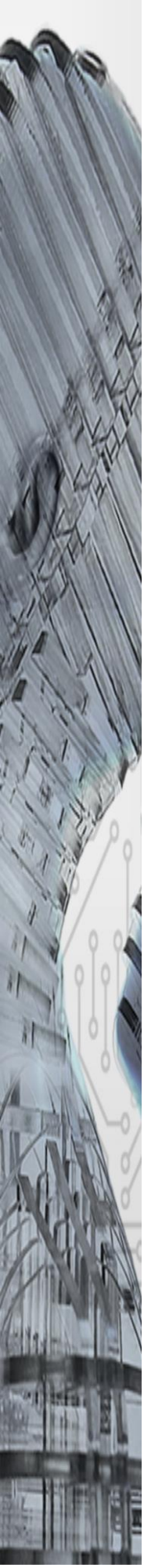
[12] Para Teixeira (2018, p. 103), "Autodeterminação informativa é o direito que cada um tem de controlar e proteger suas informações privadas, podendo ser compreendido como uma extensão do direito à privacidade".



Poderes Executivo, Legislativo e Judiciário para, em sequência, serem comentadas a Lei de Acesso à Informação e o Marco Civil da Internet, como duas importantes normas brasileiras de Direito Virtual e Eletrônico, tutelando as limitações do acesso à informação pública e as relações em ambiente virtual, para então serem introduzidos os estudos e comentários sobre a Lei Geral de Proteção de Dados Pessoais, analisada em detalhes, compreendendo: seus princípios e finalidades, a sua elaboração como medida político-econômica e os seus impactos nas empresas e na Administração Pública. Também é realizada uma análise em perspectiva comparada entre a LGPD e o RGDP, sendo verificadas as suas similitudes e as adaptações introduzidas pelos legisladores brasileiros visando as adequações e melhores ajustes ao ambiente jurídico-normativo nacional. Ao fim dos estudos conglomerados neste eixo seccional, também se busca comparar os escopos, limites e finalidades entre a Lei de Acesso à Informação e a LGPD, sob o prisma do interesse público e a segurança jurídica objetivada por ambas as legislações, com o objetivo de perceber formas de harmonização entre as duas normas e suas formas de aplicação visando a proteção do cidadão como fonte principal do chamado "interesse público".

A seção de número 4 trata da "Jurisdição na proteção de dados pessoais", tendo por escopo, no primeiro momento, a perspectiva do Direito Internacional Público e Privado, para compreender a possibilidade de sobreposição de normas internacionais às nacionais e vice-versa, no plano das Leis de Proteção de Dados Pessoais, sobretudo, em relação aos Direitos materiais e processuais Cíveis e Direitos Constitucionais. Portanto, são apresentadas as bases, os princípios e as regras comuns e internacionalmente aceitos, os quais são similarmente compreendidos e aplicados em sistemas jurídicos de *Commom Law* e *Civil Law*, retratando as adequações do modelo clássico de jurisdição para o panorama jurídico das Leis de Proteção de Dados Pessoais. Nas subseções, também são realizados os enfrentamentos a respeito da Jurisdição Exorbitante e dos possíveis desdobramentos da Jurisdição Transfronteiriça ou Jurisdição *cross-border*.

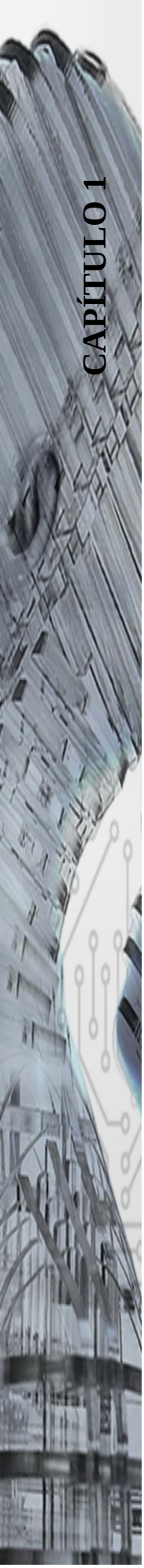
Na continuidade, são abordadas as perspectivas em jurisdição à luz da LGPD, tendo em vista a sua positivação através do diálogo entre fontes normativas, de forma a condensar as taxonomias provenientes das TICs e de proteção de dados às suas funções no ambiente jurídico prático, considerando os problemas surgidos em decorrência da coleta e do tratamento de dados por empresas físicas e virtuais, bem como pela Administração Pública, nas perspectivas nacionais e internacionais. O exame judicial preliminar dos critérios de admissibilidade e as possíveis formas de processamento são discutidos, como também as



formas mais adequadas para fixação da competência jurisdicional, sendo realizada uma abordagem voltada às leis e doutrinas nacionais, bem como apresentando formas possíveis de resolução de conflitos na esfera Administrativa e extrajudicial, no escopo reiterado de garantir maior amplitude de compreensão sobre a temática e a reafirmação da proteção aos Direitos Humanos e Constitucionais Fundamentais, quer por agentes públicos, quer pela iniciativa privada, em relação aos titulares de dados e cidadãos, de modo geral.

A última seção, de número 5, apresenta as "Conclusões", realizando uma retomada dos objetivos alcançados em sede de pesquisa, onde são elaborados comentários acerca dos dados levantados, fontes de informações localizadas, bem como as percepções advindas de um prisma em desenvolvimento no Direito Brasileiro e formam contrapontos à estrutura tradicional das relações, em complementariedade a toda a construção científica desenvolvida em prol das percepções alcançadas.

A importância do tema requer estudo detalhado e contínuo, que certamente não fica esgotado aos apontamentos adiante levantados durante a pesquisa e à pequena contribuição acrescentada aos estudos sobre Direito Virtual e Eletrônico na perspectiva do exercício jurisdicional quanto ao acesso à informação e à proteção de dados pessoais como parte integrante do direito fundamental à privacidade, face à sua relevância contextual. Outrossim, visa também oferecer uma fonte de recursos e informações que viabilizem maior compreensão sobre a Proteção de Dados Pessoais como ferramenta de positivação dos Direitos Humanos e ao exercício da Cidadania, desenvolvendo uma conscientização mais aprofundada sobre a responsabilidade de titulares de dados pessoais para com a tutela pessoal de sua intimidade e a autodeterminação informativa - como direitos e liberdades a serem defendidos e promovidos, através da Educação, cujo primeiro passo retrata uma necessidade coletiva de saber e aprender, visando a consolidação de uma infraestrutura social mais ética e capaz de fortalecer o Estado Constitucional Democrático e a dignidade da pessoa humana, como um direito realmente inalienável.



CAPÍTULO 1

GLOBALIZAÇÃO DA INFORMAÇÃO: PERFIS DE PROTEÇÃO DE DADOS E A ECONOMIA DIGITAL

Desde o aparecimento da escrita, o ser humano manipula a informação, que é traduzida por dados, mais ou menos estruturados. Comparado à invenção da imprensa por Guttemberg em meados do século XV, "o advento da ciência da computação, no final dos anos de 1940 nos Estados Unidos e na Inglaterra, introduziu a forma digital de armazenamento e transferência de dados, gravada em mídia eletrônica" (WAZLAWICK, 2017, p. 19).

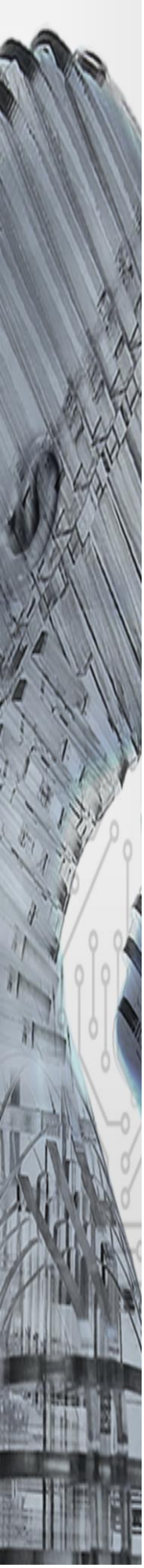
Em 1973, o sociólogo estadunidense Daniel Bell (1973), cunhou o conceito de "Sociedade da Informação" para delinear o grupamento social onde o eixo das relações de trabalho e o consumo ocorrem com base em conhecimentos teóricos, de modo que outros elementos de produção perdem a relevância. Assim, "o conhecimento teórico (*know-how)* passa a ser fonte de poder dentro da sociedade da informação, preterindo os modelos tradicionais de poder religioso, econômico ou sobre a terra" (TAPSCOTT, 1997, p. 18). A globalização da informação, como fenômeno de difusão de informações e dados em tempo real, através da Internet, oportunizou o surgimento de um mercado virtual, cujos três elementos nos quais se pavimentam são: Internet, Sociedade da Informação e Economia Digital.

A Internet representa o ambiente natural onde ocorrem as relações digitais dentro da "sociedade da informação", sendo formado por "um conjunto descentralizado de redes de comunicação interconectadas utilizando protocolos TCP/IP[13]" (ANGHERN, 1997, p. 361), de modo a garantir redes físicas heterogêneas em funcionamento como uma única rede lógica de alcance global, também figurando como "a maior plataforma com arquitetura aberta para troca de informações" (BOSTROM, 2014, p. 48-49). Neste sentido, Hermann-Joseph Blanke e Ricardo Perlingeiro apresentam os seguintes comentários, *in verbis:*

> O significado da internet está inseparavelmente entrelaçado com o significado dos dados para as sociedades do século XXI. Os dados digitais, em particular, como uma base importante para a pesquisa e a construção de opinião, bem como para a tomada de decisões, têm sido repetidamente chamados de "combustível do futuro" ou "novo petróleo". (BLANKE; PERLINGEIRO, 2018, p.09, tradução nossa[14])

[13] Os protocolos de interconexão, ou comunicação em rede, TCP/IP são distintos entre si e representam formas de linguagens de comunicação utilizadas entre computadores, permitindo a troca de informações. TCP significa *Transmission Control Protocol* (Protocolo de Controle de Transmissão) e o IP, *Internet Protocol* (Protocolo de Internet).

[14] Do original, em inglês: "*The significance of the internet is inseparably intertwined with the significance of data for the societies of the twenty-first century. Digital data, in particular, as an importante foundation for*



Segundo Elianete Vieira (2013, p. 29), o conceito de sociedade da informação possui "íntima relação com a globalização e com a expansão da utilização dos recursos de telefonia, satélites, radiodifusão e Internet, no final do século XX", quando passou-se a ter acesso quase imediato a informações e dados produzidos, publicados e armazenados, em muitas localizações do planeta. Para Frank Webster (2002, p. 64), "o uso de dados na sociedade da informação tornou-se parte integrante da economia moderna, ao possibilitar a criação de novos modelos de negócio, mercados, serviços e produtos", bem como a fomentar a pesquisa científica e aprimorar máquinas, através do desenvolvimento de inteligências artificiais. No mesmo sentido, Laura Mendes complementa o entendimento, *in verbis:*

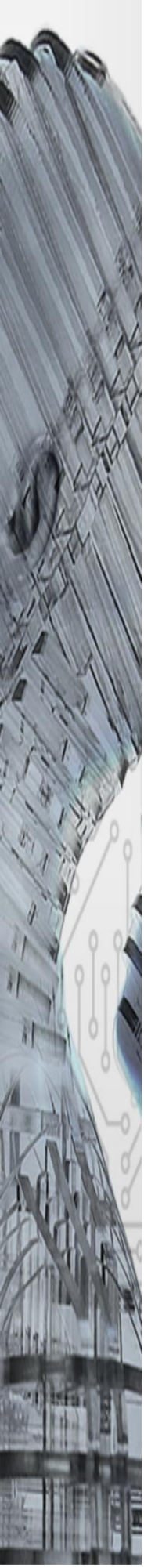
> Nos mais diversos papeis sociais como contribuinte paciente, trabalhador, beneficiário de programas sociais ou como consumidor, o cidadão tem seus dados processados diuturnamente. A vigilância deixa de ser esporádica e torna-se cotidiana. A utilização massiva de dados pessoais por organismos estatais e privados a partir de avançadas tecnologias da informação apresenta novos desafios ao direito à privacidade. A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos e a construção de verdadeiros perfis virtuais, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais. (MENDES, 2014, p. 81)

Estas novas ferramentas proporcionaram o "surgimento e expansão da Economia Digital" (WALDFOGEL; PEITZ, 2012. p. 34), como sendo um dos setores de macroeconomia. Com características inovadoras sobre a forma de produção e negociação mediante procedimentos simplificados, "a economia digital também minimiza o emprego de materiais físicos e papeis, pois gera informações eletrônicas, em formas de "*bits*" armazenados em nuvens de dados" (MATTERN, 2008, p. 29), cujo acesso ocorre em grande velocidade.

A Economia Digital compõe setor autônomo e campo recente, abarcando tanto os mercados tradicionais quanto os desenvolvidos em ambiente virtual, pela Internet. A via para que os bens de consumo sejam apresentados aos potenciais consumidores é a publicidade, "costumeiramente tratada como *marketing* virtual, neste novo espaço de compras, vendas, trocas e prestações de serviços" (TAPSCOTT, 1997, p. 64). Assim, diversos produtos, físicos e virtuais, podem ser comercializados pela Internet, em moedas nacionais, cartões bancários ou através das chamadas "criptomoedas" ou *webcoins*, "já perfazendo um montante de cerca de 20% da economia global a transitar pelas vias digitais" (CABRAL; YONEYAMA, 2001, p. 35).

---

research and opinio-building, as well as baisis for decision-making, has repeatedly been called the "fuel of the future" or "the new petroleum". *In: The Right of Acess to Public Information*, Springer, 2018.

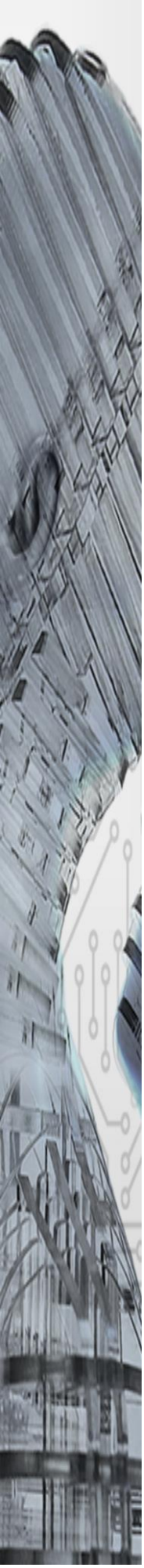


A normatização, a regulação e a tributação compõem subáreas da economia digital, nos campos socioeconômicos e geopolíticos, ainda discutidas com prioridade relativamente reduzida em projetos de Lei e regulamentos de Agências e entidades governamentais, tanto no Brasil quanto em diversos países - de modo a não estar em vigor uma grande quantidade de normas, princípios e regras especificamente voltadas para a organização e fiscalização dos fenômenos derivados do mercado virtual, sobre as negociações de produtos exclusivamente eletroeletrônicos, bens de consumo, moedas digitais e dados pessoais, os quais podem produzir evasões fiscais diárias, muitas vezes passando despercebidas, dentre outras ocorrências (FARIA; MONTEIRO; SILVEIRA, 2018, p. 24 - 45), caracterizando ilicitudes cíveis, criminais e ou administrativas. Na mesma esteira, as trocas multidisciplinares entre pessoas e organizações, promovem a criação de novos modelos de negócios e a geração de riquezas em escala global, bem como exigem a adequação de sistemas normativos e técnico-jurídicos capazes de gerir estas novas relações econômicas e financeiras, nos ambientes digitais.

As questões geopolíticas abrangidas pelo mercado digital têm como exemplo a organização legislativa e econômica visando o aprimoramento do Mercado Único Digital (HAUNTS, 2018, p. 12 - 14), no âmbito da União Europeia, cujos esforços são conduzidos pela Comissão Europeia, comas finalidades principais de redução dos entraves aduaneiros e o "aumento de oportunidades de circulação de capitais, bens, produtos e serviços em toda a União Europeia de forma legal, segura, protegida e a preços acessíveis, principalmente no setor de vendas internacionais realizadas por pequenas e médias empresas" (*Ibidem*), além de promover a harmonização das legislações nacionais e a ampliação de direitos sobre a proteção de dados pessoais através de um Regulamento Geral. Assim sendo, a Comissão tem como objetivo "criar um mercado único digital no qual os cidadãos e as empresas possam aceder ininterruptamente e de forma equitativa a bens e serviços comercializados de maneira digital, independentemente da sua nacionalidade ou da localização onde residem" (BECKER, 2018, p. 22).

Segundo o Relatório *Contribution Of The European Structural And Investment Funds To The 10 Commission Priorities Digital Single Market* (2015), os resultados pretendidos pelo fortalecimento de um mercado digital único compreendem: (I) o incentivo à criação de novas *startups*[15], num mercado de cerca de 500 milhões de pessoas; (II) o impulso

[15] Uma *startup* é uma empresa que está no primeiro estágio de suas operações. Essas empresas geralmente são financiadas inicialmente por seus fundadores empreendedores, à medida que tentam capitalizar o desenvolvimento de um produto ou serviço para o qual acreditam que há uma demanda. Devido à receita



ao comércio eletrônico na UE, solucionando o problema do bloqueio geográfico e tornando mais acessível e eficiente a entrega de encomendas noutros países; (III) a modernização da legislação europeia sobre direitos de autor em plataformas digitais; (IV) a atualização da legislação europeia aplicável ao setor audiovisual e a criação de condições equitativas para as fontes digitais comparáveis, combatendo os conteúdos ilegais em linha e protegendo os utilizadores mais vulneráveis; (V) a intensificação da resposta da Europa a ciberataques mediante a consolidação da *European Union Agency for Network and Information Security* - ENISA, a agência europeia de cibersegurança, e a criação de uma estratégia eficaz europeia de dissuasão no domínio da cibersegurança e de uma resposta em matéria de direito penal para melhor proteger os cidadãos, as empresas e as instituições públicas.

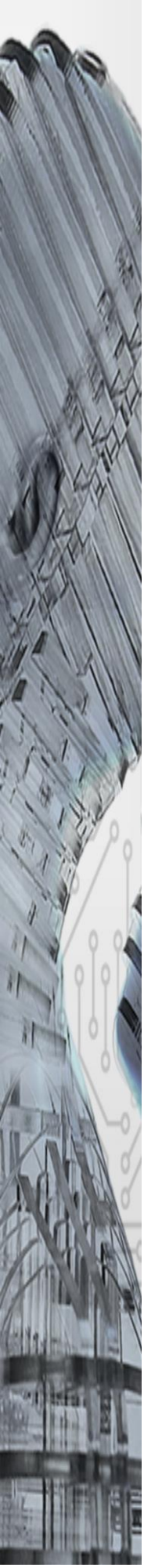
Todavia, a proteção de dados na economia digital fundada na sociedade da informação exige que as empresas, públicas e privadas, estejam melhor preparadas no setor de segurança da informação, "criando mecanismos e programas capazes o suficiente de garantir a devida proteção aos ativos intangíveis e à segurança esperada na manutenção dos dados pessoais de clientes e usuários" (WAZLAWICK, 2017, p. 44), bem como cabem aos governos a elaboração e a aplicação de leis de proteção de dados pessoais que fixem níveis de exigência e tutelem direitos, a fim de pavimentarem uma consciência comum a respeito de segurança, privacidade e proteção de dados como critérios básicos a serem disponibilizados por organizações públicas e privadas.

Nesta perspectiva transversal, as Leis de Proteção de Dados Pessoais, tem por escopo garantir a segurança de dados, enquanto viabilizam maior licitude aos modelos de negócios envolvendo informações pessoais de usuários, pois, conforme comenta Tarcísio Teixeira, *in verbis:*

> Ocorre que todos esses fatores têm trazido grande preocupação, em vista da enorme quantidade de dados que circulam na internet, das constantes e rápidas mudanças, especialmente para quem utiliza a internet, seja para fins pessoais, empresariais ou governamentais. Isso gera sério receio na sua utilização diante de tantos problemas causados. Concomitantemente, a preocupação do jurista aumenta na medida em que as infrações legais se multiplicam e passam a ser cada vez mais constantes no ambiente virtual. (TEIXEIRA, 2018, p. 88)

As leis de proteção de dados também viabilizam "parâmetros legais mais claros às formas como o comércio digital, realizado por empresas varejistas, armazenam dados como endereço e números de cartões de crédito" (BLUM, 2018, p. 26). Assim sendo, é importante que a sustentabilidade econômica no ambiente virtual seja mantida e aprimorada, enquanto as

limitada ou altos custos, a maioria dessas operações de pequena escala não é sustentável em longo prazo sem financiamento adicional de capitalistas de risco.



empresas se adaptam para estar em conformidade com as diretrizes da proteção de dados pessoais.

Todavia, as legislações de proteção de dados trazem consigo novas nomenclaturas e termos técnicos provenientes de áreas como a Ciência da Computação, a Informática e as TIC's, outrora distantes às realidades profissionais e acadêmicas da maioria dos operadores de Direito, dos Regimes Jurídicos nacionais e do público em geral, que doravante necessitam aprender a conviver e aprimorar compreensões na busca pela positivação de seus direitos à intimidade, à privacidade e à dignidade, em um momento onde a economia e as facilidades do comércio virtual favorecem o consumo e a difusão de dados pessoais, como também diminuem, ou relativizam, a inalienabilidade de Direitos Humanos e Constitucionais.

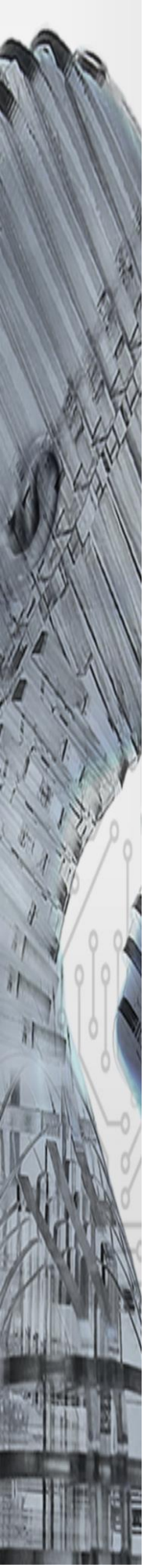
A proteção de dados como direito tutelado no ordenamento jurídico brasileiro pela Lei nº 13.709, de 14 de agosto de 2018 – a Lei Geral de Proteção de Dados Pessoais, ou LGPD (BRASIL, 2018), traz em seu bojo terminologias, princípios e, sobretudo, objetivos que abrangem um contexto imerso na ciência da informação, na linguagem computacional e na cibernética[16], os quais devem ser visitados em sede preambular, visando estabelecer critérios de acessibilidade e compreensão pormenorizada dos componentes e objetos de discussão suscitados ao longo do desenvolvimento textual.

Esta nova lei representa uma mudança radical na forma como a privacidade dos indivíduos é tratada no Brasil. Os indivíduos, representados como "titulares de dados" cidadãos e residentes no Brasil, doravante desfrutarão de maior controle legalmente amparado e autonomia sobre seus próprios dados pessoais, os quais só podem ser coletados, tratados, processados[17] e armazenados sob as regras rígidas impostas pela LGPD. Essas regras estão alinhadas com os padrões internacionais mais atualmente vigentes sobre proteção de dados pessoais.

A LGPD, em vigor a partir de agosto de 2020, concedeu às empresas e organizações brasileiras um período de transição adequado (dois anos) para adotar as novas regras. Apesar de a LGPD não fazer distinção entre dados pessoais físicos e digitais, ou digitalizados, o processamento de qualquer informação pessoal passa a obedecer aos institutos dispostos em

[16] O termo "cibernética" vem do grego Κυβερνήτης e se refere ao estudo de sistemas interdisciplinares de gestão e controle e comunicação em sistemas físicos, sociais e virtuais. A cibernética pode ser utilizada como forma de análise (controle) de sistemas e situações que contam com variáveis, como a economia, a meteorologia e as experiências científicas, perfazendo constatações probabilísticas.

[17] Embora "o uso difundido do termo processamento de dados date somente dos anos 50, as funções de processamento de dados foram executadas manualmente por milênios" (WAZLAWICK, 2017, p. 19). Por exemplo, a contabilidade envolve funções como lançar transações e produzir relatórios como o balanço patrimonial e a demonstração do fluxo de caixa. Métodos completamente manuais foram aumentados pela aplicação de calculadoras mecânicas ou eletrônicas (FRENCH, 1996, p. 22).



lei, com impactos diretos na responsabilização de instituições públicas e privadas, bem como em seus respectivos agentes, de forma mais específica. Mas, afinal, quais são o(s) sentido (s) e significado (s) taxonômicos de terminologias importadas das Ciências da Computação e da Informática, à luz das Leis de Proteção de Dados Pessoais e em quais ambientes (onde) ocorrem a coleta de dados, demonstrando quais são as finalidades de sua utilização e como podem ocorrer as principais violações a dados pessoais?

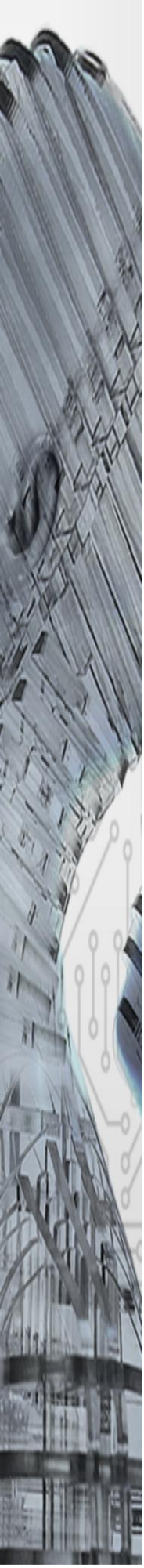
1.1 Dados Digitais: Coleta, Processamento e Tratamento

Com o advento da computação, os dados físicos têm sido paulatinamente substituídos por dados digitais[18] e metadados[19], todavia, documentos pessoais e públicos, processos judiciais, prontuários médicos, relatórios empresariais, e comunicação por correspondências (*e.g*. cartas, boletos bancários e de tributos), dentre outros, "continuam sendo utilizados e carregam consigo informações de cunho pessoal, particular ou, até mesmo, sigiloso" (PINOCHET, 2014, p. 39). Já os dados digitais, na teoria da Tecnologia da Informação e da Comunicação, "são informações apresentadas de forma descontinuada, através de letras, ícones e números, ou continuamente, como em sons e imagens" (WASLAWICK, 2017, p. 30). Nesta forma, "os dados podem ser mais facilmente lidos ou armazenados por computadores ou outros equipamentos de processamento de sinais digitais" (SMITH, 2003, p. 55). Para receber dados digitais, estes devem primeiro ser digitalizados. Posteriormente, eles podem ser transferidos e armazenados de forma eficiente e tolerante a falhas, em dispositivos e equipamentos variados.

Coloquialmente, "os dados digitais são frequentemente entendidos como documentos digitais, imagens e vídeos" (PINOCHET, 2014, p. 32). Neste sentido, os dados pessoais,

[18] Dados digitais são informações processadas ou armazenadas por um computador. É composto de dígitos binários, uma combinação de zeros e uns. Processados por um computador, esses zeros e uns compõem dados, que nos aparecem como texto, imagens, programas de *software*, clipes de áudio e documentos, entre outros tipos de informações. Como todos os computadores usam a mesma linguagem binária, podemos transferir dados digitalmente de um computador para outro. Cada interação com dispositivos gera dados digitais. Cada toque no telefone, clique no computador, compra *on-line, e-mail* ou publicação em mídia social. Mesmo indo ao trabalho ou à escola, o deslocamento do telefone gera dados.

[19] Os metadados são um tipo específico de informação que fornece contexto sobre os próprios dados. Por exemplo, quando uma foto é tirada com um telefone, este arquivo cria dados de imagem. Esta é a foto em si. Mas também são conjuntamente criados metadados sobre a foto: quando foi tirada, onde foi tirada, qual dispositivo tirou a foto e muito mais. É possível contar muito sobre uma pessoa apenas pelos metadados que ela produz. Por exemplo, se os dados de e-mail de uma pessoa estiverem protegidos por criptografia, ninguém poderá ver o conteúdo desses e-mails. Mas se alguém puder monitorar os metadados, verá que a pessoa recebe e-mails mensais de amigos, colegas de trabalho e empresas. O acesso a grandes quantidades de metadados de alguém pode criar uma imagem detalhada da rede social, interesses, política, crenças e muito mais.



conforme trata a Lei nº 13.709/2018 (BRASIL, 2018), referem-se à "meta-informação que pôde ser produzida de forma física ou digital, esta última armazenada em computadores e em bases de dados" (CAPURRO; HJØRLAND, 2007, p. 157), "acessíveis mediante o uso da rede mundial de computadores, e que podem fornecer informações capazes de individualizar o titular" (BOURGUE; CLARK, 2006, p. 81).

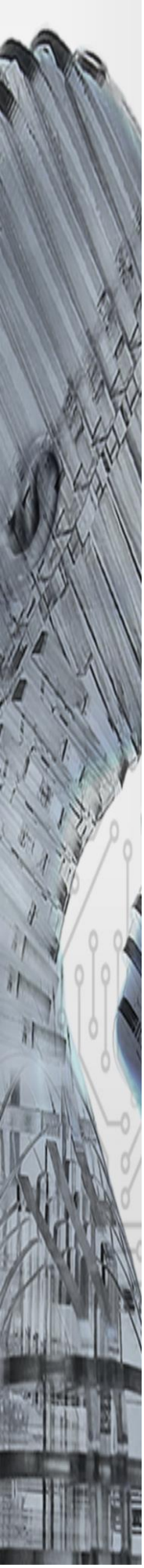
Basicamente, a criação de dados ocorre na memória do computador, onde as instruções básicas dos programas operacionais são armazenadas, sendo processadas por equipamentos de *hardware*[20], *software*[21] e sistemas, de forma a não ser possível lidar com segurança de dados, sem recordar deste aspecto fundamental (SMITH, 2003, p. 27 - 52).

Nos vários tipos de *hardware* de computador (com seus periféricos), de supercomputadores a microcomputadores, via *mainframes*[22] e sistemas abertos, será necessária a utilização dos seguintes tipos de mídia física: (I) a memória do computador; (II) os discos, armários (dispositivos) para backup e armazenamento e; (III) os sistemas de arquivamento (FRENCH, 1996, p. 26). Assim sendo, os dados podem fluir entre esses sistemas em redes físicas de comunicação, redes de telecomunicações, redes locais e as redes de telecomunicações por satélite.

Nos suportes físicos, "devem ser implementados sistemas que gerenciam o acesso e processamento de dados: o acesso lógico desses sistemas pode ser do tipo sequencial ou indexado" (FRENCH, 1996, p. 68), "sendo os arquivos mais frequentemente substituídos por bancos de dados que permitem acesso e atualizações mais avançadas, mediante conexão em linha" (WAZLAWICK, 2017, p. 34).

Os sistemas de gerenciamento de banco de dados (SGBD) em nível de *software*, "permitem que o computador possa gerir os diferentes tipos de processamento dos dados, executando-os e modificando-os (WAZLAWICK, 2017, p. 35). Segundo a conceituação apresentada pelo art. 5º[23], incisos I, II e III, da Lei nº 13.709, de 14 de agosto de 2018, os

[20] Termo da linguagem computacional de origem anglófona, que designa os componentes físicos de equipamentos eletrônicos, caracterizados como peças.
[21] Termo de linguagem computacional de origem anglófona, que designa os componentes imateriais ou os programas, manuais e especificações de uso por meio dos quais os equipamentos podem ser operados, mediante comandos capazes de alterar ou produzir dados.
[22] Computadores de grande porte capazes de armazenar alto volume de dados e processar contingente elevado de informações, em comparação com equipamentos de uso pessoal.
[23] Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;



dados podem ser: (I) pessoais; (II) sensíveis (de caráter público ou privado); e (III) anonimizados (BRASIL, 2018). Para Rita Blum os dados sensíveis podem ser compreendidos como:

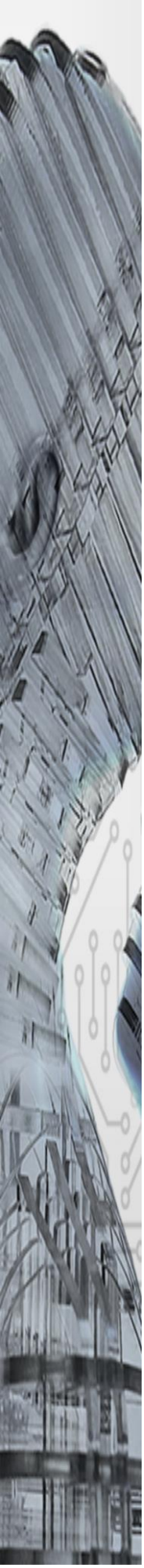
> [...]aqueles que se referem às convicções filosóficas, morais, sociais, políticas e sindicais, religiosas, questões de origem social e ética, vida sexual, orientação sexual e à saúde, incluindo, mas sem limitação, dados genéticos da pessoa. Os dados sensíveis são, sem dúvida, constitucionalmente protegidos pelo "manto" do direito à privacidade (direito fundamental de qualquer brasileiro ou estrangeiro residente no país. BLUM, 2018, p. 168).

Deste modo, "a proteção de dados pessoais possui objetivos específicos, levando em consideração a perspectiva da teoria da Tecnologia da Informação e da Comunicação" (FRENCH, 1996, p. 38), onde se fundam as principais diretrizes das empresas voltadas para a criação de programas de computador e as políticas de armazenamento de dados, figurando a segurança no posto principal, conforme melhor se explica adiante.

A respeito da titularidade, é possível a discussão acerca do crescente valor econômico dos dados pessoais digitais e sua regulamentação legal para uso e exploração, considerando a propriedade no sentido legal (VENOSA, 2016, p. 72 - 81)[24], apenas de modo tangível. Em muitos casos, no entanto, a noção de bens (também, mas não limitada a dados digitais) na linguagem geral, é equiparada ao acesso e ao poder de descarte, "considerando que os arquivos e registros digitais podem ter conotação econômica ou não" (TEIXEIRA, 2018, p. 102 – 103). O papel do chamado proprietário ou titular dos dados é independente da questão da propriedade – que descreve a responsabilidade, por exemplo, pela garantia de qualidade de determinados dados coletados, tratados e armazenados por empresas.

O tratamento de dados advém do processamento de dados, geralmente realizado mediante "a coleta e manipulação de itens de dados para produzir informações significativas" (FRENCH, 1996, p. 42). Nesse sentido, pode ser considerado "um subconjunto de processamento de informações, que produz a subscrição e a mudança (processamento) de informações de qualquer maneira detectáveis por um observador" (SMITH, 2003, p. 34), em bases físicas ou digitais.

[24] Segundo Venosa (2016, p. 72 - 81) a "propriedade compreende o direito, exercido individualmente ou por organizações, de fruição por sobre o bem móvel, imóvel ou semovente, sendo garantida a posse, a detenção e a manutenção da coisa, bem como o seu uso, gozo e direito de disposição, além do direito de reavê-la de quem a tenha injustamente se apropriado". O direito de propriedade, como instituto jurídico, está inserido na Constituição brasileira através do artigo 5°, nos incisos XXII, XXIII. XXIV, XXV, XXVI, XXVII, XXVIII, XXIX, XXX e XXXI (BRASIL, 2018).



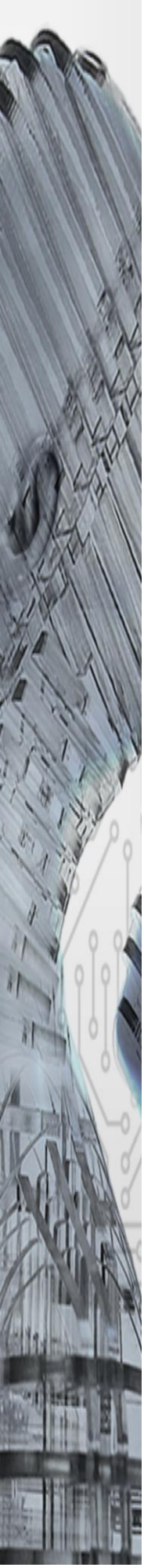
Se o objetivo não é apresentar resultados para um usuário humano, “o propósito do processamento de dados é geralmente fornecer informações de nível superior ou melhores informações para outra ferramenta de processamento ou análise” (HUDAK, 2006, p. 38). Esse “processamento de informações pode ser uma questão de fusão de dados, extração de informações ou transformação de representação” (BOURGUE; CLARK, 2006, p. 66). Por exemplo, a fusão pode envolver a combinação de várias fontes de dados para compilá-las em informações mais seguras, e a recuperação pode ser um processo de semantização ou síntese de dados. “O conjunto de ações realizadas em processamento de dados de um sistema compõem o sistema de informação” (WAZLAWICK, 2017, p. 21).

Geralmente, o termo "processamento de dados" tem aplicação análoga à semântica proposta em “tratamento de dados’ e refere-se a qualquer processo que converta dados de um formato para outro, que deve ser chamado de “conversão de dados” (BOURGUE; CLARK, 2006, p. 57 - 65)”. De acordo com essa visão, os dados podem ser convertidos em informação e vice-versa (FRENCH, 1996, p. 43). O “objetivo da conversão de dados não é responder a uma pergunta, mas apenas facilitar a execução de algoritmos” (SMITH, 2003, p. 37). Por exemplo, a informação pode ser uma cadeia de caracteres que forma uma sentença inteligível para o humano e que lhe permite entender os parâmetros do material por ele observados, mais frequentemente constituídos por sequências de figuras (*e.g.:* letras, algarismos, imagens)

A LGPD (BRASIL, 2018) apresenta o “tratamento de dados” em seu art. 1º[25]como a *cellula mater* de toda a lógica jurídica pretendida em seu escopo de regras e princípios e complementa a definição do tratamento, conforme o inc. X do art 5º[26], onde encontra-se especificado um rol taxativo das espécies de manejos e operações realizadas com dados pessoais. É na ação de tratamento de dados, desde o instrumento de cessão, à coleta de informações, passando pela guarda, conservação e manutenção, até os objetivos finais da sua utilização, que se fundamenta toda a moldura normativa envolvendo a proteção de dados, como setor de atenção e matriz de todos os conflitos advindos da inobservância de critérios que se vinculam ao tratamento, tais como a segurança e as formas de armazenamentos, conforme estudado a seguir.

[25] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018, *grifo nosso*).

[26] Art. 5º caput [...]
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 (BRASIL, 2018).



1.2 Segurança de dados

Devido ao potencial dos dados para fornecer uma grande quantidade de informações diversificadas sobre o contexto ao qual se referem, "não são principalmente os dados em si que precisam ser protegidos, mas o assunto ou o conteúdo dos dados" (HUNTER, 2018, p. 19). A proteção de dados pessoais visa "proteger os indivíduos de quem os dados se originam, em particular para proteger os seus direitos e liberdades, que podem ser comprometidos como resultado de seus dados serem utilizados de diferentes maneiras" (STAPLETON, 2014, p. 30).

A segurança de dados significa proteger dados digitais, "como aqueles em um banco de dados, contra forças destrutivas e ações indesejadas de usuários não autorizados, como um ataque cibernético[27] ou uma violação de dados" (PINOCHET, 2014, p. 62). Para tanto, é utilizada na maioria das vezes a criptografia[28] de disco, a qual refere-se a uma tecnologia que criptografa dados em uma unidade de disco rígido. "A criptografia de disco geralmente toma forma em *software* ou *hardware"* (CARVALHO; LORENA, 2016, p. 56).

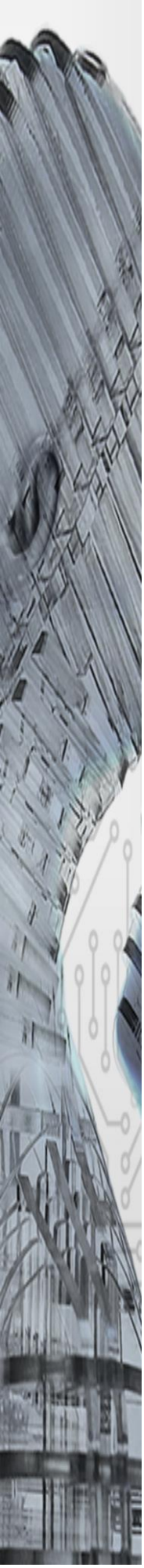
As soluções de segurança baseadas em *software* criptografam os dados para protegê-los contra invasões e roubos. No entanto, um programa malicioso ou um *hacker*[29] *"*pode corromper os dados para torná-los irrecuperáveis, tornando o sistema inutilizável" (CARVALHO; LORENA, 2016, p. 110). As soluções de segurança baseadas em *hardware* podem impedir o acesso de leitura e gravação aos dados e, portanto, oferecer níveis mais abrangentes de segurança e proteção contra adulteração e acesso não autorizado (SMITH, 2003, p. 41).

---

[27] Em computadores e redes de computadores, um ataque é qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo. Um ataque cibernético é qualquer tipo de manobra ofensiva voltada para sistemas de informação de computadores, infraestruturas, redes de computadores ou dispositivos de computadores pessoais. Um invasor é uma pessoa ou processo que tenta acessar dados, funções ou outras áreas restritas do sistema sem autorização, possivelmente com intenção maliciosa. Dependendo do contexto, os ataques cibernéticos podem fazer parte da guerra cibernética ou do ciberterrorismo e ser realizado por estados-nação, indivíduos, grupos, sociedade, agentes individuais, coletivos ou organizações e ter origem em uma fonte anônima, visando roubar, alterar ou destruir um alvo especificado, invadindo um sistema suscetível. Os ataques cibernéticos podem variar desde a instalação de *spyware* em um computador pessoal até a tentativa de destruir a infraestrutura de nações inteiras. Especialistas legais estão procurando limitar o uso do termo a incidentes que causam danos físicos, distinguindo-os das violações de dados mais rotineiras e de atividades mais amplas de *hackers*.

[28] Criptografia, segundo Pinochet (2014), é uma forma de distorcer a organização de dados, de forma a manter as informações em segredo ou ocultas. Existem vários recursos associados à criptografia, como a confidencialidade, que basicamente significa ter certeza de que ninguém verá informações enquanto elas viajam pela rede. Autenticação e controle de acesso também são dois outros recursos fornecidos pela criptografia. Alguns outros recursos fornecidos pela criptografia são o não-repúdio e a integridade de ponta-a-ponta das informações.

[29] Também chamados de "piratas da internet", são indivíduos ou programas de computadores que utilizam inteligência artificial e que têm por objetivo a invasão de dispositivos eletrônicos e a captação de dados, pessoais ou públicos, visando fins diversos, de forma criminosa.



As seguranças baseadas em *hardware* ou assistidas por computadores oferecem uma alternativa à segurança apenas por *software*. Os cartões de acesso (*tokens)* de segurança podem ser mais seguros devido ao acesso físico necessário para serem comprometidos. O acesso é ativado somente quando o *token* está conectado e a senha (ou PIN) correta é inserida, num sistema conhecido como "autenticação de dois fatores". Para tanto, um dispositivo de *hardware* permite que um usuário efetue *login, logout* e defina diferentes níveis de privilégio executando ações manuais (SMITH, 2003, p. 58). Existem também os dispositivos de tecnologia biométrica, voltados para impedir que usuários mal-intencionados consigam efetuar *login* em contas particulares, alterando ou roubando dados (CARVALHO; LORENA, 2016, p. 141 - 149), ou lendo o estado atual de um usuário.

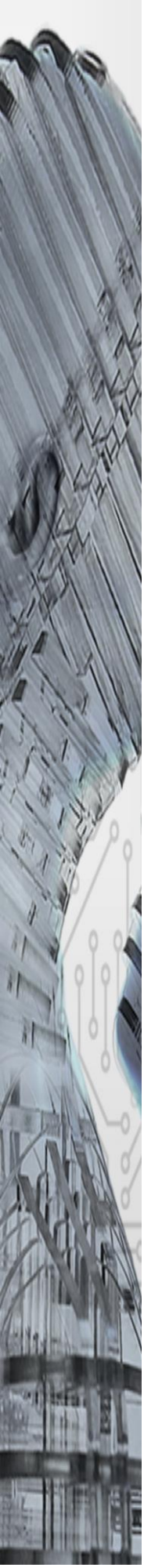
Como "a proteção é baseada em *hardware*, o *software* não pode manipular os níveis de privilégio do usuário sendo pouco possível para um *hacker* ou um programa mal-intencionado obter acesso a dados protegidos (SMITH, 2003, p. 59), por invasão do *hardware* ou realizar operações privilegiadas não autorizadas. Esta suposição é quebrada apenas se o próprio *hardware* for malicioso ou contiver um *backdoor*[30]. O hardware protege a imagem do sistema operacional e os privilégios do sistema de arquivos contra adulterações. Portanto, "um sistema completamente seguro pode ser criado usando uma combinação de segurança baseada em hardware e políticas seguras de administração do sistema" (HUDAK, 2006, p. 71).

O conceito de segurança para os fins cominados na LGPD, encontra-se insculpido em seu artigo 46[31] (BRASIL, 2018) e trata dos critérios mínimos estabelecidos para que a invasão de sistemas e os consequentes roubos ou vazamentos de dados sejam combatidos através da adoção "de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados".

Em diálogo complementar, o § 2º, do art. 46, da LGPD insere a obrigação de que tais medidas de segurança "deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução" (BRASIL, 2018), demonstrando a necessidade de se pensar em

[30] O termo de matriz anglófona pode ser traduzido para o português como "porta dos fundos" e se refere ao mecanismo inserido em alguns programas operacionais onde identificações e senhas de usuários são requisitadas, de modo a permitir o acesso não convencional, mediante a manipulação das barreiras de segurança de programas, arquivos, dispositivos ou funções protegidas.

[31] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.



segurança e mecanismos de proteção, para evitar que os dados deixem o seu local de armazenamento, público ou privado, e passem às mãos de terceiros, para fins diversos.

1.2.1 Confidencialidade, integridade e disponibilidade

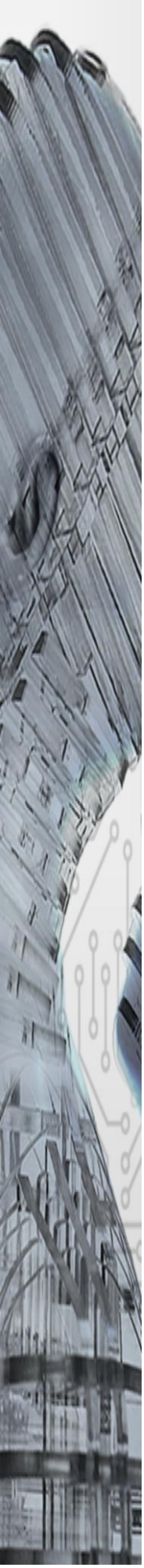
A confidencialidade, a integridade e a disponibilidade, "também conhecidas como "tríade da CIA (*Confidentiality, Integrity, Avaiability*)"[32], representam um modelo projetado para orientar as políticas de segurança da informação dentro de uma organização" (STAPLETON, 2014, p. 35). Os elementos da tríade são considerados os componentes mais importantes da segurança e da proteção de dados.

Neste contexto, a confidencialidade representa um conjunto de regras que limitam o acesso à informação; a integridade é a garantia de que a informação é confiável e precisa, e a disponibilidade é a condição de acesso confiável às informações por pessoas autorizadas (STAPLETON, 2014, p 38 - 42).

A confidencialidade é aproximadamente equivalente à privacidade, representando um conjunto de medidas realizadas para garantir que informações confidenciais não estejam disponíveis a terceiros, "certificando-se de que as pessoas certas podem de fato obtê-las: o acesso deve ser restrito aos autorizados a visualizar os dados em questão" (STAPLETON, 2014, p. 46). É comum, também, que os dados sejam categorizados de acordo com a quantidade e o tipo de danos que poderiam causar, caso viessem a ser manipulados por agentes não autorizados, tal como faz previsão o art. 5º, inc, II, da LGPD brasileira (BRASIL, 2018). Medidas mais ou menos rigorosas podem então ser implementadas de acordo com essas categorias.

A integridade envolve a manutenção da consistência, precisão e confiabilidade dos dados ao longo de todo o tratamento, bem como a fixação de um ciclo da vida que culmina no descarte, com o apagamento do arquivo original e de todas as suas cópias. "Os dados não devem ser alterados em trânsito e devem ser tomadas medidas para garantir que os dados não possam ser alterados por pessoas não autorizadas" (LIBERT, 2004, p. 28), por exemplo, em caso de quebra de confidencialidade. Essas medidas "incluem permissões de arquivos e controles de acesso do usuário" (STAPLETON, 2014, p. 65), com o concomitante controle de versão, usado para evitar alterações errôneas ou exclusões acidentais por usuários autorizados.

[32] Em inglês "*CIA triad*". Às vezes, o modelo também é chamado de "*AIC triad*" AIC (disponibilidade, integridade e confidencialidade) para evitar confusões com a *Central Intelligence Agency*.

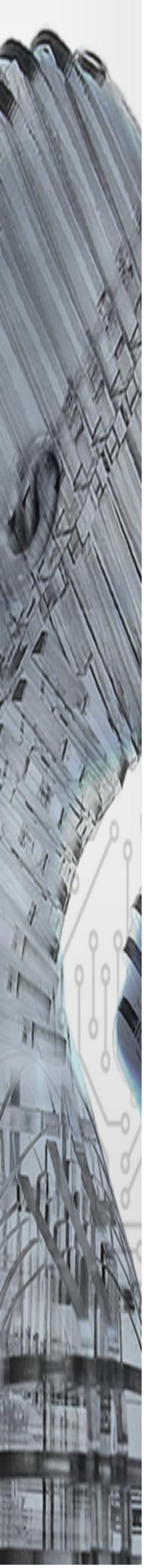


Além disso, alguns meios devem estar em vigor para detectar quaisquer alterações[33] nos dados que possam ocorrer como resultado de eventos não causados por humanos, como um pulso eletromagnético (EMP) ou falha do servidor.

Um servidor da *web* é definido, segundo Pinochet (2014, p. 152 - 167) como "um programa que aceita solicitações de informações emolduradas de acordo com o protocolo HTTP (*Hyper Text Transfer Protocol*)". O servidor processa essas solicitações e envia o documento solicitado. "O acesso à informação é alcançado em duas etapas. Primeiramente, o "usuário" (uma pessoa conectada à Internet) digita as palavras-chave apropriadas utilizadas por um mecanismo de pesquisa para listar um número de servidores que podem armazenar as informações solicitadas" (STAPLETON, 204, p. 54). No segundo estágio, o usuário clica no endereço do sítio eletrônico do servidor em questão e, se a solicitação for válida, as informações são exibidas ou baixadas para o usuário. "No *e-commerce*, tal como no mundo real, as informações são transmitidas e recuperadas até que as partes atinjam o objetivo desejado; por exemplo, concluir um contrato" (MISTRY; DHAVALE, 2011, p. 92).

A disponibilidade garante que as informações e recursos estejam disponíveis para quando usuários autorizados precisarem acessá-los, a qualquer momento, seja em dispositivos físicos ou virtuais. A disponibilidade é mantida quando todos os componentes do sistema de informação estão funcionando corretamente, pois "problemas no sistema de informação podem impossibilitar o acesso, tornando-a indisponível" (STAPLETON, 2014, p. 178). Na tríade da CIA, a disponibilidade está vinculada à segurança da informação, pois medidas eficazes costumam ser capazes de proteger os componentes do sistema e garantirem que as informações estejam prontas para uso.

[33] Alguns dados podem incluir somas de verificação, até mesmo somas de verificação criptográficas, para verificação da integridade. *Backups* ou redundâncias, portanto, devem estar disponíveis para restaurar os dados afetados ao seu estado correto.



1.3 Transferência

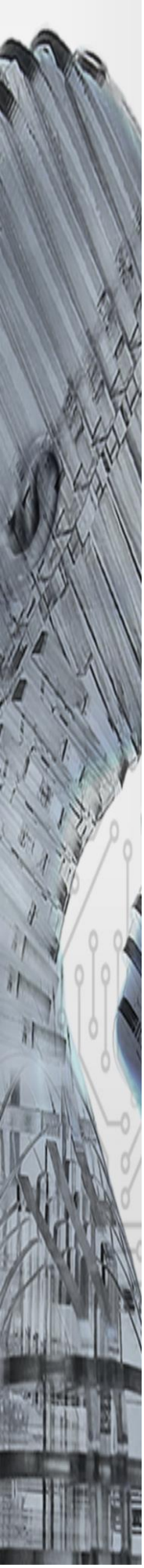
A transmissão de dados (também comunicação de dados ou comunicações digitais) é a transferência de dados em fluxo contínuo de informações digitalizadas (*bits*) ou por via de um sinal analógico digitalizado, através de um canal de comunicação ponto-a-ponto ou ponto-multiponto, os quais podem ser: fios de cobre, fibras ópticas, canais de comunicação sem fio, mídia de armazenamento e barramentos de computador (STAPLETON, 2014, p. 57 - 59). Os dados digitais são representados por sinais eletromagnéticos, como tensão elétrica, radiofrequência (como na tecnologia *bluetooth*), micro-ondas ou sinal infravermelho (BOURQUE; CLARK, 2006, p. 6).

Os dados transmitidos "podem ser mensagens digitais provenientes de uma fonte de dados, por exemplo, um computador ou um teclado" (CARVALHO; LORENA, 2006, p. 94). Também pode ser "um sinal analógico, como uma chamada telefônica ou um sinal de vídeo, digitalizado em um fluxo de *bits*, por exemplo, usando modulação de código de pulso (PCM) ou codificação de fonte mais avançada" (BOURQUE; CLARK, 2006, p. 79), além do modelo tradicional de envio de correspondências ou a reprodução de fotocópias impressas, envolvendo qualquer documento contendo dados pessoais. Assim sendo, "a transferência deve seguir os protocolos de segurança e armazenamento de dados, podendo ocorrer entre bases de dados sediados no mesmo país ou internacionalmente" (STAPLETON, 2014, p. 213).

A LGPD, considera que os dados, como informações pessoais digitalizadas e reduzidas a arquivos em *bits* e armazenados em bases de dados de responsabilidade da instituição pública ou privada que detêm sua guarda, devem atender a uma determinada finalidade de prestação de serviço ou de interesse da Administração Pública (BRASIL, 2018).

1.4 *Big Data*

A todo o instante, milhões de informações em forma de dados digitais são geradas em todo o mundo e "armazenadas para uso posterior por governos (Administração Pública) ou por personalidades jurídicas de direito privado, representadas por empresas dos mais diversos ramos econômicos" (LIBERT, 2014, p. 19). Tais dados contêm os registros produzidos pela atividade humana (*e.g.* científica, comercial, econômica e política) e dados pessoais, como também os registros naturais que ocorrem em todas as áreas do planeta (chuvas, queimadas,



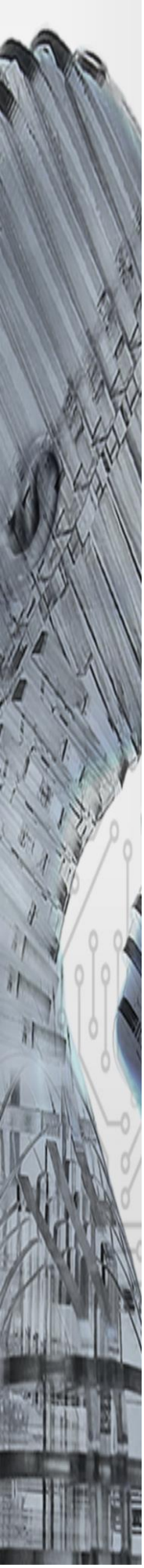
secas, terremotos). Esse "acúmulo de informações, processamento, estudo, comercialização e uso de dados em grande escala é conhecido como *Big Data"* (SCHOLZ, 2014, p. 22).

Os dados depreendidos dos registros de *Big Data* representam não somente uma valiosa fonte de informações para o setor privado, cujos benefícios são colhidos com o seu uso, outrossim podem desempenhar um papel fundamental no desenvolvimento sustentável do sistema administrativo público (GOMES, 2017, 35 - 42), além de possuírem alto valor comercial. A transformação de *Big Data* em dados sustentáveis representa um conhecimento mais aprofundado de fenômenos naturais, econômicos e sociais, dentre outros, ao coletar, cruzar e relacionar informações provenientes de fontes diversas, tais como em fenômenos naturais, com dados sobre componentes sociais (intensidade de consumo de energia elétrica por domicílio, chamadas telefônicas, atividade de redes sociais, uso de transporte, etc.).

Os dados podem ser extraídos "principalmente por fotos de satélite, relatórios econômicos e bancos de dados de acesso livre ou abertos (*open-access),* exigindo colaboração público-privada" (LIBERT, 2014, p. 26). O resultado de cruzar todos esses dados pode ajudar a evitar conflitos geopolíticos, a conhecer o comportamento humano quando ocorrem catástrofes naturais ou crises humanitárias e a compreender a vulnerabilidade e a resiliência em diferentes situações (SCHOLZ, 2012, p. 182 - 188). Como a maioria dos ambientes e indivíduos são afetados por grandes dados, a análise de *Big Data* pode ser aplicada para resolver problemas do mundo real, tendo em vista que a coleta de dados está se tornando cada vez mais avançada, assim como a capacidade humana de analisar e entender grandes quantidades dela.

Dentre as potencialidades de utilização do *Big Data*, está a capacidade de ajudar as empresas a compreenderem e agirem sobre os impactos ambientais de suas operações, diferenciando as ações possíveis entro de seus limites, de outras atividades que estão fora de seu controle direto (WALDFOGEL; PEITZ, 2016, p. 234 - 242). Anteriormente, essas informações "estavam dispersas em diferentes formatos, locais e sítios eletrônicos. Atualmente, as empresas estão tentando identificar o impacto de ponta-a-ponta de suas operações em toda a cadeia de valor" (HAUNTS, 2018, p. 34). Isso inclui contextos, situações e espécies de dados que estão fora de seu controle direto, tais como as fontes de matérias-primas, viagens de funcionários, descarte de produtos e afins.

A utilização de *Big Data* também pode ser integrada em políticas governamentais, para garantir uma melhor regulação ambiental (STAPLETON, 2014, p. 217 - 218). "Os governos podem implementar a mais recente tecnologia de sensores e adotar relatórios em



tempo real dos dados de qualidade ambiental" (SCHOLZ, 2012, p. 189). Esses dados podem ser usados para monitorar as emissões de agentes poluentes por parte de grandes empresas ou instalações de saneamento básico e serviços públicos de saúde e, se necessário, embasar a criação de marcos regulatórios mais coadunados às informações obtidas e, por consequência, mais capazes de trazer melhorias para a coletividade.

Neste sentido, a Organização das Nações Unidas - ONU, lançou o programa *Global Pulse* como uma inciativa que explora como novas fontes de dados digitais e tecnologias de análise em tempo real, podem fornecer uma melhor compreensão das mudanças no bem-estar humano e vulnerabilidades emergentes, face às preocupações e discussões sobre privacidade e proteção de dados e a utilização dos conjuntos de informações de *Big Data* para benefício público, de modo consciente e sustentável, visando a ação humanitária em áreas de alto impacto para governos e. parceiros da ONU. Nesta perspectiva, foram produzidos diversos relatórios, dentre eles os de maior destaque são o *Data Privacy, Ethics And Protection Guidance Note On Big Data For Achievement Of The 2030 Agenda*, que apresenta as principais metas de fortalecimento da segurança em dados e da sustentabilidade da economia digital até 2030 e o *International Data Responsibility Group Annual Report – 2017*, que aborda a produção de dados digitais no desenvolvimento internacional da paz, da justiça e da resposta humanitária.

A utilização de *Big Data* permite a manutenção de um registro completo em como as várias operações de negócios têm impacto sobre o mundo natural, buscando formas inovadoras de sustentabilidade também voltadas às estruturas organizacionais estatais e de tributação (FARIA; MONTEIRO, SILVEIRA, 2018, p. 45 - 68). No mundo dos negócios, o *Big Data* está ativamente "ajudando a criar uma mudança, cortando custos e aumentando a rentabilidade em longo prazo em um mundo com recursos limitados, bem como combinando grandes quantidades de dados de diferentes origens" (WALDFOGEL; PEITZ, 2016, p. 325).

Os desenvolvimentos na área de *Big Data* exigem novos modelos tecnológicos, econômicos e legais, nos quais a reutilização de dados é incentivada, e não prejudicada. "Entre os muitos desafios levantados pelo *Big Data*, a reutilização de dados é uma das mais urgentes" (LIBERT, 2014, p. 222). De uma perspectiva tecnológica, uma condição mínima para a reutilização de dados é uma infraestrutura tecnológica adequada. Obviamente, as abordagens padronizadas na arquitetura das TICs e nos formatos de dados facilitam ainda mais a reutilização de dados e a troca de dados, mas também aspectos como escalabilidade,

agregação, confiabilidade, disponibilidade e segurança são relevantes (BOFF; FORTES; FREITAS, 2018, p. 125 - 143), a fim de se evitar o descaminho de dados pessoais.

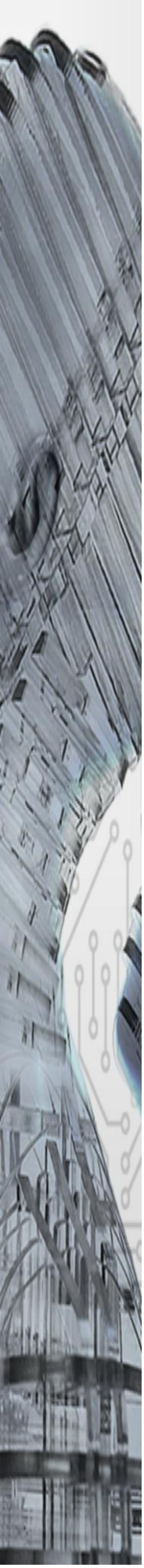
1.5 Armazenamento

A telecomunicação é dominada pelas tecnologias digitais desde 1990, quando passou-se a quantificar, em termos de armazenamento de computadores, o volume aproximado de informações novas e originais (sem contar cópias) criadas no mundo anualmente e armazenadas em quatro mídias físicas: papel, filme, ótica (CDs e DVDs) e magnético. O estudo de Hilbert e López (2011, p. 60 - 65) concluiu que, em 1999, o mundo produziu cerca de 1,5 *exabytes*[34] de informações exclusivas, ou cerca de 250 *megabytes* para cada homem, mulher e criança na Terra. Também constatou que "uma grande quantidade de informação única é criada e armazenada por indivíduos" (o que chama de "democratização de dados") e que "não apenas a produção de informação digital é a maior no total, como é também a que cresce mais rapidamente" (*Ibidem)*.

O armazenamento se refere a um método, associado a um ambiente (físico ou eletrônico), onde os dados poderão ser armazenados. Conforme Peter Lyman e Hal R. Varian (2003) da UC Berkeley apontam no estudo "*How much information* 2003?", foi estimado que a capacidade tecnológica do mundo para armazenar, comunicar e computar informações, acompanhando 60 tecnologias analógicas e digitais durante o período de 1986 a 2003, aumentou em cerca de 30.000%. Em 1986, aproximadamente 1% da capacidade mundial de armazenar informações estava em formato digital; subindo para 3% em 1993, e contando 25% no ano 2000.

Segundo Martin Hilbert e Priscila López (2011), "as armazenagens digitais compunham 97% das informações totais em 2007". Esses números correspondem a menos de três (3) *exabytes* comprimidos em 1986, e 295 *exabytes* comprimidos em 2007. "A quantidade de armazenamento digital dobrou aproximadamente a cada três anos. Em 2007, a humanidade conseguiu armazenar 2,9 × 1020 *bytes* compactados de forma otimizada, comunicar quase 2 × 1021 *bytes* e executar 6.4 × 1018 instruções por segundo em computadores de uso geral" (*Ibidem*). A capacidade de computação de propósito geral cresceu a uma taxa anual de 58%. A capacidade mundial de telecomunicação bidirecional cresceu 28% ao ano, seguida de perto pelo aumento das informações armazenadas globalmente (23%).

[34] Um *exabyte* equivale a: um trilhão (10^{18}) de *bytes*, um bilhão de *gigabytes*, um milhão de *terabytes*, mil *petabytes*.



O relatório *Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper* (2019) aponta uma projeção para o mercado de armazenamento de dados de próxima geração, o qual deverá ser avaliado em 144,76 bilhões de dólares americanos (USD) até 2022, com um crescimento anual médio de 16,76% entre 2016 e 2022. O crescimento deste mercado é impulsionado principalmente pelo volume crescente de dados digitais, aumento da proliferação de *smartphones*, *laptops* e *tablets*, as novas *commodities* de precificação da armazenagem em *datacenters*, e o crescimento do mercado de Internet das Coisas (*Internet of Things* - IoT), que para Eduardo Magrani, *in verbis:*

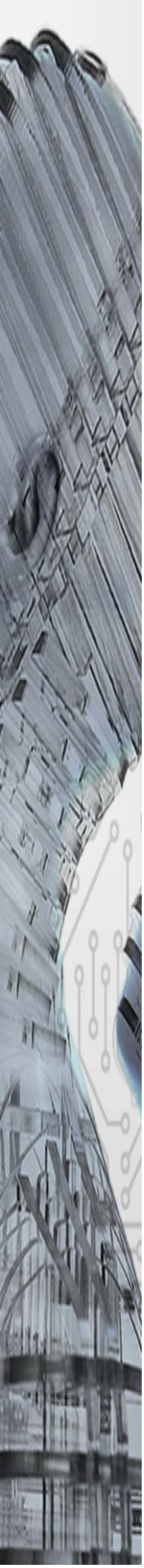
> De maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. (MAGRANI, 2018, p. 20)

As principais tecnologias e produtos futuros, conforme a tendência futura do mercado de armazenamento de dados de próxima geração são o armazenamento de DNA, armazenamento holográfico, replicação controlada em *hashing* escalável (CRUSH) e tecnologia de malha de dados. Com exceção de Códigos de barras e OCR, o armazenamento eletrônico de dados é mais fácil de revisar e pode ser mais econômico do que métodos alternativos, devido à exigência menor de espaço físico e a facilidade na troca (regravação) de dados na mesma mídia (CARVALHO; LORENA, 2016, p. 81 - 89). Entretanto, a durabilidade de métodos como impressão em papel é ainda superior a muitas mídias eletrônicas.

As "limitações relacionadas à durabilidade podem ser diminuídas ou superadas ao se utilizar o método de duplicação dos dados eletrônicos, comumente chamados de cópia de segurança ou *backup"* (STAPLETON, 2014, p. 287). Os *backups* são usados para garantir que os dados perdidos possam ser recuperados de outra fonte. Na opinião de Pinochet (2014, p. 57) "é essencial manter um *backup* de todos os dados na maioria das indústrias e o processo é recomendado para quaisquer arquivos de importância para um usuário".

Ao armazenamento também compreende o apagamento de dados, como sendo um método de sobrescrita baseado em *software* e "destrói completamente todos os dados eletrônicos que residem em um disco rígido ou outra mídia digital para garantir que nenhum dado sensível seja perdido quando uma informação ou dado pessoal for retirado(a) ou reutilizado(a)" (SMITH, 2003, p. 28).

Os ativos intangíveis, como clientes, sistemas e informações, formam a base sobre a qual o valor corporativo é construído. No ambiente de negócios altamente competitivo da



atualidade, “as organizações estão dando maior ênfase à gestão do relacionamento com o cliente como forma de ganhar participação de mercado e diferenciar a qualidade do serviço” (RAMOS *et al.*, 2014, p. 123). Grande parte dos clientes querem escolhas e facilidades de acesso, o que exige que eles forneçam informações e preferências pessoais; enquanto muitas empresas querem ser capazes de coletar dados, minerar e compartilhar essas informações com eficiência. Neste sentindo, complementa Tarcísio Teixeira, nos seguintes termos:

> Em consequência, torna-se necessário que as empresas de provimento de acesso – os provedores – aumentem os seus recursos em termos de processamento, armazenamento e banda de tráfego. Tudo isso tem um custo que, automaticamente, será repassado aos consumidores do serviço. (TEIXEIRA, 2018, p. 64)

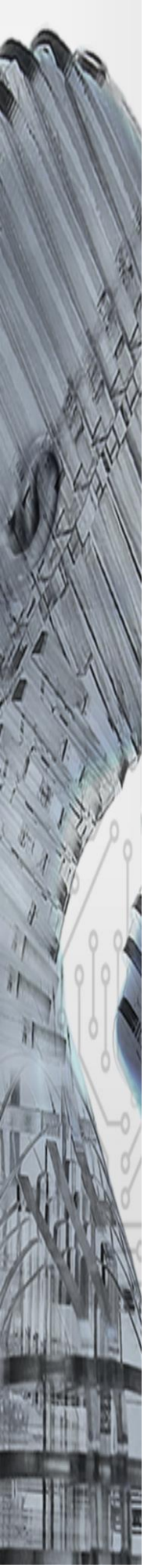
Segundo o relatório da CISCO (2019), dentre os principais problemas relacionados ao tratamento, segurança, transferência e armazenamento de dados, estão: (I) o crescimento contínuo dos volumes de dados, forçando uma certa porcentagem de conjuntos de dados gerenciados pela central (*data center)* a sair do âmbito da proteção; (II) a proliferação de dados "no limite" (escritórios remotos, trabalhadores móveis) que ficam fora do guarda-chuva de proteção de dados e do cobertor de segurança corporativa; (III) as falhas operacionais; (IV) as invasões realizadas por usuários não autorizados (*hackers)*; (V) a variação dos sistemas de proteção que são compatíveis com o grau de criticalidade do conjunto de dados, conforme as leis locais de cada país; (VI) a proliferação de cópias de dados e vazamentos de informações sigilosas e sensíveis; (VII) as taxas de falhas de programas antivírus e salvamento em nuvem; (VIII) a obsolescência de programas e componentes e; (IX) o custo crescente para gerenciar e suportar todos os itens acima.

Para Teixeira (2018, p. 86 - 88), “certos setores, como os serviços financeiros” e de saúde, “geralmente atraem a maior parte da atenção na discussão sobre privacidade por causa das informações pessoais que possuem. No entanto, todos os setores são afetados por requisitos de privacidade e proteção de dados”.

A análise trazida até a presente fase teve por escopo ilustrar e exemplificar os panoramas do ambiente onde as leis de proteção de dados têm aplicação prática, esclarecendo pontos fundamentalmente técnicos para assegurar que as ferramentas básicas de compreensão estivessem disponibilizadas, para então adentrar nas questões críticas a seguir propostas.

1.6 Sustentabilidade econômica no ambiente de comércio eletrônico virtual

O comércio eletrônico (*e-commerce*) apresenta “contínua expansão, sobretudo a partir da primeira década dos anos 2000”, segundo Laura Mendes (2014, p. 74), e com a



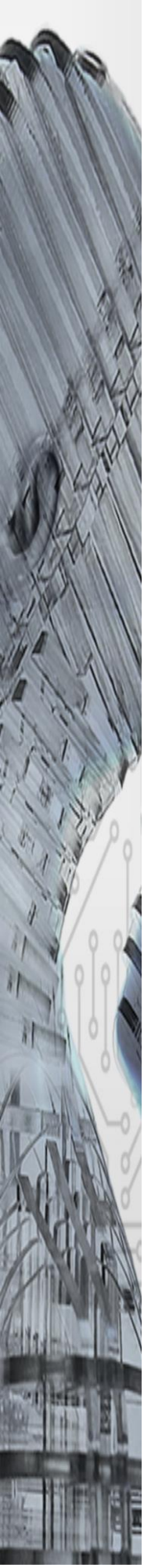
"popularização do acesso à Internet e a utilização de *smartphones*, computadores e *tablets"* (GOMES, 2017, p. 35). Devido ao potencial democrático e às oportunidades econômicas, o comércio eletrônico movimenta valores cujos montantes são aparentes nos cálculos do produto interno bruto real (PIB) de muitos países de economia fundada no modelo capitalista, atingindo setores de geração de renda real, emprego, produção industrial e vendas no atacado e varejo (FARIA; SILVEIRA; MONTEIRO, 2018, p. 567 - 569). Nas palavras de Laura Mendes:

> O século vinte apresentou, entretanto, com a sua revolução das tecnologias da informação e comunicação, um desafio único para o sistema jurídico, no tocante à regulação desse fenômeno: a infraestrutura de comunicação e informação perpassa hoje todos os aspectos da vida, estando incrustada no cotidiano do indivíduo e da sociedade, o que levou à criação do conceito de onipresença ou ubiquidade dos meios informáticos *(ubiquitous computing*). Especialmente a digitalização, os sistemas informáticos e a conectividade em rede são responsáveis por essa ubiquidade: *smartphones, web 2.0, cloud computing,* internet das coisas, são algumas expressões que representam esse fenômeno. (MENDES, 2014, p. 75)

Assim sendo, o comércio eletrônico representa um poderoso setor de impacto, cuja expansão pode ser analisada com possibilidade de promover um futuro sustentável, seja do ponto de vista econômico, seja pelo viés jurídico, posto que envolve as transações eletrônicas entre uma organização e outras partes interessadas, representadas por consumidores, prestadores de serviços logísticos, servidores públicos (*e.g.:* fiscais fazendários) e terceiros, cujas atuações possam integrar o conjunto de agentes nas relações do meio ambiente virtual.

Neste prisma, meio ambiente, "sociedades e economia são o escopo da sustentabilidade em cada comunidade" (BAUMAN, 2001, p. 22). Logo, a economia é o meio ambiente onde os recursos, produtos e serviços podem ser partilhados ou adquiridos mediante pagamento (RAMOS, *et al*, 2014, p. 22 - 34). A sustentabilidade, outrossim, "consiste na manutenção de um meio ambiente equilibrado, sem comprometer o desenvolvimento das sociedades e da economia" (SCHOLZ, 2012, p. 154). A sustentabilidade é uma noção normativa sobre a maneira como os seres humanos devem agir no tocante à natureza e como eles são responsáveis uns em relação aos outros e às gerações futuras.

Sob a égide da preservação dos recursos naturais, a conscientização sobre sustentabilidade é de grande importância no comércio eletrônico, considerando "produtos e serviços como ambientalmente comprometidos com um desenvolvimento econômico, onde todos os aspectos estão ligados uns aos outros e uma empresa não pode escolher lidar com um fator específico e omitir-se em outro" (ASHMARINA; MESQUITA; VOCHOZKA, 2019, p. 35 - 42). "A preocupação com o meio ambiente envolve recursos naturais, materiais de



embalagem, emissões de dióxido de carbono, poluição da água e a contaminação do solo" (MISTRY; DHAVALE, 2011). Logo, as empresas devem garantir que suas atividades não levem ao esgotamento e danos aos recursos naturais. Lidar com o processo de produção, produtos e serviços significa não prejudicar as criaturas vivas antes, durante e após o uso do produto, garantindo assim a permanência de um estado saudável para o ambiente.

A economia digital, liderada pela Internet, alterou muitos dos padrões envolvendo a produção, a distribuição e o consumo de bens, produtos e serviços, em escala global. Embora exista grande potencial para aproveitar as Tecnologias da Informação e Comunicação - TICs, de modo geral e a Internet em particular, os possíveis impactos negativos do comércio eletrônico no meio ambiente também devem ser considerados e tratados de maneira responsável (ASHMARINA; MESQUITA; VOCHOZKA, 2019, p. 43). Nas palavras de Capurro e Hjorland:

> A mudança terminológica de sociedade da informação para sociedade do conhecimento sinaliza que o conteúdo, e não a tecnologia da informação, é o principal desafio tanto para a economia quanto para a sociedade em geral. (CAPURRO; HJORLAND, 2007, p. 157)

Em relação ao comércio físico tradicional, que costuma obedecer às regras laborais e aos horários de funcionamento, o comércio eletrônico pode ser feito em qualquer lugar, 24 horas por dia, durante todos os dias da semana, bastando apenas a conectividade com a Internet e a disponibilidade financeira do consumidor, "superando assim as limitações geográficas e garantindo uma atividade rentável para os varejistas e trabalhadores do setor comerciário, ao oferecer uma gama de produtos e serviços para serem escolhidos" (WALDFOGEL; PEITZ, 2016, p. 353).

O comércio eletrônico tem sido alimentado pelas redes sociais, onde os clientes podem reclamar e obter *feedback* imediatamente, por meio dos serviços e suporte *on-line* oferecidos pelos vendedores em plataformas, *sites* e pelos anúncios de *marketing* e publicidade virtuais. As interações entre empresas e consumidores foram possíveis, uma vez que as demandas consumeristas continuam mudando ao longo do tempo (MENDES, 2014, p. 257 - 271). "A Internet trouxe consigo uma imensa densidade de informação, que é precisa, oportuna e acessível para fins de comparação" (STAPLETON, 2014, p. 188), ou seja, há livre comércio e poucas barreiras à entrada no mercado, oferecendo alta personalização aos clientes com base nos dados coletados durante o comportamento e o perfil de compra anterior e nas especificações de buscas, os quais formam padrões de atividades e gostos pessoais, apesar de não necessariamente identificarem o indivíduo, criam um sistema de anúncios com base em

consultas anteriores, a partir daquele dispositivo específico que coletou dados, através de uma estratégia de *marketing* conhecida como segmentação comportamental. Neste sentido, complementa Rita Blum com os apontamentos abaixo colacionados:

> Os dados dos hábitos de consumo da pessoa, somados ao seu perfil financeiro, idade, e outros elementos que possam influenciar na decisão de compra de novos e melhores produtos, ou contratação de novos serviços são hoje muito importantes para fins de *marketing*. Por esta razão têm também valor econômico para os fornecedores. Tais dados são úteis a eles, seja para estreitar o vínculo que têm com o consumidor, seja para melhor definir o teor da propaganda que será elaborada e apresentada a um consumidor potencial. (BLUM, 2018, p. 129)

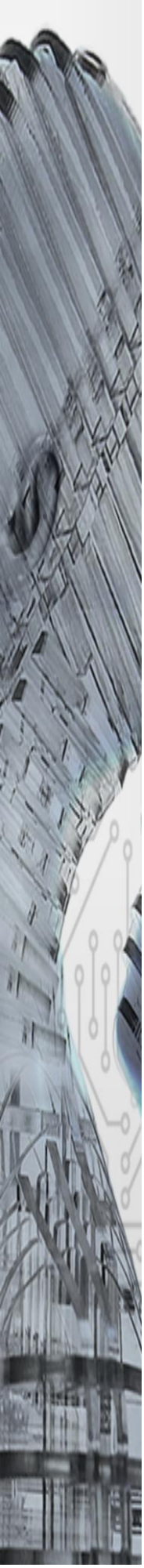
Entrentanto, Zygmunt Bauman perfaz uma análise crítica e humanística do *marketing* virtual nos seguintes termos:

> São (as pessoas) ao mesmo tempo, os promotores das mercadorias e as mercadorias que promovem. São, simultaneamente, o produto e seus agentes de *marketing*, os bens e seus vendedores […]. Seja lá o nicho em que possam ser encaixados pelos construtores de tabelas estatísticas, todos habitam o mesmo espaço social conhecido do mercado. Não importa a rubrica sob a qual sejam classificados por arquivistas do governo ou jornalistas investigativos, a atividade em que todos estão engajados (por escolha, necessidade ou, o que é mais comum ambas) é o *marketing*. O teste que precisam passar para obter os prêmios sociais que ambicionam exige que remodelem a si mesmos como mercadorias, ou seja, como produtos que são capazes de obter atenção e atrair demandas e fregueses. (BAUMAN, 2008, p. 13)

Além disso, "as plataformas *on-line* permitem que as empresas comercializem seus produtos/serviços para públicos selecionados e reduzam o ruído da publicidade irrelevante para esses públicos" (MATTERN, 2008, p. 22), permitindo a publicidade baseada em interesses depreendidos da coleta e análise dos dados pessoais dos usuários e nas características sociodemográficas. As considerações de Eduardo Magrani, retratam o contexto da seguinte forma, *in verbis:*

> Assim, ocorre uma espécie de "hipertrofia de atenção", pois os *sites* e *blogs* mais populares são os mesmos constantes nos primeiros lugares das pesquisas dos *sites* de busca, quando se procura por informação política e por isso propensos à acumulação de novos leitores. (MAGRANI, 2018, p. 20)

O comércio virtual, todavia, requer a captação de dados dos clientes, para que as compras possam ser realizadas (MISTRY; DHAVALE, 2011). Deste modo, a ecologia do ambiente virtual requer uma sustentabilidade capaz de assegurar a autodeterminação dos dados pessoais por parte dos consumidores e o equilíbrio econômico. Se não forem devidamente abordadas, tais preocupações sobre como os dados são usados, sobrevirá forte ameaça de redução à disposição das pessoas em compartilhar suas informações pessoais (WALDFOGEL; PEITZ, 2016).



Embora o potencial uso indevido de dados pessoais e as preocupações de privacidade associadas, sejam tópicos importantes que precisam ser abordados pelas autoridades, a presente pesquisa lança maior atenção ao valor econômico dos dados pessoais gerados e mantidos pelo mecanismo de mercado onde o capital econômico sobre dados pessoais é compartilhado por dois lados subjacentes, quais sejam o setor da iniciativa privada e a esfera da iniciativa pública, como vieses tutelados distintamente no ordenamento jurídico, mesmo ocorrendo mediante utilização de grandes bancos de dados, sediados no âmbito doméstico ou em países diferentes do território onde a coleta ocorreu.

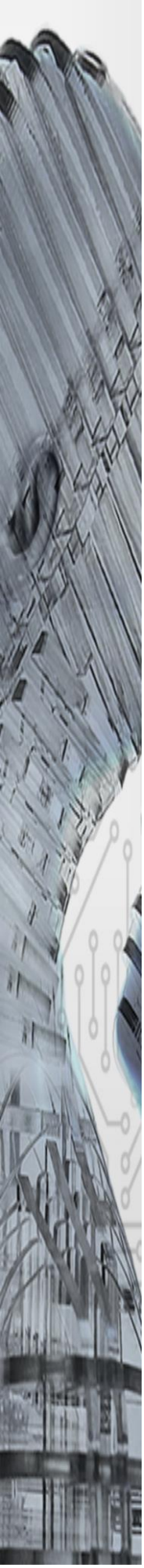
1.7 Reciclagem e reutilização de informações

Grandes bases de dados estão disponíveis em todos os lugares: quase todas as empresas, organizações governamentais e organizações sem fins lucrativos coletam dados pessoais sobre potenciais clientes, fornecedores e funcionários (STAPLETON, 2014). Além disso, a maioria das organizações coleta informações sobre seus processos de negócios, incluindo informações sobre produtos, informações de pagamento, informações de endereços de envio, faixa etária e sexo de clientes, dentre outras referências que são consideradas como dados pessoais (BLUM, 2018).

Com a introdução da "Internet das coisas", na qual os objetos são equipados com dispositivos embarcados interconectados, a transmissão de informações acerca dos *status* e localizações de usuários são também registradas em bancos de dados, caracterizando o potencial de reutilização de *Big Data* como fonte de individualização pessoal (BOFF; FORTES; FREITAS, 2018), o que caracteriza violação às proteções conferidas nas Leis de Proteção de Dados Pessoais, conforme avante exposto.

No entanto, existem várias barreiras práticas, tecnológicas e legais que impedem a fácil reutilização de dados. Conhecimento é poder econômico e, portanto, é possível compreender os motivos e escusas de muitas organizações e empresas, ao não se colocarem dispostas a compartilhar com outros setores os dados que coletaram, tendo em vista o seu valor como vantagem competitiva. Para Laura Mendes:

> A informação como objeto de regulação é tema que há muito ocupa as disciplinas jurídicas: seja no direito constitucional, com a liberdade de expressão, a liberdade de imprensa ou as garantias de sigilo constitucionais; seja no direito penal, com a proteção contra a divulgação de informações difamatórias ou injuriosas, ou no direito comercial, com a garantia de sigilo empresarial. Tão diversas quanto antigas são as formas do Direito de tentar regular esse complexo fenômeno, por reconhecer



> os efeitos da circulação (ou da não circulação) de informações na vida dos indivíduos e na sociedade (MENDES, 2014, p. 75)

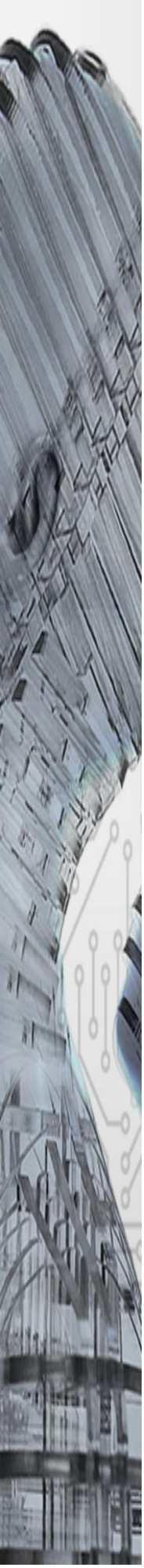
Ao mesmo tempo, para muitas organizações, seria muito eficiente se elas tivessem acesso fácil aos bancos de dados de outras organizações e pudessem usar os dados disponíveis para todos os tipos de propósitos. Segundo Stapleton (2014, p. 172), “as barreiras tecnológicas podem consistir em bancos de dados em diferentes formas que não podem ser facilmente acopladas, e as barreiras legais podem consistir em privacidade e informações de propriedade intelectual, dentre outras”.

Do ponto de vista legal, os atuais requisitos de proteção de dados pessoais, como minimização de dados e especificação de propósitos, são potencialmente hostis ao *Big Data*, pois limitam a abrangência e o escopo de sua reutilização (GOMES, 207, p. 155 - 172). “Para evitar a perda substancial de informações relevantes economicamente, pode-se argumentar que o reuso de dados deve ser incentivado” (STAPLETON, 2014, p. 283). A fim de encontrar novos modelos para reutilização de dados, é necessária uma análise aprofundada das barreiras éticas, morais e legais existentes.

A estrutura legal que regula o uso e a reutilização de dados pessoais, como tema principal da presente análise, representa um arcabouço jurídico amplamente embasado em princípios para o processamento justo de dados pessoais, codificados em legislações estrangeiras, supranacionais e nacionais. Assim sendo, a taxonomia pode ser útil para determinar até que ponto a reutilização de informações pessoais é permitida pelas leis atuais de proteção de dados, face à preservação da privacidade, por um lado, e econômica e socialmente benéfica, por outro.

Logo, a reutilização de dados pode ser subdividida em dois espectros distintos, sendo eles: (I) aquele que se aproxima da consciência e das intenções dos titulares de dados e deve ser abordado de forma menos restritiva (por exemplo, assumindo o consentimento informado) e; (II) a reutilização de dados que estão "à distância", ou seja, em casos “onde a conscientização e a transparência podem estar ausentes e os direitos dos titulares dos dados podem se mostrar mais difíceis de serem exercitados” (HAUNTS, 2018, p. 33), quando maiores restrições e proteção adicional devem ser consideradas (por exemplo, exigindo consentimento explícito no instrumento de cessão).

O termo reutilização de dados, no seu sentido mais amplo, sugere que há um “uso inicial (primário) de dados e um uso subsequente (secundário) de dados, ou seja, a reutilização de dados” (SCHOLZ, 2012, p. 203). A distinção entre uso e reutilização pode



implicar aspectos diferentes, no entanto. Neste sentido, o uso de dados (uso primário) tem por escopo o seu emprego para um propósito específico[35].

Considerando que o uso de dados e a reutilização de dados podem ser concebidos como "uma ação que ocorre após a coleta e armazenamento de dados pessoais e antes do apagamento ou destruição dos dados pessoais" (PINHEIRO, 2018, p. 36), o arcabouço legal considera a coleta, armazenamento, apagamento e destruição também como formas de dados em processamento.

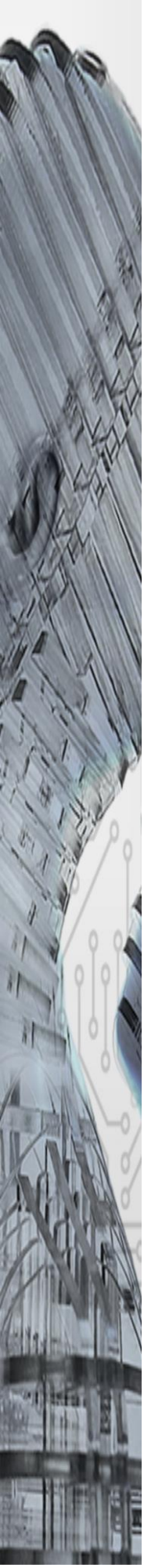
Como resultado, pode-se sugerir que o processamento de dados sempre comece com a coleta de dados (a primeira forma de processamento) e que ações subsequentes como armazenamento, preparação e análise de dados sejam todas as próximas etapas do processamento de dados e, como tal, como reprocessamento ou reutilização (STAPLETON, 2014, p. 146 - 155).

Numa perspectiva onde os dados são quase sempre coletados (e geralmente armazenados) antes de poderem ser usados para qualquer finalidade, "a coleta e o armazenamento de dados, embora sejam os primeiros passos na maioria dos processamentos de dados, já devem contar como uso de dados" (HAUNTS, 2018, p. 25). Da mesma forma, "o apagamento ou a destruição, se essas ações ocorrerem no final de um ciclo de vida de dados pessoais, não devem ser considerados como reutilização de dados" (LIBERT, 2014, p. 104).

Portanto, são possíveis várias maneiras de reutilização de dados pessoais, sendo de mais simples distinção a reciclagem de dados e a reutilização de dados (STAPLETON, 2014). A forma menos complexa de reutilização de dados é aquela capaz de reutilizar os mesmos dados, de maneira similar, por mais de uma vez (*e.g*. quando uma companhia de seguros de saúde coleta dados de pacientes para ter um banco de dados de clientes adequado usado para faturar os prêmios de seguro devidos e para reembolsar remédios, tratamentos e terapias, ou quando o endereço de um cliente é reutilizado para enviar uma fatura, mensalmente, trimestralmente ou anualmente).

Logo, a reciclagem de dados se apresenta de forma simples, uma vez que os dados são usados repetidamente da mesma maneira. Não há questões legais significativas aqui, desde que o titular dos dados não revogue o seu consentimento informado. Por exemplo,

[35] A Diretiva 95/46/EC da UE sobre proteção de dados pessoais, encontra-se atualmente revogada pelo RGPD, mas durante sua vigência não tratava dos conceitos de uso de dados e reutilização de dados, somente utilizando o conceito de "processamento de dados pessoais", que era definido no Artigo 2 como: "qualquer operação ou conjunto de operações que são realizadas mediante dados pessoais, seja ou não por meios automáticos, como coleta, registro, organização, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, bloqueio, eliminação ou destruição"(UE, 1995).



quando um titular de dados escolhe outra seguradora de saúde, a seguradora anterior não pode mais usar os dados para enviar as contas.

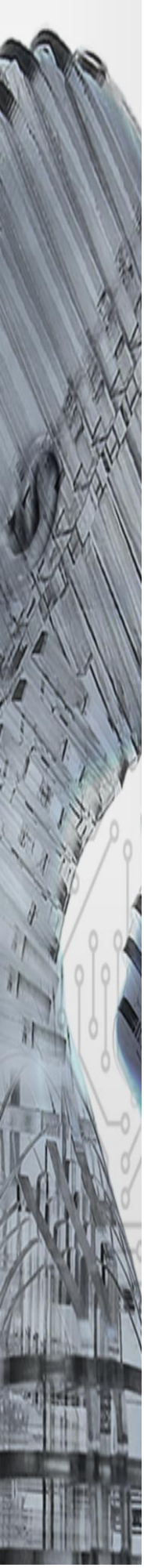
Outra forma de reutilização de dados pessoais é a classificada como "redirecionamento de dados" ou "redefinição de dados"[36], a qual pode ocorrer, por exemplo, quando a mesma seguradora de saúde começa a usar os dados para avaliar as condições clínicas dos pacientes, a fim de determinar os prêmios de seguro e valores das mensalidades, baseados em dados pessoais sobre saúde (por exemplo, prêmios mais altos para pessoas em risco ou comportamentos insalubres como fumar, não fazer exercícios, etc., com riscos baixos mostrando um comportamento saudável), eles estão reutilizando os dados para uma finalidade diferente. O redirecionamento de dados acontece sobremaneira, já que os dados são usados para muitos propósitos. Endereços não só podem ser usados para fins de faturamento, como também para anúncios e quaisquer finalidades outras que a criatividade permitir. "Os dados podem ser combinados para encontrar novos grupos de clientes em potencial, para avaliar as pontuações de crédito ou para avaliar riscos médicos" (STAPLETON, 2014, p. 185).

Quando a companhia de seguros de saúde nos exemplos acima começa a informações pessoais, outras empresas também podem fazer uso dos dados de titulares que estão enquadrados na condição de clientes, por exemplo, para comercializar seus produtos para determinados grupos-alvo (TEIXEIRA, 2018, p. 44 - 48). "Os dados são então reutilizados em um contexto (às vezes completamente) diferente, caracterizando esta forma de reutilização de dados como "recontextualização de dados"" (BOURQUE; CLARK, 2006, p. 34). Isso pode causar problemas de integridade contextual, pois os dados podem ter um significado diferente ou podem ser interpretados de maneira diferente em outro contexto. Por exemplo, dados de saúde podem ser interpretados de formas diferentes por um médico, por empresas de seguro de saúde, farmácias ou por companhias de saúde suplementar.

Usando *Big Data*, todos os tipos de novos *insights* e previsões podem ser feitos sobre as pessoas (LIBERT, 2014; GOMES, 2018). Às vezes, essa análise de dados pode até revelar informações sobre pessoas que elas não conheciam, como os riscos que correm para acometimento de formas específicas de câncer ou a sua expectativa de vida.

Segundo Scholz (2012, p. 188): (I) o princípio de que os propósitos para os quais os dados pessoais são coletados devem ser especificados com antecedência e que os dados só podem ser usados para esses fins, são chamados de princípios de especificação de propósitos;

[36] Do ponto de vista jurídico, a Diretiva de Proteção de Dados da UE 95/46 / EC enfocava a redefinição de dados no Artigo 6.1 (b): dados pessoais devem ser 'coletados para fins específicos, explícitos e legítimos e não processados de forma incompatível com esses propósitos'



(II) o princípio de que os dados pessoais não devem ser divulgados, disponibilizados ou utilizados para outros fins que não os especificados, exceto com o consentimento do titular dos dados ou pela autoridade da lei, é chamado de princípio de limitação de uso, tratados com mais profundidade nas seções posteriores.

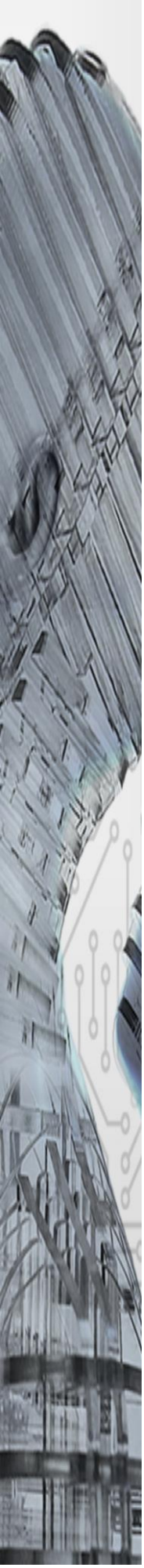
Do ponto de vista legal, não há diferença real entre o redirecionamento de dados e a recontextualização de dados (STAPLETON, 2014; HAUNTS, 2018; PINHEIRO, 2018; TEIXEIRA, 2018). Ambos os tipos de reutilização de dados são geralmente chamados de "fluência de função" e não são permitidos a menos que haja uma base legal para isso. Tal distinção se faz presente, no entanto, porque a recontextualização de dados pode trazer diferentes questões legais, por exemplo, em relação às expectativas que titulares podem ter sobre as maneiras como seus dados são utilizados, de maneira positiva ou pejorativa, quando não garantem tratamento isonômico, mas diferenciado por uma informação ou preconceito advindo da análise de dados pessoais.

Quando os dados são usados em um novo contexto, a "distância" entre o titular dos dados e o controlador de dados aumenta, pois é elevada a consciência de caráter individual, através dos dados pessoais disponíveis e revisitados sobre o novo enfoque contextual específico do caso concreto (BLUM, 2018, p. 22 - 34). Assim sendo, é importante notar que a reutilização de dados pode adquirir sentido geral diverso daquele especificamente determinado no momento de sua coleta. O redirecionamento de dados pode ser entendido como usando os mesmos dados para vários propósitos diferentes (GOMES, 2017, p. 155 - 167) havendo autorização ou não, por parte de seu titular.

Em todas as perspectivas apresentadas, os resultados podem tornar o exercício de direitos e o controle de dados pessoais duas tarefas muito difíceis para os seus titulares. Além disso, a probabilidade de erros de interpretação também pode aumentar, abalando a economia digital, a sustentabilidade econômica do ambiente eletrônico e a proliferação de informações em *Big Data*, não compatíveis com a realidade do momento da coleta.

1.8 Os dados como patrimônio e a perda de dados

O patrimônio em dados pessoais "possui valores variáveis, de acordo com o conteúdo que se armazena" (ANGHERN, 1997, p. 35). Os dados pessoais podem ser vistos como um ativo econômico gerado pelas identidades e pelos comportamentos dos indivíduos no ambiente virtual, que são monitorados, armazenados e negociados ou trocados por serviços



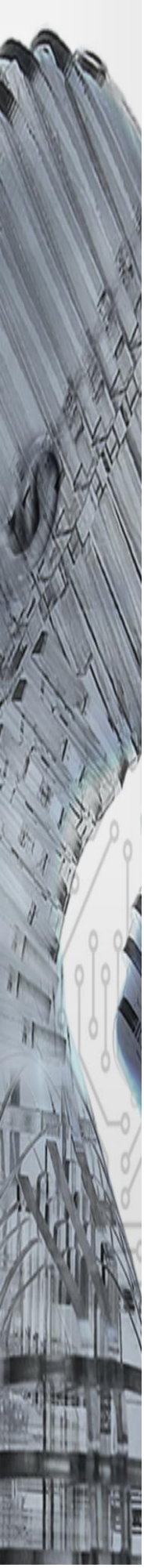
e produtos de maior qualidade (TEIXEIRA, 2018, p. 44 - 48), “num ambiente onde a quantidade de dados pessoais armazenados aumenta continuamente” (WAZLAWICK, 2017, p. 652).

Em um mecanismo de mercado bilateral, as plataformas em linha agem como intermediários que coletam informações do comportamento de consumo de seus usuários e, simultaneamente, vendem vagas de publicidade o oferecem anúncios para empresas, analisando os possíveis perfis informativos contidos nos dados advindos dos consumidores, com a possibilidade de criarem estratégias de publicidade personalizadas para produtos e serviços (TEIXEIRA, 2018, p. 44 - 46). “As empresas são, em teoria, mais bem-sucedidas na colocação de seus produtos, e os consumidores recebem recomendações adaptadas aos seus interesses” (WALDFOGEL; PEITZ, 2012, p. 455). Em outras palavras, o uso de dados pessoais pode eliminar as assimetrias de informações e contribuir para a eficiência das transações virtuais. Portanto, as necessidades de proteção e regulação tem sido cada vez mais urgentes, de forma que não sejam impedidas as suas aplicações ao mercado, mas que passem a estar mais amplamente reguladas e uniformizadas, ofertando maiores garantias contra abusos. Para Laura Mendes, a questão se traduz da seguinte forma abaixo colacionada:

> Numa sociedade da informação, que é, ao mesmo tempo, sociedade de consumo, faz-se necessário que o direito fundamental à privacidade tenha seu reflexo no âmbito infraconstitucional, mais especificamente, nas relações entre fornecedor e consumidor. Assim, entendemos que a concretização do dever estatal de proteção ao consumidor (art. 5º, XXXII, da CF) numa sociedade caracterizada pelo amplo fluxo de informações, somente pode ser atingida com o reconhecimento de um direito básico do consumidor à proteção de dados pessoais. Afinal, diante do generalizado tratamento de dados pessoais pelo setor privado para segmentar produtos e serviços e aumentar a eficiência de seu processo produtivo, ampliam-se as ameaças à personalidade do consumidor e os riscos de sua discriminação e estigmatização no mercado. Assim, pode-se dizer que, no século XXI, a proteção do consumidor e a proteção de dados pessoais são processos interdependentes: a efetividade de um depende da efetividade do outro. (MENDES, 2014, p. 364)

A perda de dados figura como “um dos principais problemas na relação entre usuários e empresas de programas eletrônicos, bem como de governos e agências públicas” (BOURQUE; CLARK, 2006, p. 61), representando uma condição de erro em sistemas nos quais a informação é destruída por falhas ou negligência no armazenamento, transmissão ou processamento (CARVALHO; LORENA, 2016, p. 49 - 53). Os sistemas de informações implementam equipamentos e processos de *backup* e recuperação de desastres para evitar perda de dados ou restaurar os dados perdidos.

A perda de dados é diferenciada da indisponibilidade de dados, que pode surgir de uma interrupção na rede. Embora os dois “tenham consequências substancialmente



semelhantes para os usuários, a indisponibilidade de dados é temporária, enquanto a perda de dados pode ser permanente" (HUDAK, 2006, p. 35). "A perda de dados também é diferente da violação de dados, um incidente em que os dados caem nas mãos erradas, embora o termo perda de dados tenha sido usado nesses incidentes" (STAPLETON, 2014, p. 238).

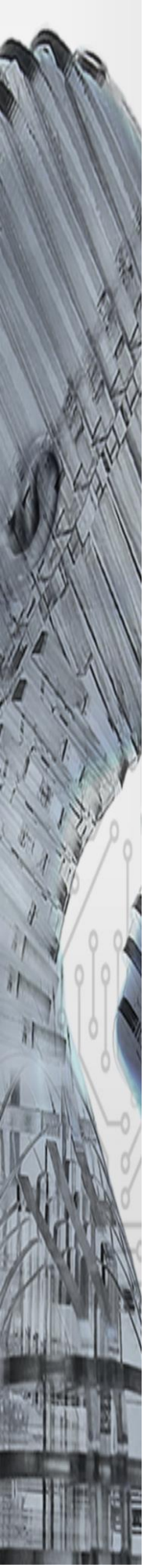
A relação privada, compreendida pelo estabelecimento de um instrumento ou contrato de cessão de dados, mediante consentimento expresso do usuário, representa uma relação de consumo. "No que diz respeito à responsabilidade civil na Internet, não haveria, em tese, maiores problemas em enquadrá-la na legislação brasileira, especialmente no Código Civil e no Código de Defesa do Consumidor" (TEIXEIRA, 2018, p. 317). Já as relações entre o Poder Público e o indivíduo que viu os seus dados sofrerem destinação diversa, podem ter suas queixas revistas com base na Lei Civil, até o ponto em que o Direito Público sobre o primeiro prevaleça.

A proteção de dados pessoais e segurança da informação podem (e devem) ser encaradas não como um acréscimo aos custos ou despesas operacionais, mas sim como uma vantagem competitiva, um diferencial de mercado. Em uma época de grandes vazamentos de informações e escândalos quanto ao uso indevido de dados, a adequação antecipada às regras claras, transparentes e harmônicas é capaz de restaurar ou aumentar a confiança do consumidor nas empresas, no mercado e, principalmente, nos sistemas de informação globalizados.

1.8.1 Roubo de Dados

O termo roubo de dados é, na verdade, incorreto no mundo digital, porque os dados geralmente não são roubados, mas sim copiados sem autorização, não havendo uma subtração, ou a transferência total do objeto jurídico sob tutela de um local para outro, de um possuidor-proprietário para o domínio de outrem, mas tão somente a sua duplicação de forma não autorizada ou ilegal. Se o roubo de dados acontece influenciando um processamento de dados, também é falada "fraude de computador" (HUDAK, 2006, p. 64). O principal objetivo do roubo de dados é a revenda com vistas à obtenção de valor econômico (MCLEAN, 2010, p. 47). Neste prisma, a aquisição ilegal de dados pessoais adquire enquadramentos da Lei Penal, além daqueles advindos dos impactos tutelados pela Lei Civil.

Os dados pessoais roubados são usados de várias maneiras. Três categorias principais de uso de seus dados se destacam: (I) a abertura de novas contas, especialmente bancárias,



onde é possível realizar pedidos de cartões de crédito, empréstimos bancários, etc.; (II) a realização de transações entre contas bancárias (sem cartões de crédito) e, finalmente; (III) o uso ilícito de contas bancárias por meio de um cartão de crédito.

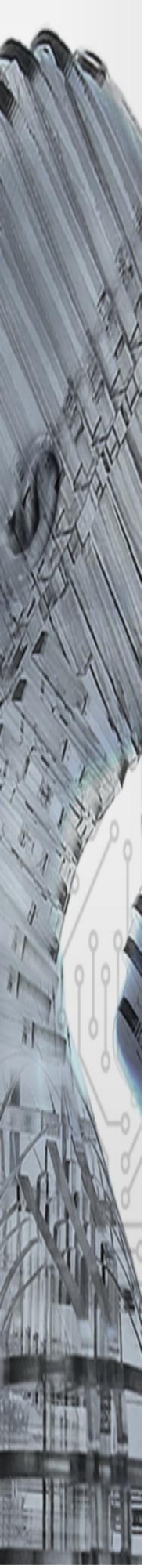
As técnicas de pirataria e demais crimes cibernéticos que buscam reunir informações confidenciais são numerosos, visando vantagens indevidas por meio da má-fé. A vítima geralmente tem seus dados pessoais e credenciais roubados ou copiados, o que possibilita, em continuidade, a consumação do ato prejudicial (por exemplo: fazendo uma transferência da conta bancária da vítima ou utilizando informações pessoais e íntimas para chantageá-la) (TEIXEIRA, 2018, p. 52 - 528).

1.9 A relação dos Direitos Humanos com a segurança e a proteção de dados pessoais

O conhecimento, ainda que superficial, a respeito das implicações da produção e cessão de dados pessoais, seu tratamento, manipulação e armazenamento, ainda não se encontra amplamente difundido para grande parte de seus titulares/usuários. Pois, muito embora algumas pessoas possam ter um entendimento profundo de como a tecnologia funciona, elas podem não compreender tão bem as nuances da proteção de dados pessoais e os desrespeitos, ilícitos e a paulatina mitigação de direitos humanos inalienáveis e direitos constitucionais fundamentais, sobrepujados por interesses econômicos, governamentais, ou colocados por detrás de nomenclaturas científicas específicas e distantes da cultura popular.

Da mesma forma, pessoas com profundo conhecimento em Direitos Humanos podem não entender realmente como a tecnologia as afeta. Logo, os Direitos Humanos enfrentam desafios de adaptação e sobrevivência na Era Digital, caracterizando uma necessidade real e urgente de conscientização comum sobre o fortalecimento da segurança digital e a manutenção de diversos direitos conexos (PRIVACY INTERNATIONAL, 2018, p. 24-25), frutos das lutas sociais durante séculos, face a novos tipos de ameaças, mascaradas pela epidemia de consumo das novas TICs e a cultura da produção de conteúdos em ambiente virtual, de forma madura, consciente e crítica (GLOBAL PARTNERS DIGITAL, 2018, p. 51 – 60).

À luz dos Direitos Humanos e Constitucionais Fundamentais, a proteção de dados pessoais deve ser interpretada como uma preocupação humana coletiva, de construção jurídico-social mais ligada à prática de bons costumes, onde exista uma otimização da absorção de informações capazes de dotar os indivíduos com habilidades e competências para

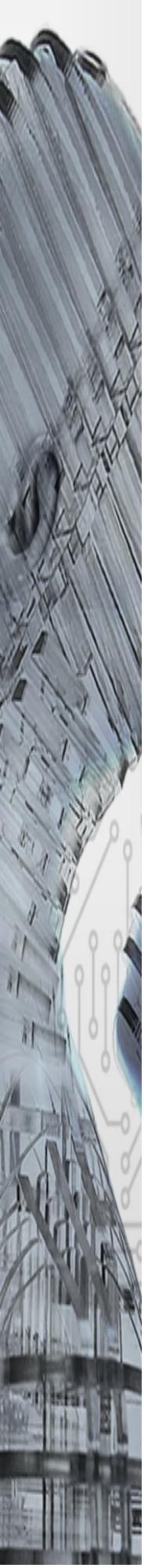


operarem em ambiente virtual, agindo de modo responsável para mensurar os impactos de suas escolhas em médio e longo prazos, sob a perspectiva do armazenamento perpétuo. Afinal, os "Direitos Humanos são proteções que, quando reivindicados, ampliam a proteção comum" (ADC, 2016, p. 37), num panorama onde a privacidade é, antes de tudo, a liberdade de insistir que direitos não sejam retirados. Nesta perspectiva, a prática da segurança digital capacita indivíduos a exercitarem os seus direitos de maneira consciente e responsável, preservando tanto a liberdade de expressão, quanto a intimidade da vida particular e enviando uma forte mensagem a quem pretenda ou possa produzir qualquer tipo de violação de direitos, em sua concepção generalizada.

Todavia, pairam sobre a segurança digital e a proteção de dados pessoais alguns mal-entendidos populares, fomentados por anseios de controle e monitoramento por parte de empresas e governos, enquanto poucos setores sociais se atentam para os impactos trazidos pelo mau uso de informações em geral e investem tempo, estudo e capital em medidas capazes de produzir uma "harmonização normativa supranacional de aplicação direta e a forte outorga de garantias e proteção aos direitos humanos" (ADC, 2016, p. 13), mediante a utilização de novas tecnologias, aliadas à privacidade.

Um exemplo comum pode ser observado nas cláusulas sobre formas de utilização (tratamento) de dados em termos ou contratos de cessão, onde pessoas geralmente não realizam uma leitura com atenção, permitem acesso a outras fontes de dados armazenados em dispositivos, ou se sentem confortáveis para aceitar restrições ao seu direito à privacidade (TEIXEIRA, 2018, p. 312 – 314), acreditando que isso permitirá ao governo proteger melhor a segurança nacional, quando na realidade, alguns governos têm o costume de violar direitos humanos por razões mesquinhas e em contextos bem mais aparentes do que os virtuais, simplesmente porque a sociedade civil não reage ou não enxerga determinados atos como uma violação de seus direitos inalienáveis e fundamentais.

Entretanto, a segurança digital não se coaduna com a ocultação de algo ilícito, mas sim com a capacidade individual de desejar níveis variados de intimidade para a própria vida, em seus variados setores - e de não divulgar ou publicar informações para a sociedade de aspectos de sua vida privada, além da sua liberdade para buscar informações de seu interesse, manifestar opiniões e demais liberdades básicas (PRIVACY INTERNATIONAL, 2018, p. 38 – 39). Nesta ótica, as leis de proteção de dados (como um direito acessível à coletividade) e as posturas adotadas individualmente no controle da cessão de dados pessoais e na segurança digital, formam uma dupla de ações as quais são vitais para a democracia, principalmente



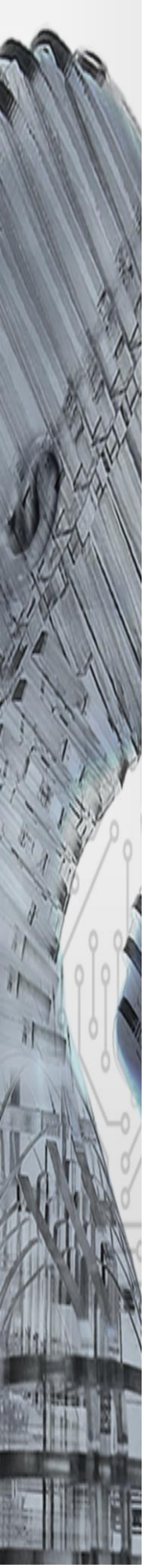
quando governos e empresas podem considerar realizar quaisquer mudanças para pior, de formas perigosas ou ilegítimas, de acordo com as suas visões sobre os Direitos Humanos e com o apoio de regimes político-administrativos.

Para outras tantas pessoas, a segurança digital é tida como necessária apenas para quem age de maneira antiética, sob uma perspectiva antagônica e preconceituosa à própria essência de "privacidade" e "autodeterminação", contidas nas leis de proteção de dados pessoais, afirmando que "a pessoa defensora e cuidadora de sua privacidade e da sua liberdade em ambientes virtuais e eletrônicos, provavelmente se envolve em comportamentos sorrateiros ou suspeitos". Outros temem que, se praticarem a segurança digital, outras pessoas farão a mesma suposição sobre eles. De qualquer maneira, as pessoas com tais visões rejeitam e enfraquecem a proteção que os Direitos Humanos oferecem a todos, indistintamente. A segurança transpessoal também depende da segurança da proteção de dados pessoais, principalmente quando um dos interlocutores se encontra em situação de risco ou de indiferença quanto à exposição, colocando todos os correlacionados em idêntico ou majorado perigo.

As boas práticas de segurança digital podem ser divididas em cinco grandes grupos de atenção de titulares de dados, como perfis de proteção a serem exercidos diuturnamente e em quaisquer relações de cessão de dados pessoais, em redes sociais, para com empresas ou governos, devendo ser fortes em todas elas, a saber:

(I) Utilização de ferramentas digitais: reflete a existência de muitos aplicativos de *software* que afetam a segurança virtual. Alguns deles são muito úteis e instalá-los pode ajudar a proteger os dispositivos, a localização, senhas e dados sensíveis. Outros têm vulnerabilidades distintas e devem ser limitados ou desativados, de modo que a escolha estratégica de *softwares* priorize a segurança e a não permissão de captação de dados pessoais que parecem não ter a menor ligação com a finalidade a que se propõe a ferramenta digital. Para tanto, o usuário pode dedicar um tempo maior à leitura dos termos ou condições de uso;

(II) Comunicações digitais: como as novas tecnologias permitem a comunicação digital a grandes distâncias e o compartilhamento de pensamentos, ideias e sentimentos mais íntimos, até a produção de mídias audiovisuais de momentos privados, além de informações profissionais, dados confidenciais, como contas bancárias e registros de saúde, o usuário pode buscar *softwares* e dispositivos de comunicação que ofereçam a criptografia como regra e rigorosas limitações ao tratamento de dados, sob o risco



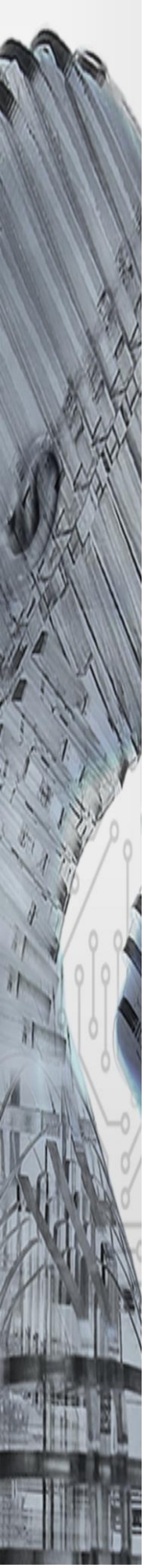
de facilitação de interceptações, invasões e roubos por *hackers*. As comunicações digitais também dizem respeito ao direito fundamental de sigilo telefônico e de correspondências físicas ou eletrônicas.

(III) Espaços digitais: os espaços digitais se referem a espaços *online* (como uma plataforma de mídia social) e espaços *off-line* com infraestrutura digital (como uma sala com *wi-fi*). Alguns ambientes e infraestruturas são mais confiáveis que outros, principalmente quando se tratam de redes públicas ou privadas, com a utilização de sistemas de segurança, *firewall* e utilização de senhas fortes e trocadas com regularidade. Conhecer a diferença e agir de acordo é um enorme benefício de segurança.

(IV) Hábitos digitais: enquanto as ferramentas digitais podem ser instaladas ou desativadas uma vez para maior proteção, algumas práticas de segurança digital precisam ser executadas repetidamente para se proteger, tais como a exclusão de arquivos inúteis, a utilização de navegadores que não utilizam *cookies* e não armazenam dados e a limpeza ou a subscrição de dispositivos, de tempos em tempos, como formas simples de manutenção de aparelhos e aplicativos, bem como o salvamento de *backups* de arquivos contendo dados sensíveis em dispositivos externos, como *pendrives, chips* e discos de memória externa, deixando somente o essencial nos dispositivos de IoT.

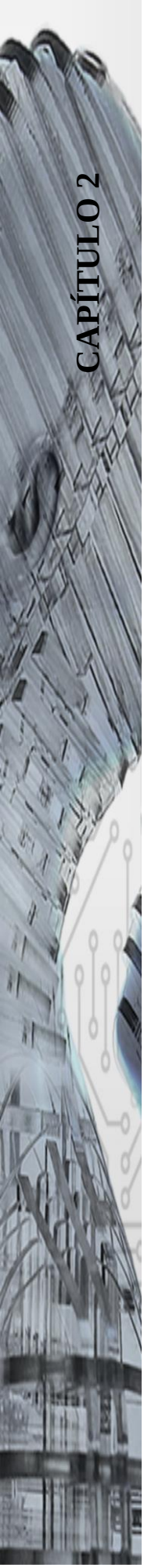
(V) Prudência digital: em um mundo *online* em ritmo acelerado, com tanto conteúdo digital competindo por atenção, muitas pessoas não dedicam tempo para analisar criticamente os riscos e ameaças potenciais aos quais estão expostos. A desaceleração para avaliar as formas e naturezas das comunicações poderá reduzir o risco de ser vítima de intenções maliciosas, muitas vezes provocadas pela própria exposição ou a confiança depositada em ambientes digitais pouco seguros ou que produzem suspeitas.

Pelos exemplos apresentados, dentre outros popularmente observáveis, torna-se de imensa relevância que as pessoas busquem aprender e compreender mais amplamente a segurança digital não apenas como uma prática individual, mas também desenvolvendo uma consciência cidadã de responsabilidade interpessoal e coletiva. Afinal, os direitos à privacidade, à intimidade e à segurança abrangem muitos dos aspectos públicos e privativos da vida do indivíduo, os quais encontram-se atualmente correlacionados também com o



processamento de dados pessoais por organizações governamentais e privadas e a manutenção de informações em bases de dados de acesso aberto e em caráter perpétuo. Portanto, as boas práticas em segurança digital são fundamentais para o fortalecimento e a promoção de direitos inalienáveis e fundamentais, os quais produzem esferas de proteção contra abusos daqueles que detêm o poder administrativo, fiscalizatório e econômico-financeiro.

Outrossim, é possível perceber a migração do mercado e da economia, conforme tradicionalmente concebidos na maneira física, para os meios digitais. Deste modo, a proteção de dados pessoais, muito além de seu valor como ativo financeiro, aduz aos direitos à personalidade e à privacidade. As leis de proteção de dados pessoais têm, portanto, a missão de tutelar as relações entre pessoas físicas que depositam seus dados aos cuidados de personalidades sejam de Direito Público ou de Direito Privado, conforme trazido com maior profundidade na seção seguinte, que trata especificamente das leis de proteção de dados e apresenta as criações legislativas como respostas às transformações econômicas, sociais e tecnológicas no mercado comum mundial, compreendidas até este momento da análise.



CAPÍTULO 2

A POSITIVAÇÃO DO DIREITO DE PROTEÇÃO DE DADOS PESSOAIS

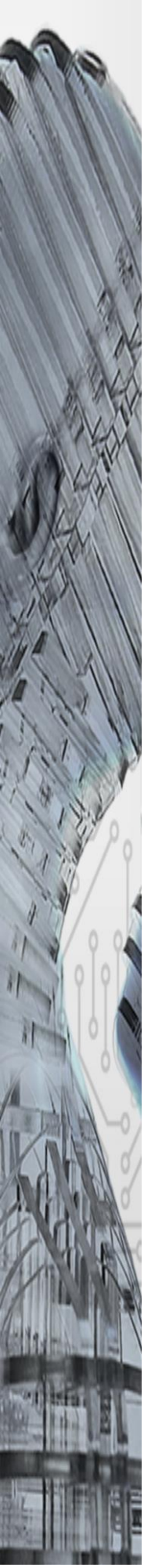
Enquanto os dados permaneciam grafados e acautelados em suas vias físicas, o sistema burocrático mantinha a salvo as informações de cunho pessoal e os seus portadores detinham maior controle sobre a destinação e a publicidade conferidas às mesmas, "até que se descobriram os *bits*, que conseguiram agregar, por meio do sistema binário de dígitos (1 e 0), a informação em unidades menores" (BIONI, 2018, p. 6). A desmaterialização da informação e o ampliado acesso à Internet desencadearam uma cultura popular de maior participação na política e no conhecimento das finanças públicas, características do *zeitgeist*[37] ocidental do início do século XXI, incentivando muitos governos a tornarem abertas as suas contas, bem como a prestarem informações melhor detalhadas acerca de planos orçamentários, salários de agentes e servidores públicos e a distribuição da verba pública para setores de interesse coletivo, tais como a saúde, a educação, a previdência, as licitações e a seguridade social. No mesmo sentido, complementam Josef Blanke e Ricardo Perlingeiro, nos seguintes termos:

> Simultaneamente, a nível internacional, ocorreu uma ampla interpretação do direito clássico à informação ou, como no Conselho da Europa, uma codificação de um direito especial ao acesso à informação. Os convênios globais e regionais de direitos humanos fornecem explicitamente apenas o direito à liberdade de expressão, incluindo a liberdade de buscar, receber e transmitir informações e ideias de todos os tipos [...] (BLANKE; PERLINGEIRO, 2018, p. 8, *tradução nossa*[38]).

A mudança na forma e no acesso à informação incentivaram as ocorrências virtuais envolvendo o tratamento de dados pessoais de maneira conexa, atingindo os mercados transnacionais fundados nas práticas capitalistas, "de modo a se fazerem presentes nas economias e políticas nacionais, na senda pública ou privada" (DÖRR; WEAVER, 2014, p. 1 - 3). Estas novas relações financeiras e administrativas, atreladas às tecnologias eletrônicas, têm o condão de incentivar a adoção de normas mais específicas, "por cada país que deseje tutelar e controlar as suas próprias regras a respeito de dados eletrônicos armazenados em ambientes virtuais interconectados" (BECKER, 2018, p. 17), bem como manter diálogos entre normas de conteúdo jurídico semelhante, mas vigentes em Estados distintos, ou seja,

[37] A expressão de matriz alemã, cunhada por Johann Gottfried Herder, em 1769, reflete *zeitgeist* como sendo o pensamento e sentimento (mentalidade) de uma época. O termo denota a peculiaridade de uma época particular ou a tentativa de visualizá-lo, bem como o estilo de vida fundado na consciência coletiva de uma população.

[38] Do original em inglês: *Simultaneously, at the international level, a broad interpretation of the classical right to information or, as in the Council of Europe, a codification of a special right to access to information has taken place. The global and regional covenants on human rights provide explicitly only for the right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds [...]*



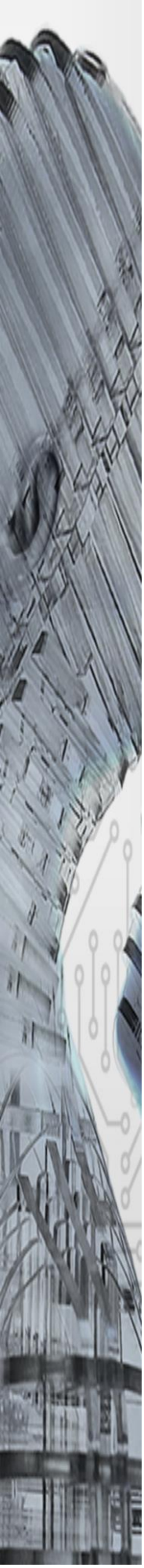
incentivando o desenvolvimento das Leis de Proteção de Dados Pessoais em países e blocos econômicos.

Tais fatores culminam, obviamente, em "implicações significativas para os direitos dos indivíduos, bem como para o desenvolvimento das economias e das sociedades de maneira mais ética" (HAUNTS, 2018, p. 13), promovendo regiões geográficas a "ilhas de proteção", face a outros países em total desvalia de segurança jurídico-normativa sobre dados pessoais. Há também um desafio sistêmico e estrutural que agrava essa situação: a tomada de decisão e os processos legislativos, com demasiada frequência, não estão sujeitos a um escrutínio público muito amplo, de modo que os interesses governamentais e empresariais sobrepujam as necessidades suportadas pelas classes populares. "Desta perspectiva, a proteção de dados e a liberdade de informação são objetivos mutualmente complementares ao invés de diametralmente opostos" (BLANKE; PERLINGEIRO, 2018, p. 42)

Em um ambiente favorável ao crescimento de uma forte indústria de processamento de dados, "os interesses do mercado global requerem também a criação de leis de proteção de dados pessoais" (BECKER, 2018, p. 28). Deste modo, a evolução da proteção de dados no Direito Constitucional está intimamente ligada aos avanços tecnológicos e foi estabelecida como uma resposta ao aumento da informatização, "pois as legislações estrangeiras sobre o tratamento de dados têm o potencial de atingir internautas e empresas utilizadoras, operadoras ou produtoras de tecnologias" (HAUNTS, 2018, p. 34).

Toda e qualquer companhia que manipule dados pode ser impactada, caso guarde ou receba informações de indivíduos naturais de outros países, sem residência fixa ou profissional em país estrangeiro, incluindo desde instituições financeiras até pousadas ou restaurantes em pontos turísticos.

Portanto, torna-se necessário compreender os novos desafios para a proteção de dados mediante a análise comparativa de mecanismos constitucionais e demais normas nacionais e internacionais, principalmente em países cujas legislações e mercados estão mais desenvolvidos para o contexto digital, como Canadá, Estados Unidos, e determinadas regiões, como a Ásia, América Central e do Sul, assim como nos países membros da União Europeia, a fim de contextualizar a temática em um patamar internacional, para então ser possível delinear percepções em relação ao Brasil de modo comparativamente mais aproximado da realidade e esclarecer quais são os objetos jurídicos comuns tutelados pela proteção à privacidade, à segurança e aos dados pessoais, à luz dos Direitos Humanos e Constitucionais Fundamentais.



2.1 A Proteção de Dados na perspectiva internacional comparada

A União Internacional de Telecomunicações – UIT, atua como uma Agência do Sistema da Organização das Nações Unidas – ONU, com enfoque no mapeamento e conhecimento de temas relacionados às Tecnologias da Informação e Comunicação (TICs). Segundo o relatório *Global Cybersecurity Index (GCI) 2018*, produzido pela UIT, foram apontadas as posições de vários países, em relação a questões envolvendo segurança e proteção de dados. Em 2018, 58% dos estados membros da UIT informaram ter uma estratégia nacional de segurança cibernética, um aumento significativo em relação ao ano anterior (50%). A legislação sobre crimes cibernéticos está bem implementada em todo o mundo, com 91% dos países com legislação sobre cybercriminalidade, um aumento de 79% em relação à legislação de 2017.

Uma das áreas significativas do estudo trata das medidas preventivas dos países, compreendidas em ações, tecnologias e legislações voltadas para a repressão e prevenção de ataques cibernéticos, envolvendo a perda e o roubo de dados (UIT, 2018, p. 5). Os países com maior consciência cibernética foram classificados como Suíça, Luxemburgo, Reino Unido, Estados Unidos da América - EUA, França, Lituânia, Estônia, Singapura, Espanha, Malásia, Noruega e Canadá, seguidos de perto, nas primeiras colocações por Austrália, Luxemburgo, Holanda, Arábia Saudita e Japão. Maurício, Quênia e Ruanda foram os países da África mais comprometidos com a segurança cibernética, de acordo com o Índice Global de Segurança Cibernética (*Ibidem*).

A legislação mais atualizada foi pontuada com base na legislação existente (e esboços) que abrangeram sete categorias (estratégia nacional, militar, conteúdo, privacidade, infraestrutura crítica, comércio e crime). Para cada critério, o país recebeu um ponto baseado em sua classificação entre os países com pontuações mais elevadas, face aos países posicionados em condições menos elevadas. Segundo os níveis de segurança e proteção cibernéticas, conferidas por cada legislação nacional, os países com as camadas normativas menos adequadas receberam 0,001 pontos, enquanto os países com legislações mais robustas receberam 100 pontos (UIT, 2018, p. 5).

Todos os países analisados e com escores atribuídos, receberam também uma pontuação em valores percentuais, dependendo de suas classificações comparadas aos demais.

Dos 194 países analisados, foi distribuída uma classificação de 0,000 a 1,000, sendo o último o mais alto (*Ibidem*), de modo a ser possível extrair o seguinte quadro:

Tabela 1: Posição global da segurança digital em 2018.

País	Posição	Classificação
Reino Unido	1ª	0,931
EUA	2ª	0,926
França	3ª	0,918
Lituânia	4ª	0,908
Estônia	5ª	0,905
Singapura	6ª	0,898
Arábia Saudita	13ª	0,881
Japão	14ª	0,880
Brasil	70º	0,577
Maldivas	175	0,004

Fonte: Elaboração própria, segundo os dados GCI, UIT, 2018.

O estudo *Global Cybersecurity Index (GCI) 2018*, produzido pela UIT, também apontou os países de onde partem a maioria dos ataques virtuais por *hackers*, de modo que foi possível extrair informações para compor a tabela abaixo da seguinte forma:

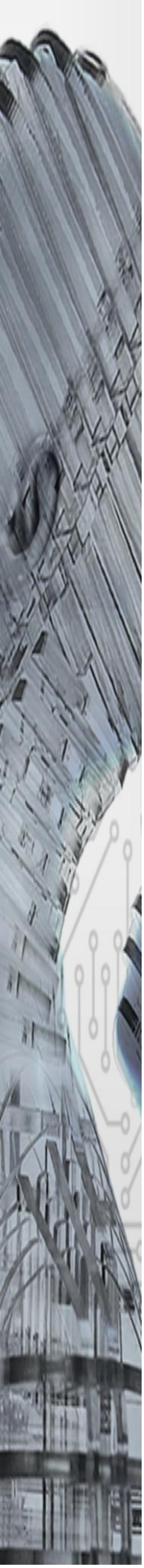


Tabela 2: Índice dos países onde mais ataques virtuais são iniciados.

1	China	41 por cento (do tráfego de ataque do mundo)
2	EUA	10 por cento
3	Peru	4,7 por cento
4	Rússia	4,3 por cento
5	Taiwan	3,7 por cento
6	Brasil	3,3 por cento
7	Roménia	2,8 por cento
8	Índia	2,3 por cento
9	Itália	1,6 por cento

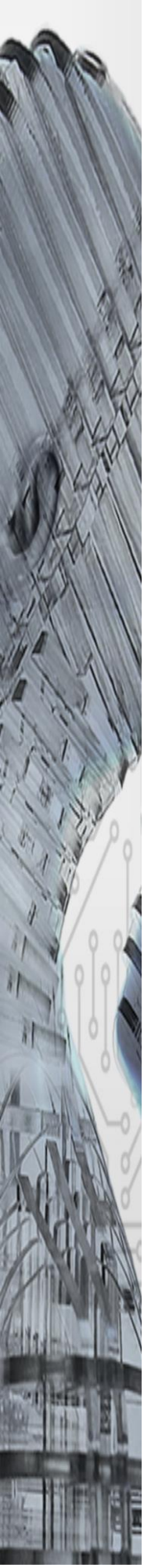
Fonte: Elaboração própria, segundo os dados GCI, UIT, 2018.

Em observação somente aos países do continente americano, a pesquisa levantada no Relatório *Global Cybersecurity Index (GCI) 2018* também apontou que o Brasil está em 6º lugar na pontuação dos países do continente americano de maior comprometimento com a segurança eletrônica, de forma a ser observada a seguinte tabela, segundo informações extraídas do estudo em comento:

Tabela 3: Índice do comprometimento legislativo em proteção de dados no continente americano.

Estado membro	Pontuação Geral	Classificação Regional	Classificação global
EUA	0,926	1º	2º
Canadá	0,892	2º	9º
Uruguai	0,681	3º	51º
México	0.629	4º	63º
Paraguai	0,603	5º	66º
Brasil	0.577	6º	70º
Colômbia	0,565	7º	73º
Cuba	0,481	8º	81º
Chile	0,438	9º	88º
República Dominicana	0,430	10º	92º

Fonte: Elaboração própria, segundo os dados GCI, UIT, 2018.

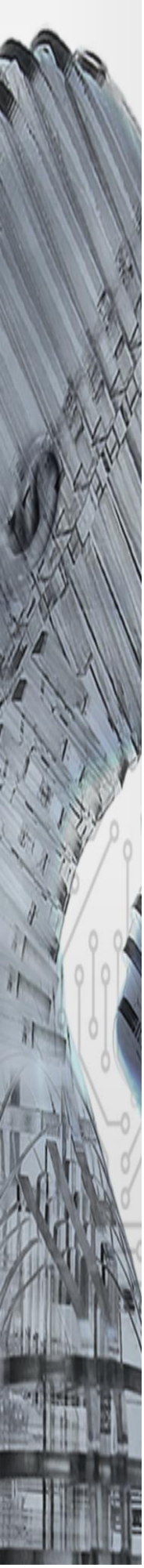


Logo, é perceptível a continuidade da existência de uma grande lacuna no compromisso com a segurança cibernética em todas as regiões do mundo, sendo os países europeus os mais comprometidos com a segurança cibernética e os países africanos os menos preparados para enfrentar crimes cibernéticos e ataques cibernéticos apoiados por forças estrangeiras hostis (UIT, 2018). Tais nuances legislativas produzem peculiaridades em cada país, mas mantêm como eixo-principal o fortalecimento da segurança digital, a privacidade e a dignidade da pessoa humana, presentes em seus vários textos constitucionais.

A saber, a Constituição da República da Coreia, de 12 de julho de 1948, emendada em 1987, protege a privacidade em geral e a privacidade do lar e das comunicações, em particular nos seus artigos 17 e 18. O art. 37 (1) da Constituição sul-coreana também assegura que os direitos e liberdades dos cidadãos não devem ser negligenciados, mesmo quando não estiverem expressos na Constituição (COREIA DO SUL, 1948). Em 2003, o Tribunal Constitucional da Coreia interpretou estas disposições como protegendo as pessoas de acesso inadequado, abuso ou uso indevido de suas informações pessoais[39] (WALTERS; TRAKMAN; ZELLER, 2019).

A Constituição do Japão de 3 de novembro de 1946, em seu art. 22, prevê que "todas as pessoas devem ser respeitadas como indivíduos" (JAPÃO, 1946). O direito à vida, à liberdade e à busca da felicidade devem, na medida em que não interfiram no bem-estar público, ter consideração suprema na legislação e em outros assuntos governamentais (WALTERS; TRAKMAN; ZELLER, 2019). Embora a Suprema Corte nunca tenha se referido ao direito de controlar a própria informação (*Umeda*) ou de lidar explicitamente com a questão da autodeterminação informacional, ela forneceu inerentemente o potencial para o art. 13 (JAPÃO, 1946) ser usado para garantir proteções à privacidade da informação em geral em suas decisões. Da mesma forma, tribunais superiores em vários países asiáticos, como Taiwan, Coreia do Sul e Japão, onde as constituições não se referem à proteção de dados ou a esses aspectos da privacidade de maneira explícita, usaram a privacidade ou outros direitos fundamentais para enfatizar a proteção, o controle de dados e a autodeterminação em

[39] Em 2005, na ocorrência conhecida como "Caso das Impressões Digitais", a Corte Suprema da Coreia do Sul determinou que o poder governamental deveria coletar e manter um conjunto completo de impressões digitais de todos os cidadãos com 17 anos ou mais, afim de utilizá-las em investigações, o que não viola excessivamente o direito de controlar informações pessoais (GREENLEAF, 2014). Já em 2012, a Corte Suprema determinou que o estatuto que exige que os usuários da Internet usem seu nome real em sítios eletrônicos e perfis virtuais é inconstitucional, pois o monitoramento público produzido ao fornecer os nomes reais dos indivíduos para publicações on-line não é substancial o suficiente para justificar restrições aos direitos individuais à liberdade de expressão quanto à manutenção da privacidade por não utilização de nomes reais, alegando se tratar de uma violação do direito dos usuários à autodeterminação de informações pessoais (GREENLEAF, *idem*).



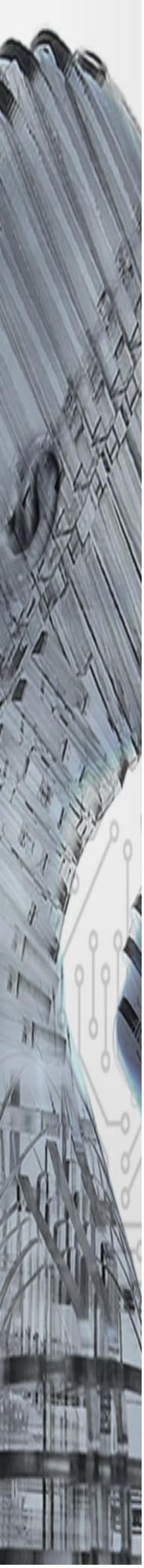
matéria de informação pessoal (GREENLEAF, 2014; ASAI, 2018; WALTERS; TRAKMAN; ZELLER, 2019).

No continente africano a abordagem das legislações em dados está levando a uma interpretação do controle de dados derivado da autodeterminação dos indivíduos. Com muitas culturas e populações distintas distribuídas em países que lutam para combater a fome, enfermidades epidêmicas, questões civis, a corrupção de governos e a exploração de *commodities* por empresas estrangeiras, segundo Makulilo (2016, p. 14 - 26), o caminhar das normas a respeito da proteção de dados ainda é uma realidade longínqua. Todavia, em países onde o capitalismo já se fixou e as tecnologias eletrônicas estão mais amplamente distribuídas, os aspectos informacionais da privacidade são estabelecidos em um nível constitucional, tal como ocorre no texto da Constituição da República Árabe do Egito, de 18 de janeiro de 2014, em seu art. 57, onde está prevista a proteção da privacidade e o sigilo de diferentes métodos de comunicação (EGITO, 2014). Os princípios constitucionais relativos à privacidade dos indivíduos foram interpretados como regendo a coleta, o uso e o processamento de dados pessoais (MAKULILO, 2016). A Constituição da República Federal da Nigéria, de 29 de maio de 1999 em sua Seção 37 faz previsão à proteção dos aspectos informativos da privacidade dos cidadãos (NIGÉRIA, 1999).

Na África do Sul, o direito à privacidade foi consagrado na Seção 14 da Declaração de Direitos na Constituição da República da África do Sul, de 11 de outubro de 1996, enumerando em um rol exemplificativo o escopo e a abrangência da proteção às informações pessoais, bem como apresenta, predominantemente, as possíveis infrações do Estado (AFRICA DO SUL, 1996). A Seção 32 da Constituição Sul-africana (*Ibidem*) também prevê o direito de acesso às informações pessoais[40].

Já na América Latina, o respeito pela privacidade dos indivíduos é tema de grande relevância. A defesa deste princípio representa dois pilares: os direitos constitucionais à privacidade e a regulação abrangente da proteção de dados. Mais da metade dos países da região já adotaram um ou ambos desses mecanismos para proteger a privacidade de dados pessoais, empresariais e públicos, com a expectativa de que os demais países da região que

[40] Um processo de positivação da privacidade como direito fundamental semelhante ao Japão e à Coreia-do-Sul, ocorreu durante um período mais longo na África do Sul. Segundo Makulilo (2016), embora a Constituição sul-africana (AFRICA DO SUL, 1996) defina a privacidade, por muito tempo os tribunais só levaram em consideração os seus aspectos informacionais no grau necessário para proteger os indivíduos de buscas e apreensões pelo governo. Conforme estabelece o Tribunal Constitucional da África do Sul, embora a violação da privacidade informacional não tenha sido expressamente mencionada na Constituição (AFRICA DO SUL, 1996), ela é coberta pela ampla proteção do direito à privacidade (MAKULILO, 2016). O Tribunal Constitucional também listou algumas diretrizes gerais que regem a proteção de dados (MAKULILO, *idem*.).



ainda não adotaram legislações do tipo seguirão a maioria em breve. Para empresas que fazem negócios na América Latina ou que desejam investir na região, a privacidade de dados é um dos principais tópicos a serem considerados.

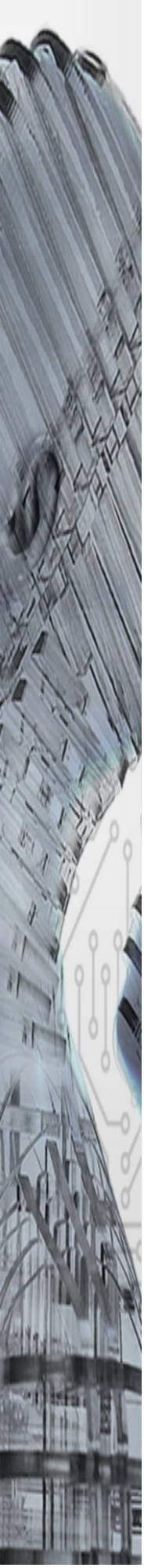
A conexão entre a proteção de dados pessoais e o direito de acesso a documentos públicos é o fator que mais influenciou os países da América Central e do Sul na interpretação da proteção de dados pessoais (ADC, 2016, p. 13). O texto da Constituição da República Federativa do Brasil, de 05 de outubro de 1988, estabeleceu o pleno direito constitucional à denúncia individual de "*habeas data*", em procedimentos individuais (BRASIL, 1988), de modo a permitir que os "indivíduos tenham o direito de acessar arquivos contendo informações sobre si mesmos e de corrigir dados imprecisos quando estes são de caráter público" (GREGÓRIO, 2004, p. 98).

Outros países da América Central e do Sul também incorporaram o direito ao "*habeas data"* às suas constituições, tal como se observa na Constituição Política da Colômbia, de 06 de julho de 1991; na Constituição da República do Paraguai, de 20 de junho de 1992, na Constituição Política da República do Peru: 31 de outubro de 1993, na Constituição da Nação Argentina, de 22 de agosto de 1994 e na Constituição da República do Equador, de 11 de agosto de 1998. Segundo Gregório (2004, p. 110) "a jurisprudência constitucional também estabeleceu, em relação à conservação de dados pessoais, o conceito e o reconhecimento do direito ao esquecimento, em muitos dos tribunais de países latino-americanos", também estendendo a compreensão de que os legisladores têm o poder de estabelecer limitações quanto ao período durante o qual os dados pessoais podem ser mantidos em bancos de dados e arquivos físicos (*Ibidem*).

Segundo o relatório *Global Cybersecurity Index (GCI) 2018*, o Uruguai é o país da América Latina com o melhor sistema legislativo e de cibersegurança voltado para a proteção de dados (UIT, 2018), contando desde 2008 com a Lei nº 18.331/2008, a Lei de Proteção de Dados Pessoais (URUGUAI, 2008) e figurando como o primeiro país latino-americano a promulgar uma lei geral sobre a proteção de dados pessoais, a qual estabelece o direito à proteção de dados pessoais como inerente ao ser humano, de acordo com a seção 72 da Constituição da República (URUGUAI, 1997)[41].

O México figura, conforme o relatório *Global Cybersecurity Index (GCI) 2018* como o segundo o país da América Latina com o melhor sistema de proteção de dados pessoais

[41] O regime de proteção de dados será aplicado a dados pessoais armazenados em qualquer plataforma na qual possam ser processados e a todos os modos em que os dados possam ser de uso posterior. A União Europeia reconheceu o Uruguai com um nível adequado de proteção, o que permite a transferência internacional de dados para este país (BECKER, 2018, p. 29).

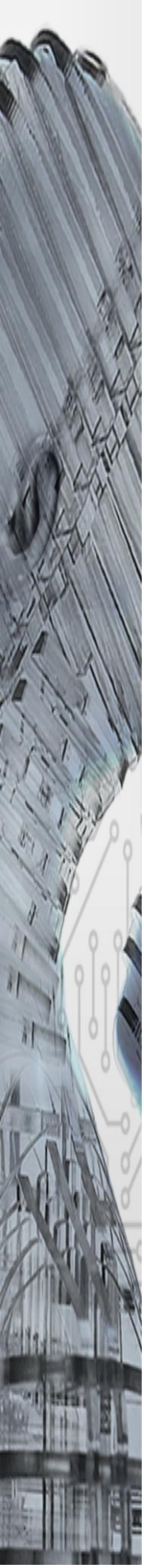


(UIT, 2018). A principal legislação de proteção de dados no México é a Lei Federal de Proteção de Dados Pessoais em Posse de Particulares ou Lei Federal de Proteção de Dados Pessoais de Pessoas (LFPDPP). A lei entrou em vigor em julho de 2010 e foi seguida em dezembro de 2011 por regulamentações secundárias que esclareceram as obrigações dos controladores de dados pessoais sob o LFPDPP (MÉXICO, 2010). Todavia, o México ainda não agregou ao seu ordenamento jurídico nenhuma legislação que padronize linearmente o tratamento de dados, em alcance público e privado (ADC, 2016).

A proteção de dados pessoais é considerada um direito fundamental sob a Constituição do Peru. A Lei de Proteção de Dados Pessoais ou Lei de Proteção de Dados Pessoais nº 29733 baseou-se nesse princípio constitucional fundamental e foi promulgada em junho de 2011, entrando em vigor em 2013 e fazendo previsão à proteção e a salvaguarda dos direitos individuais, bem como fixando obrigações a serem cumpridas pelas empresas que realizam tratamento de dados (PERU, 2011).

Na Colômbia, o direito à intimidade e à proteção de dados encontram-se constitucionalmente assegurados, bem como são reprisados em regulamentos de escopo mais específico, tal como na Lei nº 1.273/2009, a qual tipifica uma série de infrações penais relacionadas a dados pessoais, como divulgação ou venda de dados pessoais; na Lei nº 1.581/2012 e no Decreto nº 1.377/2013, os quais versam sobre a proteção a direitos de titulares de dados, além de fixar deveres e regras para as entidades que realizam coleta, tratamento e processamento de dados (ADU, 2016, p. 11), os quais posteriormente foram utilizados pela Superintendência de Indústria e Comércio colombiana, cuja atuação se assemelha à Autoridade de Proteção de Dados do país, para elaborar uma lista de países considerados como sendo possuidores de normas, regulamentos e medidas de proteção em níveis adequados para permitir transferências internacionais, conforme estabelecido pela Lei nº 1.581 (COLOMBIA, 2012).

Na Argentina, a Lei Federal 25.326/2000, trata das disposições e princípios da proteção geral a dados pessoais armazenados em arquivos, registros, bancos de dados e outras plataformas de processamento de dados, públicas ou privadas, a fim de garantir o direito à privacidade e a direitos correlatos, como honra, imagem e intimidade (ARGENTINA, 2000). O artigo 43 da Constituição da Nação Argentina (ARGENTINA, 1994) também concede aos indivíduos o direito de acesso a informações sobre eles armazenadas em bancos de dados públicos. Conforme aponta a *Associación de Derecho Civil* (2016), o país também possui uma Autoridade de Proteção de Dados com poderes de execução.



O Chile foi o primeiro país da América do Sul a aprovar uma legislação abrangente de proteção de dados (ADU, 2016), mediante a publicação em 1999, da Lei nº 19.628 sobre a proteção da vida privada. No ano 2018, o Congresso Nacional do Chile alterou o artigo 19 da Constituição chilena (CHILE, 2018) para incluir a proteção pessoal de dados como um direito individual[42].

Conforme o relatório *Global Cybersecurity Index (GCI) 2018,* (ITU, 2018) países latino-americanos estão desenvolvendo regulamentos de privacidade e proteção de dados em conjunto com as diretivas da União Europeia, demonstrando diálogos e similaridades legislativas capazes de facilitar as transações financeiras, em um sistema equilibrado no plano internacional, adaptado às realidades geopolíticas e socioeconômicas de cada país e com maiores perspectivas de sustentabilidade lastreada na segurança jurídica.

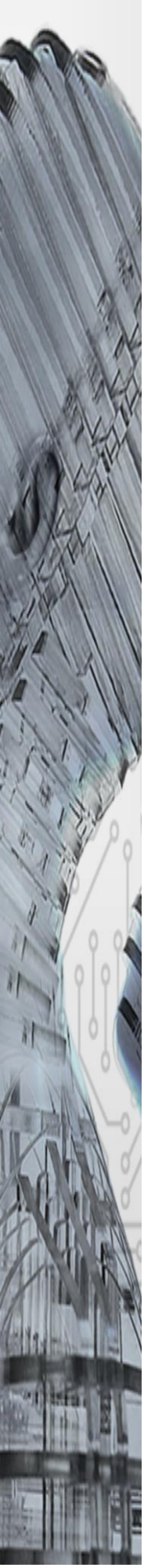
Na América Latina, as transferências de dados pessoais entre países somente podem ser realizadas mediante expresso consentimento do seu titular, devendo este ser cientificado e realizar a respectiva autorização para o tratamento de dados no momento da cessão e aceite de depósito de dados, conforme as finalidades especificadas.

2.2 A proteção de dados nos Estados Unidos e Canadá

A Lei de Privacidade dos EUA data de 1974, sendo destinada a salvaguardar a privacidade individual de ser violada através do uso indevido de registros federais e fornecer aos indivíduos acesso a tais registros[43]. Neste caso, a privacidade é entendida de forma inequívoca como privacidade da informação (EUA, 1974). A Suprema Corte dos Estados Unidos reconheceu pela primeira vez o direito à privacidade da informação em 1977, observando que a Constituição protegia dois tipos de interesses individuais: um é o interesse individual em evitar a divulgação de assuntos pessoais; outro é o interesse pela independência

[42] No entanto, ainda persistem os ditames da Lei nº 19.628, a respeito de quais dados pessoais são protegidos e como devem ser processados por terceiros, não tratando de questões referentes ao processamento de informações por meio de mídia digital e não colocando em prática mecanismos de supervisão adequados. Como consequência, atualmente, o Chile não possui uma autoridade de proteção de dados dedicada à aplicação de sua legislação de proteção de dados, mas um projeto de lei para modificar a Lei nº 19.628 (CHILE, 1999), visando acrescentar disposições relativas à proteção e ao processamento de dados pessoais e à criação de dados. O projeto de lei que prevê a criação de uma autoridade de proteção de dados foi submetido e aprovado pelo Senado chileno em abril de 2018.

[43] O modelo de proteção de dados dos Estados Unidos baseia fundamentalmente sua abordagem em torno do conceito de liberdade como proteção contra a interferência do Estado na vida dos indivíduos (KLOSEK, 2000). Esta proteção da liberdade aponta mais fortemente para uma compreensão da privacidade da informação como um direito de defesa contra as atividades do Estado e menos para um direito de acesso ou retificação (BAMBERGER; MULLIGAN, 2015)



e a segurança na tomada de certos tipos de decisões importantes (BAMBERGER; MULLIGAN, 2015).

A garantia da Quarta Emenda à Constituição dos EUA (EUA, 1792) pode ser entendida como abrangendo certos "dados relacionados a uma determinada pessoa, tais como registros telefônicos ou bancários" (FEILER, 2012, p. 77). No entanto, tal norma é somente aplicável aos casos nos quais o indivíduo tem uma "expectativa razoável de privacidade" (EUA, 1792), o que significa que o indivíduo tem uma "expectativa real e subjetiva de privacidade e a sociedade está disposta a reconhecer essa presunção como razoável" (BAMBERGER; MULLIGAN, 2015, p. 35).

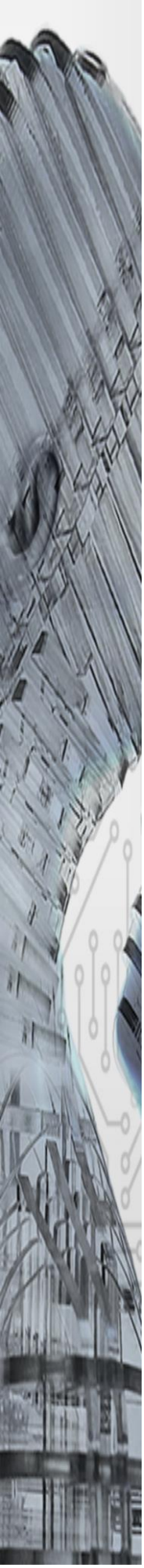
Esse conceito foi amplamente reduzido para excluir todos os casos em que um indivíduo tenha voluntariamente transferido as informações em questão para terceiros, retirando efetivamente uma ampla variedade de dados pessoais da proteção da Quarta Emenda (EUA, 1792). Todavia, apontam Dörr e Weaver que:

> A jurisprudência da Quarta Emenda da Suprema Corte dos EUA não conseguiu acompanhar o avanço da tecnologia ou fornecer muita proteção aos indivíduos contra o uso governamental de novas tecnologias. Juízes individuais pressionaram por mudanças na jurisprudência da Corte, e a Suprema Corte dos EUA proferiu decisões de proteção, mas o equilíbrio de decisões não forneceu muita proteção para os cidadãos. A falta de proteção é preocupante, pois novas formas de tecnologia continuam a ficar online. (DÖRR; WEAVER, 2014, p. 21, *tradução nossa*[44])

A proteção de dados de residentes nos EUA é regulada "por leis promulgadas em nível nacional e estadual" (FEILER, 2012, p. 67), não existindo uma legislação única sobre proteção de dados. Os estatutos federais "são destinados principalmente a setores específicos e à regulação de agências federais, enquanto os estatutos estaduais estão mais focados na proteção dos direitos de privacidade de consumidores individuais" (*Ibidem*). As leis que protegem os dados e a privacidade do consumidor baseiam-se no "princípio de que um indivíduo tem uma expectativa de privacidade, a menos que essa expectativa tenha sido diminuída ou eliminada por acordo, estatuto ou divulgação" (BAMBERGER; MULLIGAN, 2015, p. 37).

A proteção de dados e os estatutos de privacidade nos EUA são promulgados para proteger as pessoas que residem nos EUA ou em um de seus estados. Logo, as leis federais

[44] Originalmente, em inglês: *The U.S. Supreme Court's Fourth Amendment jurisprudence has failed to keep pace with advancing technology or to provide much protection to individuals against governmental use of new technologies. Individual justices have pushed for changes in the Court's jurisprudence, and the U.S. Supreme Court has rendered protective decisions, but the balance of decisions have not provided much protection for the citizenry. The lack of protection is worrisome as new forms of technology continue to come online*.



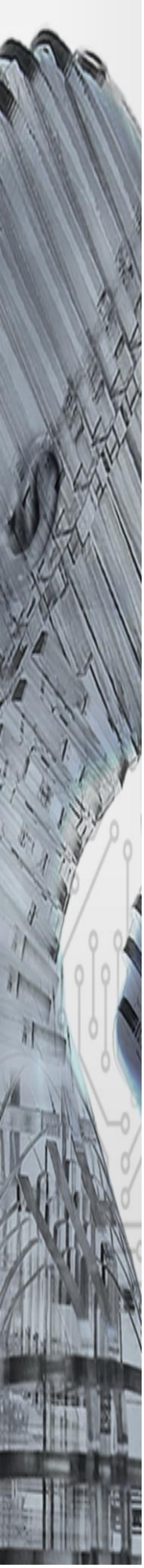
aplicam-se para proteger residentes de todos os estados, enquanto as leis estaduais são projetadas para proteger apenas os seus residentes[45].

Para entender a proteção de dados pessoais na legislação dos Estados Unidos é necessário entender alguns conceitos que envolvem as políticas de tratamento de dados pessoais. Existe uma agência independente chamada FTC – *Federal Trade Comission* que tem papel fundamental na proteção do consumidor, como também para evitar a criação de monopólios e práticas anticompetitivas, conhecidas como *unfair or deceptive acts* (DÖRR; WEAVER, 2014, p. 22 - 26). Segundo Klosek (2000, p. 66), "a atuação desse órgão é efetiva e existem departamentos específicos dentro da FTC para cuidar de ramos críticos do mercado em geral, existindo o *Bureau of Consumer Protection*, *Bureau of Competition* e o *Bureau of Economics"*, cada um com atuação especializada e histórico de forte inserção no mercado.

Existem outras legislações esparsas sobre o tratamento e a proteção de dados pessoais, tal como o *Children's Online Privacy Protection Act,* conhecido como COPPA, que regula as questões relativas à coleta e tratamento de dados de crianças menores de 13 anos (EUA, 1990) e o *Health Insurance Portability and Accountability Act*, conhecido como HIPPA, que busca tutelar questões sobre a proteção dos dados pessoais e relacionados à saúde dos pacientes, estabelecendo preceitos para a tutela de informações de saúde protegidas. As unidades devem, também, manter registro e se organizarem para promover maiores garantia no sigilo dos dados pessoais relativos à saúde dos pacientes, impondo uma série de exigências para as entidades de saúde (EUA, 1996).

No Canadá, o contrapeso mais significativo às proteções à privacidade é a liberdade de expressão garantida pela emenda à Seção 2b da Carta Canadense de Direitos e Liberdades, de 1982 e suas atualizações posteriores. Ambas, a emenda e a seção foram interpretadas como também "protegendo o direito das pessoas de conhecer informações de interesse pessoal (próprio ou de outrem) ou interesse público, mesmo que isso venha a interferir na privacidade individual até certo ponto" (GEIST, 2015, p. 54). Todavia, "não existe nenhum direito constitucional explícito à privacidade ou proteção de dados no Canadá" (DÖRR; WEAVER, 2014, p. 27).

[45] Em contraste com a UE e a América Latina, não existe legislação horizontal de proteção de dados nos EUA, aplicável tanto a atores públicos como privados. O setor privado é governado por uma mistura de iniciativas legislativas *ad hoc*, autorregulação da indústria e forças de mercado (DÖRR; WEAVER, 2014, p. 56). Também não há autoridade supervisora e os Tribunais Federais podem apenas trazer uma série limitada de mudanças na conduta sob a Lei de Privacidade de 1974 (EUA, 1974) e não têm poderes para obrigar as agências federais a alterarem suas práticas gerais, resultando assim em um paradigma constitucional incompleto.



A Seção 8 da Carta Canadense de Direitos e Liberdades garante a todos o direito de estarem protegidos contra buscas ou apreensões não razoáveis (CANADÁ, 1982). Este direito foi interpretado como também protegendo uma expectativa razoável de privacidade, que também se aplica às modernas tecnologias de comunicação.

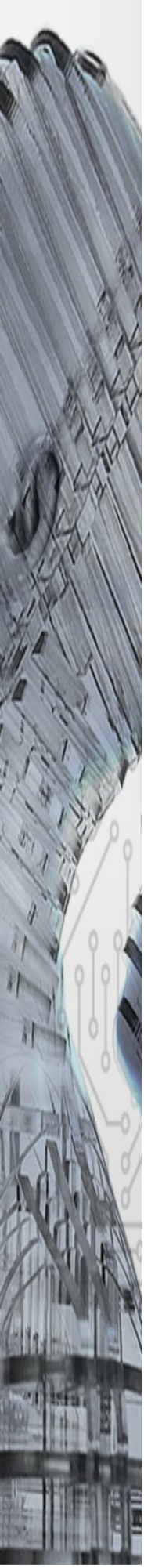
Desde os seus primeiros estágios, o desenvolvimento da proteção de dados como sistema normativo nos países da América do Norte tem sido cada vez mais "impulsionado pelo desenvolvimento de novas tecnologias nacionais e, portanto, pelo entendimento da privacidade em geral como parte da proteção de dados pessoais e segurança de informações" (DÖRR; WEAVER, 2014, p. 32). Não obstante, a jurisprudência da Suprema Corte dos EUA sobre a Quarta Emenda (EUA, 1792), conforme aponta Geist (2015, p. 59) "não conseguiu fornecer proteção substancial aos indivíduos contra o uso governamental de novas tecnologias e não acompanhou os avanços da tecnologia".

2.3 Países europeus: das normas nacionais ao RGPD

As discussões acerca da proteção de dados na Europa tiveram início, principalmente, por meio de emendas constitucionais e atos jurídicos (KAZEMI, 2018, p. 19). A Suécia foi o primeiro país da Europa a introduzir uma lei nacional de proteção de dados em 1973, sendo seguida pela Alemanha em 1977 e pela França em 1978. As justificativas para a criação das leis nacionais de proteção de dados têm fundamentos similares. Na Suécia, foi vinculada ao princípio da integridade pessoal (FEILER, 2012). Na Alemanha utilizou-se como base o princípio da dignidade humana (GREENLEAF, 2014). Já na França, o escopo é o conceito de liberdade individual[46].

O reconhecimento constitucional do direito à proteção de dados pessoais teve início em Portugal, Áustria e Espanha (FEILER, 2012). Em Portugal, o art. 35 da Constituição da República Portuguesa[47], de 25 de abril de 1976, regulamentou o uso do processamento de

[46] *Loi Portant Création d'une Couverture Maladie Universelle*.
[47] CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA Artigo 35º Utilização da Informática
1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.



dados, nomeadamente os direitos de receber, acessar e retificar informações (PORTUGAL, 1976). O direito fundamental à privacidade (*Grundrecht auf Datenschutz*), foi reconhecido no ordenamento jurídico austríaco em 1978, sendo posteriormente ampliado pelo advento da *Datenschutzgesetz* (ÁUSTRIA, 2000) que o trouxe no seu art. 1 § 1[48] como um direito constitucional fundamental à proteção de dados, "baseado no direito ao respeito pela vida privada e familiar (proteção da família)" (BARBERGER; MULLIGAN, 2015, p. 85). A Constituição da Espanha de 1978 introduziu no art. 18[49] a norma que regulamentou o direito à privacidade e também limitou o uso de computadores, a fim de garantir a privacidade dos cidadãos a nível individual e familiar (ESPANHA, 1978). Tais normas caracterizam a primeira fase da criação de marcos regulatórios sobre a proteção de dados no direito europeu.

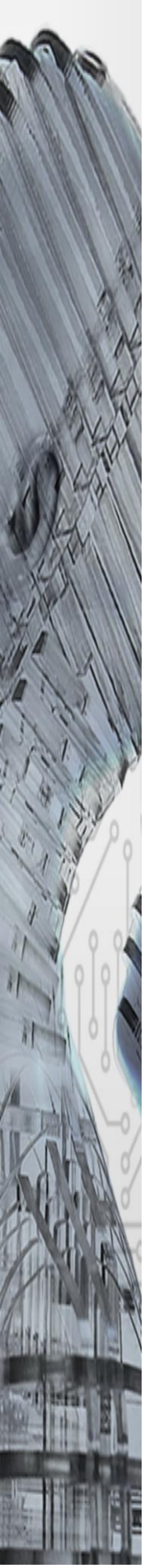
Durante a segunda fase de criação das normas em proteção de dados pessoais, o Parlamento do Reino Unido, obteve o real consentimento (*Royal Assent*) e adotou a Lei de Proteção de Dados (*Data Protection Act*) em 1984, tendo ocorrido independentemente de qualquer direito à privacidade, o qual não obteve reconhecimento como um direito no sistema legal do Reino Unido até a revisão da referida Lei em 1998 que substituiu a Lei de Proteção de Dados de 1984 e a Lei de Acesso a Arquivos Pessoais de 1987 e implementou a Diretiva de Proteção de Dados da UE de 1995, até a sua mais atualizada versão em 2018.

O Ato LXIII de 1992 da Hungria regulou a proteção dos dados pessoais e a publicidade dos dados de interesse público, enfatizando aspectos de controle, colocando o direito à proteção de dados pessoais dentro da estrutura do direito fundamental à

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.

[48] *Artikel 1 (Verfassungsbestimmung) Grundrecht auf Datenschutz § 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.*
Artigo 1 (Determinação Constitucional) Direito fundamental à privacidade § 1. (1) É conferido a todos e, em particular, também no que diz respeito à sua vida privada e familiar, o direito ao sigilo de dados pessoais que lhe digam respeito, na medida em que este se configure como sendo um interesse legítimo. A existência de tal interesse é excluída se os dados não estiverem disponíveis para confidencialidade devido à sua disponibilidade geral ou por falta de rastreabilidade face à pessoa interessada (tradução nossa).

[49] *Artículo 18. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
Artigo 18. O direito à honra, à privacidade pessoal e familiar e à própria imagem é garantido. O endereço é inviolável. Nenhuma inscrição ou registro poderá ser feito sem o consentimento do proprietário ou ordem judicial, exceto em caso de flagrante delito (tradução nossa).



autodeterminação informacional. Na Suíça, a previsão de proteção de dados sobreveio mediante o texto inserido no art. 13[50] da Constituição Federal da Confederação Suíça, alterada em 1999, pelo qual foi concedido a todas as pessoas o direito à privacidade e, em particular, o direito à proteção contra a utilização indevida de dados.

Em 1995, a ratificação da Convenção do Conselho da Europa para a Proteção de Indivíduos no que diz respeito ao Processamento Automático de Dados Pessoais resultou na elaboração, pela União Europeia, da Diretiva de Proteção de Dados (DPD), oficialmente conhecido como a Diretiva de Proteção de Dados 95/46 – CUE (DPD), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que regulamentava o tratamento de dados pessoais na União Europeia. É um componente importante da privacidade da UE e dos Direitos Humanos.

Os países pioneiros no domínio da proteção de dados, como a Áustria, a Alemanha e a Suécia, utilizaram essencialmente a implementação legislativa da Diretiva (EU, 1995) como "uma oportunidade para consolidar as suas atuais abordagens à proteção de dados nas respectivas posições constitucionais" (FEILER, 2012, p. 378). Em contraste com isso, a Espanha e Portugal começaram a classificar a proteção de dados em relação à privacidade como entendida em seu sentido mais amplo - e, portanto, além das esferas mais protegidas da vida pessoal e familiar. "Na Itália e na Finlândia, a DPD conferiu à proteção de dados uma nova influência constitucional ao vincular a proteção de dados à privacidade e à proteção da vida privada pela primeira vez, colocando-a dentro do escopo potencial dos direitos fundamentais" (BARBERGER; MULLIGAN, 2015, p. 144). A maioria dos Estados membros que aderiram à UE em 2004 já tinham leis sobre proteção de dados. Na maior parte destes casos, "a proteção de dados estava ligada ao direito fundamental à privacidade, como aconteceu na Eslovênia e na Lituânia" (GREENLEAF, 2014, p. 87).

O Parlamento Europeu e o Conselho Europeu promulgaram o Regulamento Geral sobre a Proteção de Dados (RGPD) em abril de 2016, com vigência iniciada em 25 de maio de 2018 (CUE, 2016). A peça legislativa[51] demorou cinco anos para ser redigida e foi

[50] *Art. 13 Protection de la sphère privée - 1 Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications. 2 Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.*
Art. 13º proteção da esfera privada - 1 Todos têm o direito à preservação de sua vida privada e familiar, seu domicílio, bem como ao sigilo postal, da correspondência e das telecomunicações. 2 Todos têm o direito à proteção contra o emprego abusivo de seus dados pessoais (tradução nossa).

[51] O Regulamento Geral de Proteção de Dados faz parte da reforma da proteção de dados da UE, introduzida pela Comissão Europeia em 25 de janeiro de 2012. O GDPR consiste em 99 artigos em onze capítulos: Capítulo 1 (artigos 1.º a 4.º): Disposições gerais (matéria e objetivos, âmbito e âmbito territorial, definições); Capítulo 2 (artigos 5.º a 11.º): Princípios e legalidade (princípios e legalidade do tratamento de dados pessoais, condições de

concebida para harmonizar as leis de privacidade de dados nos países membros (KAZEMI, 2018, p. 25), para proteger e fortalecer a privacidade de dados de todos os cidadãos da UE e para reformular o modo como as organizações em toda a região abordam a privacidade de dados (HAUNTS, 2018, p. 22).

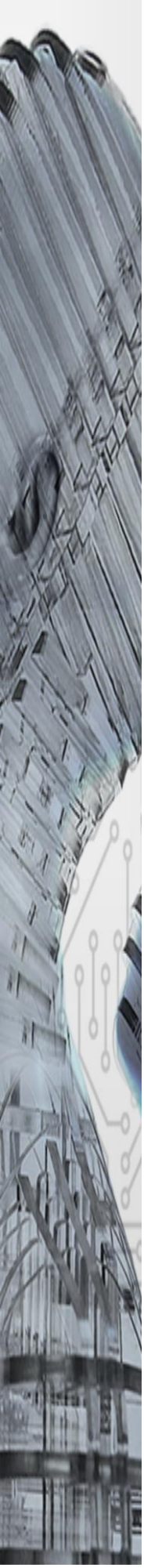
O RGPD foi projetado para modernizar as práticas de proteção de dados, principalmente em relação aos protegidos e armazenados em bancos de dados em linha, quando se tratem de informações básicas e pessoais de identidade[52] (HAUNTS, 2018, p. 34). Por possui o caráter e a condição de regulamento ao invés de uma diretiva, "o RGPD não precisa ser incorporado ao texto de legislação de cada país para ter força legal, pois representa um regulamento da União Europeia, com as regras para o processamento de dados pessoais por empresas privadas e organismos públicos da UE de modo padronizado" (ASAI, 2018, p. 53). O objetivo não é apenas salvaguardar a proteção dos dados pessoais na União Europeia, mas também garantir a livre circulação de dados no mercado único europeu. Todavia, o conceito de "dados pessoais" no § 4[53] permanece amplo (CUE, 2016). Além disso, o tratamento de dados pessoais só é permitido com base numa licença. Estas estão listadas no § 6[54]: Segundo Robert Kazemi (2018, p. 133), "a mudança de cultura nas empresas europeias e

consentimento, tratamento de categorias especiais de dados pessoais); Capítulo 3 (artigos 12 a 23): os direitos da pessoa em causa (transparência e modalidades, obrigação de informação e direito à informação aos dados pessoais, retificação e supressão - o "direito a ser esquecido" - direito de se opor e automatizado tomada de decisões em casos individuais, incluindo *profiling)*; Capítulo 4 (Artigos 24 a 43): Responsável e processador (Obrigações gerais, Segurança de dados pessoais, Avaliação de impacto de privacidade e consulta prévia, Comissário de Privacidade, Código de Conduta e Certificação)
Capítulo 5 (artigos 44.º a 50.º): Transferências de dados pessoais para países terceiros ou organizações internacionais; Capítulo 6 (artigos 51.o a 59.o): autoridades de supervisão independentes; Capítulo 7 (artigos 60.º a 76.º): Cooperação e coerência, Comité Europeu para a Proteção de Dados; Capítulo 8 (artigos 77 a 84): remédios, responsabilidade e sanções; Capítulo 9 (artigos 85 a 91): Para requisitos científicos aplicáveis a situações específicas de processamento (incluindo processamento e liberdade de expressão e liberdade de informação, processamento de dados no local de trabalho, o acesso do público aos documentos oficiais, processamento em fins de arquivamento de interesse público ou para fins de pesquisa histórica e de estatística Propósitos, regulamentos existentes de proteção de dados de igrejas e associações religiosas ou comunidades); Capítulo 10 (artigos 92.º a 93.º): atos delegados e de execução; Capítulo 11 (artigos 94.oa 99.o): Disposições finais (nomeadamente, revogação da Diretiva 95/46 / CE e entrada em vigor do RGPD); Antes dos 99 artigos são apresentados 173 considerados, que são utilizados para interpretar os artigos.

[52] *E. g.* nome, endereço, número de identificação e dados da web, como localização, endereço IP, dados de cookies, dados genéticos e de saúde, dados étnicos ou raciais. opiniões e orientação sexual.

[53] "Dados pessoais" significa qualquer informação relativa a uma pessoa singular identificada ou identificável (a seguir designada "pessoa em causa"); Considera-se que uma pessoa singular é identificável, direta ou indiretamente, nomeadamente através de um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou uma ou mais características especiais que exprimam as características físicas, fisiológicas, a identidade genética, mental, econômica, cultural ou social dessa pessoa natural, de forma a permitir sua identificação". (tradução nossa)

[54] A pessoa afetada deu seu consentimento; o tratamento é necessário para a execução de um contrato ou para a implementação de medidas pré-contratuais; o processamento é necessário para cumprir uma obrigação legal; o processamento é necessário para proteger interesses vitais; o processamento é necessário para o desempenho de uma tarefa de interesse público; O tratamento é necessário para salvaguardar os legítimos interesses do



a adaptação ao novo cenário pressupõe que os dados das pessoas não podem pertencer às empresas ou aos estados, pois o ambiente virtual deve ser seguro e utilizado de maneira privativa"[55].

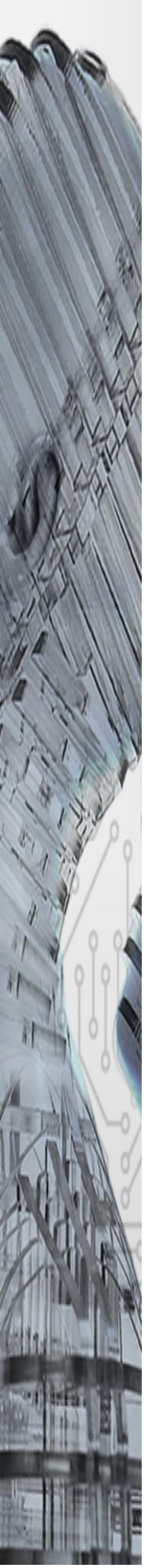
A partir do enquadramento proposto pela RGPD, as autoridades fiscais, policiais e judiciais da União Europeia adquiriram autoridade ampliada para investigar e processar crimes envolvendo privacidade pessoal. "O RGPD aplica-se a todas as empresas que lidam com as informações pessoais dos cidadãos da UE, mesmo que a empresa esteja sediada fora da EU, de forma a alterar as relações entre empresas, consumidores, cidadãos e governos que se relacionem com os países do bloco europeu" (HAUNTS, 2018, p. 28).

O RGPD prioriza a transparência, o acesso à informação e o controle do cliente e do cidadão a respeito do depósito e armazenamento de dados, bem como pretende padronizar as leis de segurança de dados em nível da comunidade de países integrantes da União Europeia, embora os estados individuais ainda mantenham alguma liberdade.

Alguns dos parâmetros fixados pelo RGPD determinam que: (I) os usuários podem, em algumas situações, ver, corrigir ou até deletar (apagar) as informações que empresas guardam sobre eles; (II) empresas devem coletar apenas dados necessários para que seus serviços funcionem; (III) a coleta e o uso de dados pessoais só podem ser feitas com consentimento explícito; (IV) qualquer serviço conectado tem de conceder o chamado "direito ao esquecimento"; (V) as informações de crianças ganham proteção especial; (VI) os clientes que tiverem dados "hackeados" devem ser avisados em até 72 horas; (VII) as empresas devem informar com linguagem compreensível as suas políticas de proteção de dados; (VIII) infratores são punidos com multa pesada, de € 20 milhões ou 4% do volume global de negócios da empresa; (IX) os dados de europeus podem ser transferidos só para países com lei de proteção de dados equivalente à europeia; (X) as empresas que tratem dados de europeus têm de seguir a lei europeia caso estejam em países não considerados "seguros" e, por fim; (XI) grandes processadoras de informação têm de guardar registros sobre todas as vezes em que manipularam dados (CUE, 2016).

responsável pelo tratamento ou de terceiros. Neste último caso, é necessária uma ponderação de interesses em relação aos interesses do titular dos dados. (tradução nossa).

[55] O Regulamento Geral de Proteção de Dados (GPDR, na sigla em inglês) também representa uma reação em busca de proteção, face às denúncias de espionagem promovidas pelo governo dos Estados Unidas da América e denunciadas em 2013, através do WikiLeaks, sob o comando de Edward Snowden e seus colaboradores, acelerando os processos de revisão da legislação, bem como mensurando os seus impactos diretos nas economias, forças políticas e circulação de produtos, baseados na confiança em empresas, além de informações secretas de pesquisas de governo, nas áreas da medicina, tecnologias nucleares e aeroespaciais, dentre outras áreas de grande interesse.



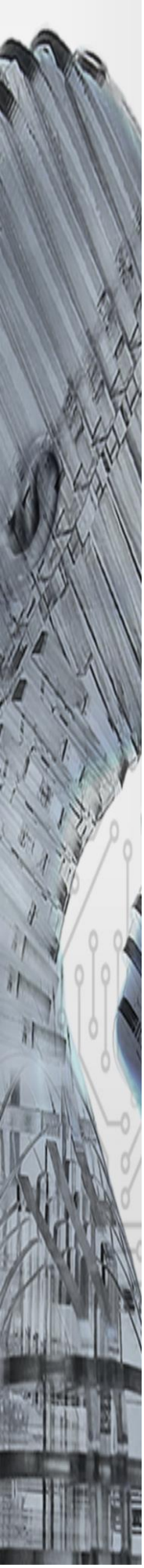
Pretende-se que o RGPD obrigue as organizações a compreender os seus riscos de privacidade de dados e tomem as medidas adequadas para reduzir o risco de divulgação não autorizada de informações privadas dos consumidores (HAUNTS, 2018).

Contrariamente à Diretiva 95/46 (CE, 2005), que teve de ser transposta pelos Estados-Membros da UE para a legislação nacional, o RGPD é diretamente aplicável em todos os Estados-Membros da EU. Contudo, os Estados-Membros suprimem o direito pela legislação. A proteção dos dados pessoais tem conformidade com o referido regulamento e com os direitos à liberdade de expressão e de acesso à informação (CUE, 2016).

O RGPD menciona explicitamente no artigo 5º (CUE, 2016) os seguintes seis princípios para o processamento de dados pessoais: (I) Legalidade e boa-fé no processamento e tratamento de dados; (II) Limitação de finalidade (processamento apenas para fins específicos, claros e legítimos); (III) Minimização e anonimização de dados de forma apropriada e substancial para o propósito e limitada, conforme a necessidade do caso; (IV) Precisão (todas as medidas razoáveis devem ser tomadas para garantir que as informações pessoais corrompidas ou equivocadas sejam prontamente apagadas ou corrigidas); (V) Limite de memória (os dados devem ser armazenados de forma a permitir que os titulares dos dados sejam identificados apenas durante o tempo necessário) e; (VI) Integridade e confidencialidade (segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda acidental, destruição acidental ou danos acidentais).

A segurança de dados também está abrangida por padrões internacionais, tais como a ISO/IEC 27001: 2013 e ISO/IEC 27002: 2013 (ABNT, 2013; ABNT,2013), sob o tópico de segurança da informação, cujo princípio basilar é o de que todas as informações armazenadas, ou seja, dados, devem ser de propriedade e responsabilidade de seu detentor, devendo o seu acesso ser protegido e controlado.

Neste prisma, os Estados-Membros não podem, em princípio, aplicar as regras de proteção de dados previstas no Regulamento (CUE, 2016), ainda que mitigado ou reforçado pelas regulamentações nacionais (ASAI, 2018). Contudo, o regulamento contém várias cláusulas de abertura, que permitem aos Estados-Membros individualmente regulamentarem certos aspectos da proteção de dados, mesmo no caso do unilateralismo nacional (HAUNTS, 2018). Por conseguinte, o Regulamento Geral de Proteção de Dados é também chamado de "híbrido" entre a diretiva e o regulamento.



Há, portanto, necessidade de regulamentação, tanto no que diz respeito às cláusulas de abertura do Regulamento Geral de Proteção de Dados (CUE, 2016), como à necessidade de corrigir a legislação nacional de proteção de dados. Deste modo, o RGPD não altera fundamentalmente o conceito e, em grande medida, os regulamentos detalhados nas legislações nacionais sobre proteção de dados.

Ao contrário, muitas disposições da Diretiva da Comunidade Europeia de Proteção de Dados 95/46 são adotadas, formando base para muitas legislações recentes, como a francesa e a italiana (KAZEMI, 2018, p. 57). Ademais, a RGPD se apresenta como um modelo para a criação das Leis de Proteção de Dados Pessoais em muitos países, tal como no caso da respectiva legislação brasileira.

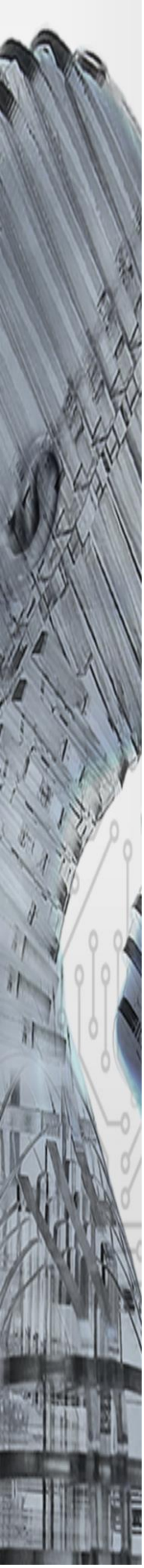
2.4 Panorama das legislações virtuais e eletrônicas brasileiras

A proteção de dados no Brasil, na perspectiva de tutela a direitos constantemente fragilizados pela amplitude de proliferação de informações na rede mundial de computadores, a diminuição da pessoalidade e da intimidade e o mau uso de dados pessoais, remonta um arcabouço jurídico voltado para os Direitos Virtual, Digital e Eletrônico, estes em contínua expansão no panorama normativo do Direito Brasileiro Moderno, correlacionando-se a áreas como as dos Direitos e Processos Civil, Penal e do Administrativo, (TEIXEIRA, 2018, p. 115), além das já citadas anteriormente[56].

Nesse espeque, diversas legislações têm sido inseridas nos ordenamentos jurídicos, a fim de assegurarem direitos e ampliarem a previsão normativa às relações envolvendo dados públicos e privados. Como exemplo, os Direitos Virtual, Digital e Eletrônico produzidos no Brasil têm parte de suas origens no modelo estadunidense conhecido como *Cyberlaw*, compreendendo os títulos e nomenclaturas das seguintes subáreas: (I) Direito Eletrônico; (II) Direito Digital; (III) Direito da Informática; (IV) Direito da Tecnologia; (V) Direito das Telecomunicações e; (VI) Direito da Internet, todos eles observáveis também nas doutrinas brasileiras a respeito do tema (LORENZETTI, 2005; MAGRANI, 2018; PINHEIRO, 2018; TEIXEIRA, 2018).

No Brasil, somente através da promulgação da Lei nº 7.232, em 29 de outubro de 1984, regulamentaram-se os princípios, objetivos e diretrizes da Política Nacional de

[56] *Vide* pág. 15.



Informática[57] (BRASIL, 1984; LORENZETTI, 2005). A consciência do acesso e a "utilização de novas tecnologias nos campos públicos e privados nas últimas décadas ensejaram o surgimento de aparatos legislativos desenvolvidos com o intuito de dar celeridade à transmissão de informações e atos processuais" (TEIXEIRA, 2018, p. 575). No início da década de 1990, já havia a possibilidade de efetuar citações por meio de aparelho *fac-símile* (fax), conforme dispositivo encontrando no art. 58, IV, da Lei nº 8.245/91 (Lei do Inquilinato)[58], caso houvesse previsão contratual (BRASIL, 1991; LORENZETTI, 2005).

Em 1995 a promulgação da Lei nº 9.099/95, que criou os Juizados Especiais, previu que as intimações poderiam ser feitas, da mesma forma que a citação, ou por qualquer outro meio idôneo de comunicação, dentre os quais se inclui o meio eletrônico (BRASIL, 1995). Contudo, somente após o advento da Lei n° 9.800/99, a Lei do Fax (BRASIL, 1990) tida como o exemplo exponencial de reforma legislativa com previsão à utilização de equipamentos eletrônicos no Judiciário, foi possível começar a inserir aparatos tecnológicos no cotidiano jurídico e observar o desenrolar de seus impactos.

Já em 2001, com a instituição dos Juizados Especiais Federais mediante promulgação da Lei nº 10.259/01, no § 2º, do art. 8º[59], pela primeira vez, surgiu uma legislação capaz de propiciar a prática dos atos processuais de forma totalmente eletrônica, sem a necessidade de apresentação posterior de documentação original, através do desenvolvimento de um sistema conhecido por e-Proc (processo eletrônico), com objetivo de reduzir quase totalmente o uso do papel em documentos e atos processuais, remessas físicas entre Tribunais e órgãos públicos[60] e a diminuição da necessidade de deslocamento de advogados à sede da unidade judiciária (BRASIL, 2001).

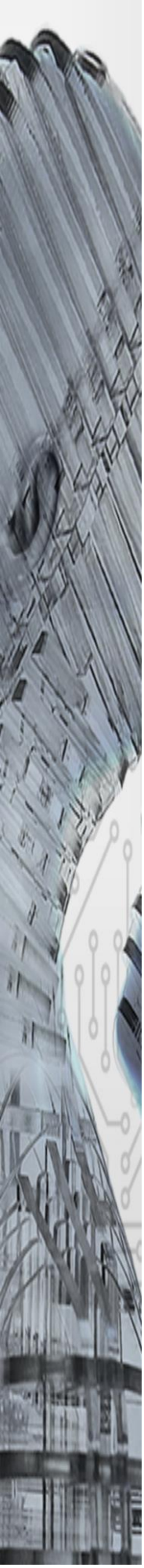
---

[57] A saber, o parágrafo 1º da mencionada Lei oferece a seguinte redação:
Art. 1º Esta Lei estabelece princípios, objetivos e diretrizes da Política Nacional de Informática, seus fins e mecanismos de formulação, cria o Conselho Nacional de Informática e Automação - CONIN, dispõe sobre a Secretaria Especial de Informática - SEI, cria os Distritos de Exportação de Informática, autoriza a criação da Fundação Centro Tecnológico para Informática - CTI, institui o Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação.

[58] "Art. 58. Ressalvados os casos previstos no parágrafo único do art. 1º, nas ações de despejo, consignação em pagamento de aluguel e acessório da locação, revisionais de aluguel e renovatórias de locação, observar - se -á o seguinte:
V - desde que autorizado no contrato, a citação, intimação ou notificação far-se-á mediante correspondência com aviso de recebimento, ou, tratando - se de pessoa jurídica ou firma individual, também mediante telex ou fac-símile, ou, ainda, sendo necessário, pelas demais formas previstas no Código de Processo Civil;"

[59] "Art. 8º As partes serão intimadas da sentença, quando não proferida esta na audiência em que estiver presente seu representante, por ARMP (aviso de recebimento em mão própria).
[...]§ 2º Os tribunais poderão organizar serviço de intimação das partes e de recepção de petições por meio eletrônico."

[60] *Exempli gratia:* Defensorias Públicas, Ministério Público, Procuradorias (Municipais, Estaduais, Federais) e Advocacia da União, dentre outros.



Também no ano de 2001, a Medida Provisória n° 2.200/01 inseriu no ordenamento pátrio a Infraestrutura de Chaves Públicas Brasileiras, vulgo ICP-Brasil, em conformidade com o disposto no art. 1.º[61],no sentido de instituir e regulamentar o sistema de "assinaturas digitais" no país, bem como garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica por meio do uso de certificados digitais (BRASIL, 2001).

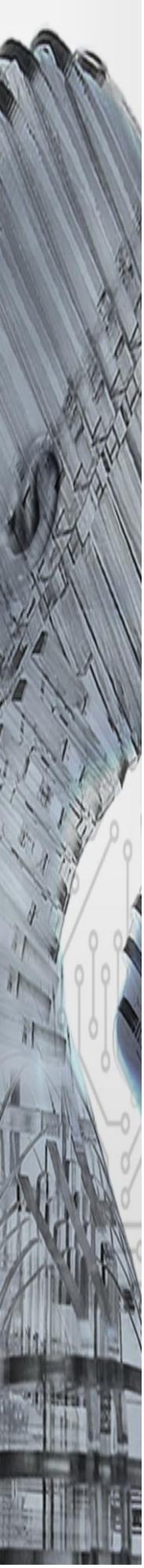
Ainda em 2001, a Lei n° 10.358/01, trouxe alterações ao então vigente Código de Processo Civil de 1973, com vistas a permitir a prática de quaisquer atos processuais por meio eletrônico, em todas as instâncias (BRASIL, 2001). Contudo, o referido dispositivo jurídico recebeu veto, tendo em vista as considerações feitas sob o aspecto de que determinadas mudanças apresentadas poderiam trazer, de certa forma, insegurança jurídica ao processo, pois, ainda vigorando a MP n° 2.200 (ICP-Brasil), com suas proposições para manutenção de uma estrutura padronizada e integralizada de certificação digital, ensejaria a cada tribunal o condão para desenvolver seu próprio sistema de certificação eletrônica, diferente do padrão adotado na MP n° 2.200. Desta forma, fixou-se que apenas os documentos assinados digitalmente no âmbito da ICP-Brasil têm validade legal jurídica.

Por meio da Lei n° 11.280/06, fora inclusa no art. 154, do CPC de 1974, a permissão para a prática de atos processuais eletrônicos nas várias instâncias, ressalvando explicitamente a observação às regras da ICP-Brasil (BRASIL, 2006). No mesmo caminho, a Lei n° 11.341, de agosto de 2006 também trouxe modificações ao CPC; desta vez para conceder validade aos recursos fundados em divergência jurisprudencial que tivessem por prova a reprodução de julgados disponíveis na Internet, desde que sua respectiva fonte seja claramente citada. Tais adequações já vieram inseridas no CPC de 2015.

Ainda em 2006, a instituição da Lei nº 11.382/06, "passou a prever em vários dispositivos o uso de meios eletrônicos na execução judicial" (TEIXEIRA, 2018, p. 624) e modificou o processo de execução cível, incorporando os institutos da penhora *online* (art. 655-A) e do leilão *online* (art. 689 - A), visando à satisfação do crédito executivo e evitando possíveis esquivas por parte dos executados.

O mais conhecido e utilizado sistema de penhora *online* na atualidade é o BACEN-JUD. Trata-se de uma ferramenta de comunicação eletrônica entre o Poder Judiciário e instituições financeiras bancárias, por intermédio do Banco Central, através do qual, juízes

[61] "Art. 1º. Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".



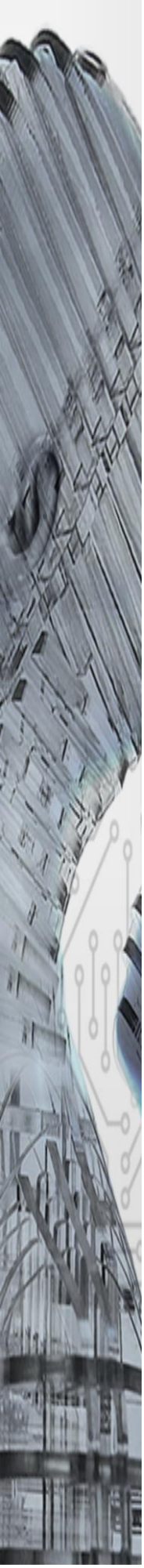
federais e estaduais, podem utilizar o referido *software*, para requerer informações sobre a existência de ativos financeiros, bloquear, desbloquear e transferir ativos financeiros existentes em contas bancárias em nome dos executados, por meio de decisões judiciais que serão transmitidas às instituições bancárias para cumprimento e resposta.

Após, o Sistema de Restrição Judicial de Veículos, amplamente conhecido como RENAJUD, apresenta-se como um sistema online que possibilita a comunicação eletrônica entre o Poder Judiciário e o Departamento Nacional de Trânsito - DENATRAN. Por meio dele o magistrado pode, além de consultar os veículos registrados em nome dos executados, enviar instantaneamente ordens judiciais eletrônicas de restrição de veículos automotores na base de dados do Registro Nacional de Veículos Automotores - RENAVAM.

Em 19 de dezembro de 2006, foi sancionada a Lei nº 11.419, a qual dispõe sobre a implantação e informatização do processo judicial, tornando-se o marco regulatório brasileiro no uso de meios eletrônicos na tramitação de processos, na comunicação de atos e transmissão de peças em todos os graus de jurisdição (BRASIL, 2006).

Em 21 de junho de 2011, o Processo Judicial Eletrônico – PJE, foi oficialmente lançado pelo então presidente do CNJ, Cezar Peluso, com a publicação da Resolução nº 185, de 18/12/2013, modernizando as práticas do processamento judicial no Brasil. Logo nos dias seguintes, presidentes de tribunais de todo o país receberam informações e detalhes do sistema, bem como um manual para auxiliar os técnicos na instalação dos *softwares*. O portal eletrônico do CNJ realizou transmissão ao vivo e contou com 1.315 acessos, sendo 135 simultâneos. Além disso, 32 tribunais retransmitiram a apresentação via *streaming* aos seus servidores. “Este tema da informatização do processo judicial (ou processo eletrônico) tem como consequência a modernização do Poder Judiciário” (TEIXEIRA, 2018, p. 567), contudo, sem diligenciar a recuperação e digitalização de informações dos processos provenientes de autos físicos, de modo a não integralizar o conteúdo em maior escala possível de completude e mantendo, ainda, a dificuldade de acesso a informações regionais provenientes das instâncias inferiores do Judiciário.

Na senda do Direito Penal, a proteção aos dados pessoais e à privacidade também se manifestou “pela inclusão de um parágrafo único ao art. 298 do Código Penal, decorrente da Lei nº 12.737/2012 (apelidada de Lei Carolina Dieckmann, em razão da repercussão do vazamento de fotos íntimas da atriz)” (TEIXEIRA, 2018, p. 518), a qual introduziu três novos tipos penais específicos envolvendo crimes informáticos, sendo eles (I) a invasão de dispositivo informático alheio (artigo 154-A do Código Penal); (II) a interrupção ou



perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (artigo 266, §§ 1º e 2º do Código Penal); e (III) a falsificação de cartão de crédito ou débito (artigo 298 do Código Penal). Desta forma, é possível observar que o ambiente virtual também padece com o mau comportamento de alguns indivíduos e está vulnerável a ações fraudulentas e criminosas.

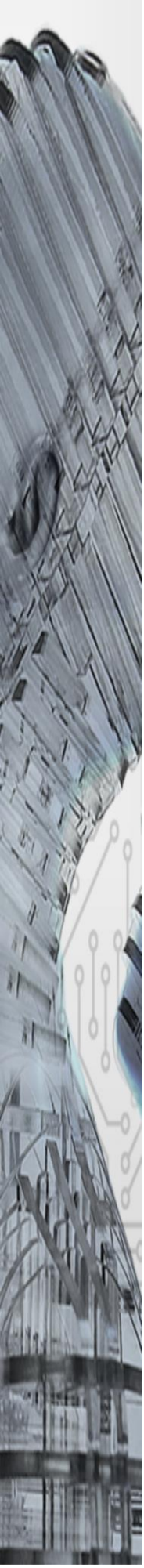
Outra atualização de norma já existente que buscou se aproximar das relações econômicas e consumeristas no ambiente virtual, ocorreu com a promulgação do Decreto nº 7.962/2013, que trouxe novas regulamentações ao Código de Defesa do Consumidor (BRASIL, 1990), em relação a contratos e compras realizados em comércio eletrônico. Assim sendo, o Decreto nº 7.962/2012 oferece um rol de informações e esclarecimentos ao consumidor no tocante às compras virtuais, atendimentos, políticas de troca, direito de arrependimento, garantias de produtos, compras coletivas, compras internacionais e formas de reclamação, advindos do comércio eletrônico (TEIXEIRA, 2018, p. 310 - 314).

O Sistema de Informações ao Judiciário (INFOJUD) se apresenta como uma ferramenta *online* que permite a comunicação eletrônica entre o Judiciário e a Receita Federal, por meio do qual é possível ao magistrado ter acesso às declarações prestadas pelos executados à Receita Federal. Marco Aurélio Greco, no mesmo sentido, argumenta:

> Em vários países, a informática vem sendo utilizada mais intensamente na melhoria da qualidade e da celeridade dos serviços judiciários, bem como na montagem de uma infraestrutura normativa e administrativa amplamente indispensável ao desenvolvimento seguro das relações jurídicas. (GRECO *et al*., 2001, p. 86).

As autoridades brasileiras perceberam que a modernização do Judiciário não pode se pautar unicamente na mudança das leis. Segundo Cândido Dinamarco (2017, p. 40) deve-se, também, perquirir "a alteração da postura dos operadores e administradores do judiciário, na mudança estrutural com o uso de novas técnicas e tecnologias de resolução de conflito".

A reformulação das rotinas processuais e internas, com vistas à desmaterialização dos atos processuais e à racionalização dos procedimentos, bem como à otimização da prestação jurisdicional e dos serviços judiciários, confere concretude aos princípios da celeridade processual, da economicidade e da instrumentalidade e ao direito fundamental à efetividade, a partir do abandono de formalidades arcaicas na tramitação do processo, configurando a adoção dos mecanismos eletrônicos na esteira da modernização e amplificação da acessibilidade ao judiciário, numa consciência mais próxima do cidadão e do operador do direito.



2.4.1 Lei de Acesso à Informação

O princípio da "Publicidade" no acesso à informação pública surge como um dos princípios basilares da democracia representativa, instituído, desde o início deste regime político-administrativo, em declarações, cartas magnas e leis (BANDEIRA DE MELLO, 2015, p. 8 - 25). A "Transparência", entretanto, "é um conceito mais recente, tendo ganhado destaque durante o século XX, em suas décadas finais" (CANOTILHO, 2002, p. 258). Tais princípios possuem interpretações complexas, mas assemelham-se por prestigiar a convergência dos interesses público e privado na existência de um mercado financeiro dotado de um mínimo de confiabilidade no tocante à solvência potencial dos tomadores de empréstimos, o governo sendo o mais expressivo deles.

Desta forma; as crises fiscais, econômicas e orçamentárias com as quais se deparam os governos, desde o início da crise petrolífera dos anos 1970, "cujos danos acarretaram a convivência com o *déficit* público estrutural, dirigido ao sabor de políticas econômicas anticíclicas de natureza keynesiana (uso das finanças públicas para combater o desemprego e a inflação)" (BELL, 1973, p. 84), produziram "desestabilidade contínua e a descrença da população na capacidade administrativa do setor Público e de seus governantes" (BAUMAN, 2001, p. 38), face ao capital econômico e a manipulação do setor privado.

Logo, visando coibir práticas abusivas, crimes diversos, inclusive os de natureza econômica, garantir maior lisura e, principalmente, oportunizar o controle societal e a democratização de todos os atos da Administração Pública, foi promulgada a Lei nº 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação, que, dentre outras medidas, tem como objetivos simplificar e facilitar a publicação de informações de todas as espécies (BRASIL, 2011), produzidas pela Administra Pública.

Neste sentido, a Lei nº 12.527/2011, regulamentou o artigo 5º, inciso XXXIII da Constituição Federal (BRASIL, 1988), na busca por expandir a consolidação do seu regime democrático e ampliar a participação cidadã, através do fortalecimento dos instrumentos de controle da gestão pública, estabelecendo que o acesso à informação é a regra e o sigilo, a exceção. "A lei brasileira de acesso à informação do governo, deixa claro que o acesso à informação se refere às atividades administrativas, de ambos os setores - o Legislativo e o Judiciário" (BLANKE; PERLINGEIRO, 2018, p. 14).

Nesta esteira, o recém-completado aniversário de seis anos da Lei de Acesso à Informação e as plataformas de pesquisa do CNJ, tais como o BNMP - Banco Nacional de

Mandados de Prisão, o Banco Nacional de Demandas Repetitivas e Precedentes Obrigatórios, como também a publicação do Anuário "Justiça em Números" (CNJ, 2018), demonstram formas de cruzamento de dados em órgãos públicos.

2.4.2 Marco Civil da Internet

O Marco Civil da Internet, introduzido pela Lei nº 12.965, de 23 de abril de 2014, trata sobre o regime jurídico do uso da Internet no Brasil. Contém os princípios, regras e obrigações de uma "constituição da Internet", garantindo certos direitos fundamentais aos seus usuários, tais como: (I) os direitos de privacidade; (II) a neutralidade da rede; (III) o estabelecimento de portos seguros para provedores de serviços de Internet e provedores de serviços em linha; (IV) abertura de dados públicos e do governo e (V) o estabelecimento do acesso à Internet como um requisito para o exercício de direitos cívicos. Nas palavras de George Souza e Alexandre Lemos, é possível compreender o Marco Civil da Internet nos termos *in verbis:*

> Muito se fala em "*Internet freedom*", que poderia ser traduzido como "Internet livre". Um primeiro entendimento sobre o que significa uma Internet livre pode estar ligado à ideia de que essa seria uma Internet sem leis. A liberdade aqui consistiria justamente na inexistência de leis (ou normas jurídicas) que determinassem qualquer rumo ao desenvolvimento tecnológico. Ao contrário do que a ideia acima propugna, o Marco Civil da Internet apresenta um novo cenário no qual o conceito de "Internet livre" está ligado não à ausência de leis, mas sim à existência de leis que possam garantir e preservar as liberdades que são usufruídas por todos justamente por causa da tecnologia e mais especificamente pelo desenvolvimento da Internet. (SOUZA; LEMOS, 2016 p. 16)

O Marco Civil da Internet (BRASIL, 2014), enquanto política pública de transparência representa o início da tutela normativa a respeito da proteção de dados pessoais, muito embora não o tenha feito de forma específica. "Trata-se de uma lei principiológica, pois estabelece parâmetros gerais acerca de princípios, garantias, direitos e deveres para o uso da Internet no Brasil, além de determinar algumas diretrizes a serem seguidas pelo Poder Público sobre o assunto" (TEIXEIRA, 2018, p. 105), como demonstra a previsibilidade insculpida no inciso III, do art. 3º da Lei nº 12.965/14[62], quanto à regulação de dados pessoais mediante legislação específica. Nas palavras de Tarcísio Teixeira:

> De qualquer forma, sempre deverão ser obrigatoriamente respeitadas as normas brasileiras e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das

[62] Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios:
III - proteção dos dados pessoais, na forma da lei;

> comunicações privadas e dos registros quanto às operações que envolvam coleta, armazenamento guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional (MCI, art. 11, *caput*). Aqui vale o mesmo comentário sobre a sede não ser no Brasil. (TEIXEIRA, 2018, p. 115)

O art. 7º, nos incisos VI, VII, VIII, IX e X[63], da Lei nº 12.965/2014 também versa sobre coleta, uso, armazenamento, tratamento, exclusão e proteção de dados pessoais, todavia sem determinar exatamente como os procedimentos devem ser executados. "Em todo caso, ressalta-se uma vez mais que esse modelo invasivo, e amplamente poderoso, encontra-se em vigor hoje no Brasil e à disposição das autoridades de investigação e de instrução processual penal ou mesmo civil." (SOUZA; LEMOS, 2016, p. 144).

Ainda assim, estes enunciados foram capazes de especificar alguns conceitos normativos muito genéricos no ordenamento jurídico brasileiro, acerca do tratamento e dos procedimentos judiciais envolvendo dados (LEITE; LEMOS, 2014), tais como orientados, *e.g.* pela dicção do art. 21 do Código Civil[64] (BRASIL, 2002), ou de forma muito ampla, conforme trazido pelo art. 43 do Código de Defesa do Consumidor[65] (BRASIL, 1990).

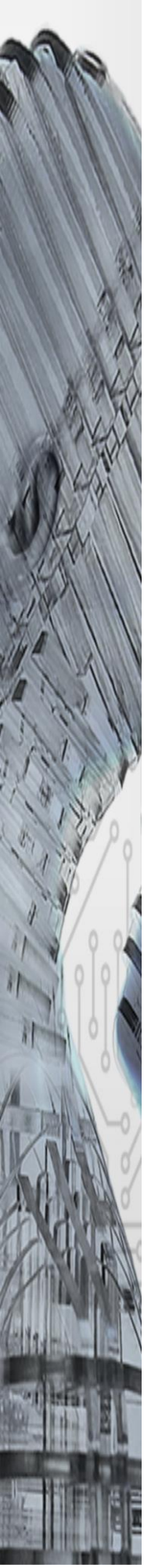
O escopo e a amplitude do Marco Civil da Internet foram aumentados pelo advento do Decreto nº 8.771, de 11 de maio de 2016, que regulamentou o Marco Civil da Internet e pelo Decreto nº 8.777, também de 11 de maio de 2016, que instituiu a Política de Dados Abertos do Governo Federal. Sob as égides de ambas as normas, segundo Teixeira:

> No que diz respeito à proteção da privacidade (direito inerente à inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, nos termos da

[63] Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

[64] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. Vida privada e intimidade.

[65] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.



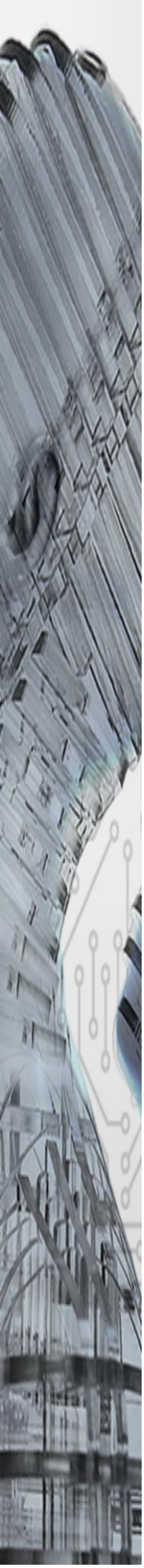
> Constituição Federal, art. 5º, inc. X, como estudado em outro ponto), a lei garante o sigilo de dados pessoais do usuário, do que ele acessa na rede e do conteúdo de suas comunicações. Assim, não é permitido monitorar ou fiscalizar os pacotes de dados (conteúdos) transmitidos pelos usuários na internet, sendo que o acesso a esses dados necessita de ordem judicial. (TEIXEIRA, 2018, p. 107 - 108)

Igualmente, os Direitos Virtual, Digital e Eletrônico no Brasil ganharam maior destaque, proximidade com a população e segurança jurídica também no panorama internacional, em comparação com outros países que já estavam desenvolvendo legislações capazes de conferir maior segurança e privacidade a dados pessoais e públicos, conforme os critérios de escalonamento utilizados pela ONU e pela UIT (2018), para confecção do relatório anual *Global Cybersecurity Index (GCI).*

No dia 20 de setembro de 2017, o Ministério do Desenvolvimento, Planejamento e Gestão concluiu a consulta pública sobre a Estratégia Brasileira para a Transformação Digital (EBTD), cujo escopo foi a elaboração de uma Lei de Proteção de Dados, a qual também fez previsão à instituição de uma autoridade reguladora. Como passo seguinte, foi publicada a Portaria nº 107, de 02 de Maio de 2018, do mesmo Ministério, que aprovou a versão revisada da EBTD para o período 2016-2019, como também atribuiu à Secretaria de Tecnologia da Informação e Comunicação a competência para coordenar a formulação, o monitoramento, a avaliação e a revisão da Estratégia de Governança Digital da Administração Pública – EGD, instituída pela Portaria nº 68, de 07 de Março de 2016. Segundo preceitua a EBTD, é importante amparar os setores da economia, atualmente retardados pela insegurança jurídica gerada pela ausência de legislação específica no Brasil. Assim, um dos grandes desafios se refere à privacidade e proteção de dados, cujos impactos podem se estender a campos como: Saúde, Mercado Financeiro, Educação e Governo, entre outros.

A EBTD também traçou diretrizes e determinações, para nortear a transformação digital de diferentes setores, incluindo novas atribuições a órgãos afetos, planos a ações estruturantes, no âmbito de diferentes Ministérios, mediante acriação e a atualização de marcos regulatórios adequados. No segmento de infraestrutura, por exemplo, o plano de ação inclui formas de uso do Satélite Geoestacionário de Defesa e Comunicações (SGDC), construído em parceria com o Ministério da Defesa, que permitirá o fornecimento de Internet de banda larga em todo o território nacional[66] e a revisão do marco regulatório das Telecomunicações.

[66] O consequente tráfego de informações e dados, por via deste satélite pode levantar questionamentos sobre ser possível o controle do Estado em relação à transmissão dos mesmos e quais são os impactos e consequências deste monitoramento para a privacidade e a proteção de dados pessoais, apesar de também viabilizar a distribuição de internet e a expansão de campo de muitos provedores do serviço.



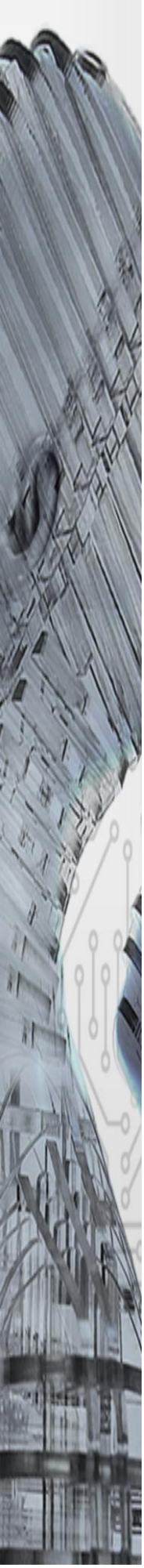
Outro mecanismo regulatório em vigor é o Decreto nº 9.319, de 21 de março de 2018, que instituiu o Sistema Nacional para a Transformação Digital e estabeleceu a estrutura de governança e a implantação da Estratégia Brasileira para a Transformação Digital. O referido Decreto é voltado para a proteção de dados públicos, bancários e oficiais, de registro de informações, tendo por objetivo o maior controle e poder de fiscalização e modernização dos sistemas e aparatos eletrônicos e virtuais dos órgãos ligados à Administração Pública, criando espaço para a normatização da proteção a dados pessoais.

2.5 A Lei Geral De Proteção De Dados Pessoais: princípios e objetivos almejados

No dia 14 de agosto de 2018 foi sancionada a Lei nº 13.709, cujo *nomem iuris* é Lei Geral de Proteção de Dados Pessoais do Brasil – LGPD, após um processo legislativo iniciado em 2011. A Medida Provisória n° 869, de 27 de dezembro de 2018, convertida na Lei nº 13.853/2019, inseriu acréscimos a pontos da LGPD que permaneciam indefinidos ou haviam sido vetados pelo então Presidente da República à época (2018), e permaneciam controversos - sendo capazes de impactar negativamente a efetividade normativo-jurídica pretendida pelo Legislador. Na Lei nº 13.853/2019 também foi postergada a previsão inicial de entrada em vigor da referida lei, sendo estipulada para o mês de agosto de 2020[67].

Após a aprovação da LGPD, o Brasil passou a figurar como Estado possuidor de um nível considerado "adequado" em relação à proteção de dados pessoais, conforme também apontou o anuário *Global Cybersecurity Index* (UIT, 2018), aumentando significativamente seu regime de proteção, como também comprovando sua equiparação aos padrões de segurança já impostos pela UE, com o RGPD e as demais leis internacionais sobre a

[67] O prazo para a entrada em vigor da LGPD (*vacatio legis*) obriga os setores econômicos, administrativos, sociais e a todos os indivíduos que realizam atividades envolvendo tratamento de dados pessoais, a se adequarem à referida Lei. Na prática, tais setores precisam alinhar equipamentos e programas de segurança junto à atuação de um encarregado de dados, dentre outras exigências, para estarem em conformidade com a LGPD. Porém, os custos para a aplicação de tais ajustes podem ser interpretados de maneira qualitativamente diferente, ainda que o prazo legal para os fazer seja quantitativamente igual para todos os tratadores e controladores de dados, sem considerar a possibilidade de realização das despesas necessárias, conforme a capacidade financeira de cada situação concreta. Logo, o surgimento de movimentos políticos, econômicos e sociais pedindo por mais prazo para promoção das adequações pavimentou o Projeto de Lei nº 5.762/2019 (BRASIL, 2019), cujo escopo trata da prorrogação do início da vigência da LGPD - de agosto de 2020 para agosto de 2022. Os impactos suportados pela economia, acarretados pela pandemia da COVID-19 (ou coronavírus), também incentivaram a pretensão de prorrogação da vigência efetiva da LGPD, mediante previsão do art. 25, do Projeto de Lei nº 1.179/2020, ou Regime Jurídico Especial e Transitório das Relações Jurídicas do Direito Privado (BRASIL, 2020), alterando o art. 65, II, da LGPD, de 24 para 36 meses após a data de sua publicação, ou seja, de agosto de 2020 para agosto de 2021. Até a data de depósito da presente pesquisa junto à Secretaria do Programa de Pós-Graduação em Justiça Administrativa, da Universidade Federal Fluminense, o Projeto de Lei nº 5.762/2019 não havia sido aprovado e o Projeto de Lei nº 1.179/2020 encontrava-se aprovado somente pelo Senado Federal.



segurança e a proteção de dados pessoais (PINHEIRO, 2018, p. 22 - 31). A LGPD complementa a moldura jurídica já introduzida anteriormente pela Lei de Acesso à Informação e o Marco Civil da Internet, dentre outras normas e regulamentos brasileiros, como já mencionado.

A LGPD criou também diversas estruturas e previsões legais para a "coleta, tratamento e utilização de dados pessoais no Brasil nos setores públicos e privados, quer no ambiente *online*, quer nas situações *off-line"* (BIONI, 2018, p. 51), de modo a balizar, padronizar e harmonizar toda e qualquer relação envolvendo informações pessoais, simples ou classificadas com "sensíveis", bem como conferir maior segurança jurídica aos indivíduos de um modo geral, às Administrações e empresas nacionais ou transnacionais que realizem atividades no Brasil, ou com dados de brasileiros e aumentando a competitividade e a clareza das relações de consumo, nos mercados interno e externos. No mesmo sentido, a LGPD se apresenta como um requisito importante para a participação do Brasil em novas parcerias na área comercial, atualmente realizadas de forma indissociável à captação e tratamento de dados (BLUM, 2018, p. 34 - 35).

O desenvolvimento econômico e tecnológico, além da ampliação dos direitos individuais, pretendidos pela LGPD, também visam à promoção de um critério didático voltado para a conscientização, responsabilização e conhecimento sobre a autodeterminação em dados permitida quando do aceite e da informação a respeito da destinação de dados pessoais por parte de seus titulares, os quais devem desenvolver maior atenção quanto à cessão e ao consentimento sobre o uso de seus dados pessoais por empresas e pela Administração Pública, visando promover o conhecimento da lei mediante relações adequadas, baseadas em regras claras, objetivas e de fácil compreensão.

2.5.1 A LGPD como medida política e a participação do Brasil na OCDE

As leis de proteção econômica, de regulação de setores bancários e de crédito, bem como as normas sobre dados e transferências de tecnologia coexistem com as normas internas de muitas empresas brasileiras que negociam ou pretendem negociar com mercados e economias em países do exterior (LORENZETTI, 2018, p. 309 - 310), de forma que *compliance* com regras internacionais já se encontra pacificado como prática empresarial e "em âmbito internacional, organizações têm se dedicado à questão por meio de conferências,

convenções e tratados sobre problemas jurídicos advindos do comércio eletrônico internacional."(TEIXEIRA, 2018, p. 311).

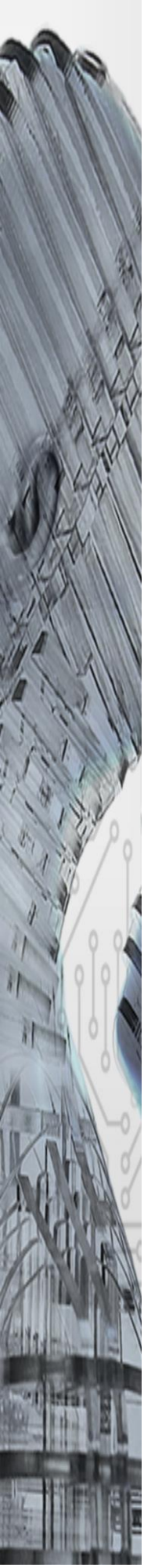
Já para o setor público brasileiro, a aprovação da LGPD, representa o início da compreensão das possíveis consequências (desastrosas) da não regulamentação do direito à privacidade e à proteção de dados pessoais, tendo em consideração "a possibilidade de agentes públicos sofrerem imputações ligadas à improbidade administrativa e demais consequências do tratamento de informações no dia-a-dia, que compreende grande parte das atividades executadas no âmbito do serviço público" (TEIXEIRA, 2018, p. 318 - 322), com a possibilidade de multas rigorosas e demais sanções previstas na LGPD (BIONI, 2018, p. 60).

Ademais, a falta de atenção para com os assuntos normativos de cunho transnacional, pode denotar a incapacidade dos gestores brasileiros em conhecer as necessidades das economias internacionais e a dificuldade de se adequarem às mais recentes demandas legislativas em setores desprotegidos, fazendo com que o Brasil seja visto em situação de atraso jurídico, perdendo oportunidades e parceiros comerciais importantes para a alavancagem da economia, interna e externamente (PINHEIRO, 2018, p. 32 - 34).

O pedido de ingresso realizado pelo Brasil, em 2017, na Organização para a Cooperação e Desenvolvimento Econômico – OCDE[68], em muito acelerou o processo de confecção e aprovação da LGPD, que é um dos requisitos político-diplomáticos, observados no processo de aceitação de um novo membro na Organização, a qual também analisa as requisições formuladas pela Argentina, Peru, Croácia, Bulgária e Romênia.

Além do controle inflacionário e fiscal, requisitos técnicos, negociações político-diplomáticas e os custos adicionais à economia (em um momento de fragilidade nacional), o entrave legislativo também desponta como um fator de grande dificuldade. São necessários cerca de 245 construtos legais, contendo normas, regras e princípios que tutelem no ordenamento jurídico nacional os valores defendidos pela OCDE. Neste sentido, a segurança, a privacidade e a proteção de dados pessoais são alguns deles, de modo que no panorama internacional moderno adquiriram grande relevância, pois abrangem setores economicamente amplos e as suas legislações são consideradas de difícil aprovação. Logo, o Brasil já cumpriu uma das etapas mais difíceis.

[68] A Organização para a Cooperação e Desenvolvimento Econômico - OCDE, é um organismo internacional atualmente formado por 36 países considerados desenvolvidos (de elevado PIB e IDH), os quais aceitam os princípios de democracia representativa, de economia de mercado e juntos detêm mais da metade do valor absoluto da economia global. A OCDE é apelidada de "clube dos ricos".



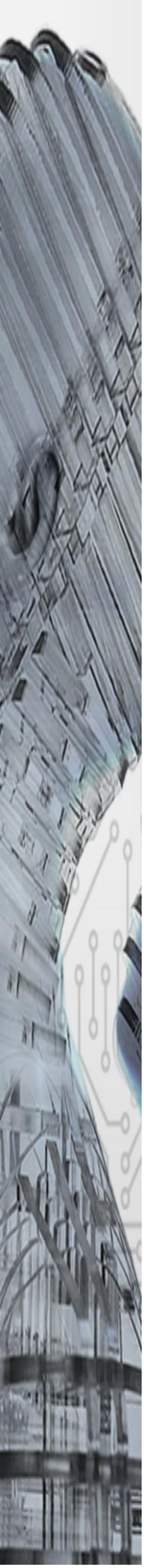
2.5.2 Princípios e finalidades da proteção de dados segundo a LGPD

A entrada em vigor da LGPD representa, também, a inserção no ordenamento jurídico brasileiro de uma série de princípios e finalidades envolvendo a segurança e a proteção de dados pessoais, como derivativos do direito fundamental à privacidade, de forma a possuírem matriz constitucional e infraconstitucional. “A LGPD exige que as atividades de processamento sejam feitas de boa-fé e para fins legítimos, específicos e explícitos” (PINHEIRO, 2018, p. 42).

O princípio da adequação da LGPD procura assegurar a compatibilidade do processamento com os objetivos comunicados ao indivíduo no contexto de seu processamento de dados pessoais (PINHEIRO, 2018, p. 44 - 46). Ao mesmo tempo, os indivíduos devem ser informados de tais propósitos. É proibido processar os dados pessoais para uma finalidade subsequente que seja diferente e incompatível com os propósitos originais, sem possibilidade de processamento subsequente que seja incompatível com esses propósitos (BIONI, 2018).

O Princípio da Finalidade tem grande destaque, por nortear a coleta, o tratamento e o processamento de dados pessoais, os quais devem ser realizados apenas para fins justos, específicos, legítimos e propósitos explicitamente informados ao titular, sem a possibilidade de tratamento de forma incompatível com estes fins, tendo profunda correlação para com o Princípio da Adequação, o qual determina que o tratamento de dados deve se limitar apenas aos propósitos informados ao titular dos dados. Pelo princípio da Finalidade também é possível depreender o chamado “direito ao esquecimento”, tendo em vista que o titular de dados, conforme redação do art. 18, IV, da LGPD, tem o direito de solicitar a exclusão de seus dados de cadastros ou bancos de dados de pessoas jurídicas de direito público ou privado, tão logo estes tenham atingido os fins colimados no momento da coleta, decaindo a necessidade de prorrogação na armazenagem (BRASIL, 2018).

A abrangência da proteção de dados pessoais inserida na Lei nº 13.709/2018, elenca os fundamentos jurídicos para a sua utilização, bem como apresentam um total de dez bases jurídicas dos setores de maior interesse protetivo, sendo elas: (I) consentimento; (II) cumprimento de uma obrigação legal ou regulamentar; (III) quando necessário para a execução de um contrato ou procedimentos preliminares relacionados com o contrato do qual o titular dos dados é parte, a pedido do mesmo (titular dos dados); (IV) quando necessário, para satisfazer o interesse legítimo do responsável pelo tratamento de dados ou de terceiros; (V) no exercício regular de direitos em processos judiciais, administrativos ou arbitrais; (VI)

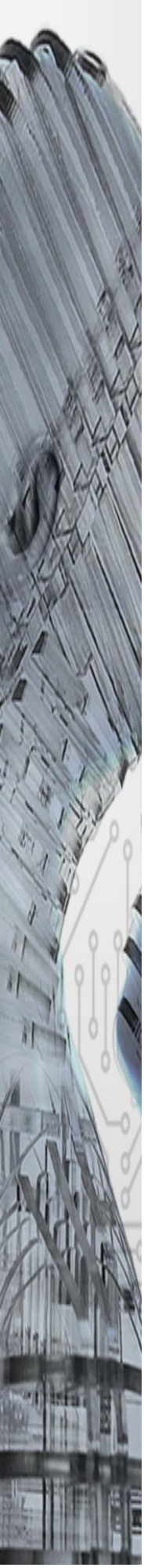


proteção da vida ou segurança física da pessoa em causa ou de terceiros; (VII) proteção à saúde, em coletas de dados sobre procedimentos e tratamentos realizados por profissionais de saúde ou por entidades de saúde; (VIII) proteção a órgãos de pesquisa, para realizar estudos, garantindo, sempre que possível, a anonimização dos dados pessoais; (IX) proteção de dados pela Administração Pública, para a execução de políticas públicas; e (X) a proteção do crédito (BRASIL, 2018).

Para cumprir o princípio da não discriminação, as organizações nunca devem processar dados pessoais para fins ilegais, abusivos ou discriminatórios (BIONI, 2018, p. 148 - 150). A LGPD inclui requisitos rigorosos para o processamento de dados pessoais de crianças e adolescentes (BRASIL, 2018). Tais requisitos incluem a necessidade de consentimento específico, independente e destacado de pelo menos um dos pais ou representante legal. Além disso, as informações sobre o processamento de dados que estão sendo fornecidas em tais casos, devem ser simples, claras e acessíveis para informar aos pais ou representante legal e para serem apropriadas para o entendimento das crianças e adolescentes.

Além disso, a LGPD distingue especificamente uma categoria de dados pessoais sensíveis para os quais o processamento só é permitido: (I) com o consentimento específico do indivíduo ou; (II) sem o seu consentimento quando é indispensável para uma das dez bases jurídicas delineadas (BRASIL, 2018). Dados pessoais confidenciais sob o regime jurídico proposto pela LGPD, incluem dados pessoais relativos à origem racial ou étnica, crença religiosa, opinião política, associação sindical ou religiosa, filosófica ou política, dados relativos à saúde ou vida sexual, dados genéticos ou biométricos, quando relacionados a uma pessoa singular.

A LGPD permite a transferência de informações pessoais para fora do Brasil "somente se as condições forem atendidas por uma das bases legais para a transferência de dados transfronteiriça" (PINHEIRO, 2018, p. 132). Estas condições podem ser satisfeitas, por exemplo, com base na decisão de adequação que estabelece um nível "adequado" de proteção aos dados pessoais em um país específico. Além disso, a transferência pode basear-se em várias formas de garantias de conformidade do controlador (cláusulas contratuais padrão, etc.). Existem também várias bases legais para a transferência, abordando a necessidade de explicitar os motivos legais e de interesse público (PINHEIRO, 2018, p. 132 -133), também podendo ser realizada com base no consentimento específico e distinto do indivíduo.



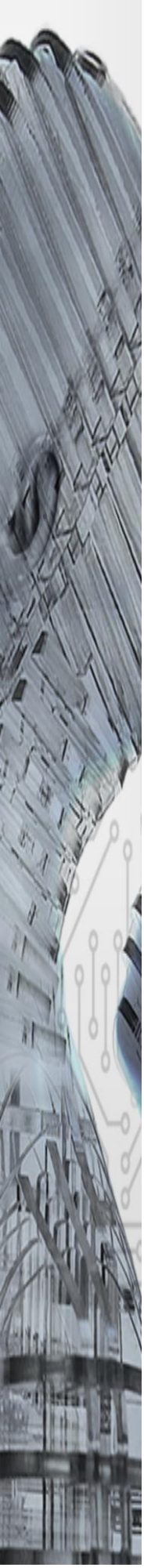
O princípio de prevenção da LGPD exige que as organizações adotem medidas para prevenir incidentes e danos devido ao processamento de dados pessoais (PINHEIRO, 2018, p. 137). Sob a LGPD, as organizações devem implementar medidas técnicas e administrativas de segurança que lhes permitam proteger os dados pessoais de acesso não autorizado e destruição, perda, alteração ou exclusão acidental ou ilegal (BRASIL, 2018). Além disso, as medidas de segurança devem ser seguidas por todas as organizações envolvidas no processamento de dados ao longo do ciclo de vida dos dados.

O princípio da anonimização ou minimização de dados sob a LGPD exige que as organizações limitem a quantidade e o escopo dos dados pessoais que processam, ao mínimo necessário para alcançar seus objetivos (BRASIL, 2018). Somente dados relevantes, proporcionais e não excessivos em relação aos propósitos do processamento devem ser usados. Além disso, as organizações geralmente devem excluir os dados pessoais após o término de seu processamento, a fim de limitar seu armazenamento.

2.5.3 Reestruturações setoriais acarretadas pela LGPD

As reestruturações de cunho transversal e multisetorial em setores socioeconômicos e geopolíticos, acarretados pela LGPD, referem-se a qualquer empresa privada ou organismo público, bem como aos seus agentes e representantes (BRASIL, 2018), “de modo que durante o seu prazo de *vacatio legis,* os setores público e privado, caso queiram continuar operando em conformidade, devem se adequar à nova conformação” (PINHEIRO, 2018, p. 77), até a entrada definitiva em vigor da LGPD e continuarem atentos às diretrizes firmadas pela ANPD.

Portanto, o primeiro impacto trazido pelos artigos 50 e 51, da LGPD (BRASIL, 2018), se refere às modificações nos processos internos e investimentos em setores operacionais, com a adequação de funcionários e agentes, em relação à consciência sobre tratamento de dados pessoais e suas regulações setoriais. Já no setor público, a adequação sobre dados requer a adaptação de sistemas e o reconhecimento da segurança e da privacidade, de modo que servidores e agentes públicos compreendam as distinções entre informações públicas e dados pessoais (PINHEIRO, 2018, p. 65 - 71), nos moldes do art. 5º da LGPD, não publicando nenhuma informação além daquela estritamente necessária para a continuidade do serviço público (BRASIL, 2018).



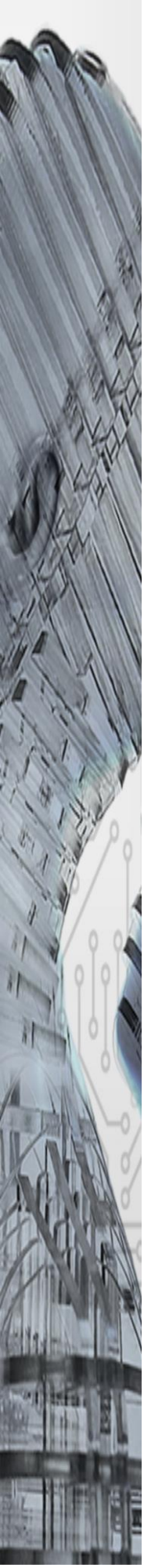
No setor financeiro, como uma das áreas de maior tratamento de dados pessoais, as regras sobre proteção de informações, tais como o sigilo bancário instituído pela Lei Complementar 105/2001, a Lei do Cadastro Positivo (Lei 12.414/2011), as normas de Direito do Consumidor, as regras do Banco Central do Brasil - BACEN e a supervisão da Comissão de Valores Mobiliários (CVM), compõem uma parcela setorial com alta regulação, bem como de proximidade com clientes e contínuo tratamento de dados pessoais mediante utilização de anúncios publicitários, a manutenção de contas, ligações de cobrança, envio de correspondências, dentre outras ações, que estarão sujeitas às regras da LGPD.

Muito embora as informações de *Big Data* e de Inteligência Artificial sejam utilizadas como ferramentas para mapeamento de perfis de clientes, ofertas e desenvolvimento de modelos de negócios (GOMES, 2017; MENDES, 2014), a vigência da LGPD acarretará a necessidade de readequação do *modus operandi* de muitas empresas do setor financeiro (BLUM, 2018, p. 35 - 38), visando não romper a linha tênue da privacidade e da segurança de dados, principalmente no tocante à publicidade abusiva, tendo em vista o conhecimento das condições financeiras de clientes.

Ademais, as áreas de Publicidade e Propaganda, como setores autônomos e presentes em grande parte dos bens, produtos e serviços oferecidos no mercado, a partir dos ditames do art. 45, da LGPD, devem redobrar os cuidados quando realizarem perfilamento de consumidores "utilizando de informações advindas da coleta de dados pessoais, para direcionar anúncios" (PINHEIRO, 2018, p. 87). Todavia, a LGPD apresenta maior fluidez e tolerância à publicidade virtual ou física, bem como estabelece claramente os limites e a forma como os anúncios deverão se estruturar.

A Saúde é um setor de atenção especial, conforme se observa pela redação do art. 13 da LGPD (BRASIL, 2018). Seja no setor público, seja no setor privado, a sensibilidade dos dados coletados e tratados representa uma fonte de conhecimento e de estratégias administrativas, no conhecimento das moléstias que acometem a população, sendo permitida a coleta de dados com fins científicos e a criação de políticas públicas, por entes da Administração Pública, devendo ocorrer anonimização conforme preceitua o art. 12 da LGPD.

Todavia, o consentimento para a coleta de dados utilizados em formulários e prontuários médicos e o armazenamento de informações em bancos de dados, deve ocorrer com confidencialidade, sigilo e segurança (TEIXEIRA, 2018, p. 99 - 101), com fulcro na privacidade, sendo também permitidos, quando a finalidade for a prestação de serviços de



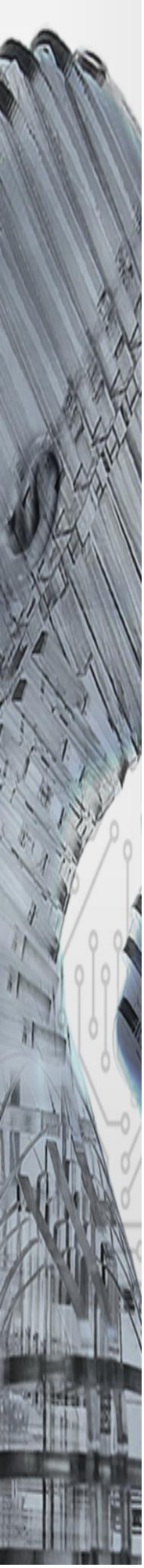
saúde suplementar, mesmo se houver obtenção de vantagem econômica, sendo vedada a simples comercialização da dados obtidos em decorrência da coleta de dados de pacientes, na esfera pública ou privada. O uso de *Big Data*, de informações obtidas consensualmente e em conformidade com a LGPD, pode auxiliar na adoção de medidas profiláticas e preventivas, bem como no controle de epidemias, mas jamais tais informações devem ser utilizadas para justificar atitudes discriminatórias ou desiguais.

As relações trabalhistas também estarão tuteladas pela vigência da LGPD, com a criação dos cargos de *Data Protection Officer* (DPO), que atua como um encarregado da empresa, podendo ser um funcionário ou uma pessoa jurídica terceirizada (PINHEIRO, 2018, p. 38 - 42), comitê ou grupo de serviço. Este setor da empresa terá por função precípua a aplicação de *compliance* em segurança de dados pessoais, "de modo que equipamentos de trabalho e funcionários estejam ajustados à realização de serviços em conformidade com os níveis de segurança esperados" (BIONI, 2018, p. 167) e observando as determinações emitidas pela ANPD.

No setor público, tornou-se possível que a Administração Pública realize o tratamento de dados armazenados em bancos, a respeito da segurança nacional e da segurança pública, sob sua guarda, ou terceirize estas funções a uma pessoa jurídica de direito privado, de modo que "a geração de relatórios dos atos realizados pelo Poder Público deve ser disponibilizada à população, aumentando a transparência" (BLUM, 2018, p. 156). O compartilhamento de informações do setor público para entidades privadas também foi previsto pelo art. 26 da LGPD, bem como o § 1º do art. 26 trouxe as exceções ao compartilhamento de tais dados com entes privados (BRASIL, 2018).

Por força da Medida Provisória 869/2018, posteriormente convertida na Lei nº 13.853/2019, ficou instituída a Autoridade Nacional de Proteção de Dados – ANPD, vinculada à Presidência da República (BRASIL, 2018). Dentre as suas competências, a ANPD pode requisitar informações e fiscalizar quando houver configurado o descumprimento à legislação, mediante processo administrativo. Deste modo, a atuação da ANPD se dá de forma articulada com outras autoridades reguladoras e órgãos do Executivo, como o BACEN e a Receita Federal. Como a criação da ANPD deve estar vinculada à Presidência da República, compondo órgão do Executivo Federal, suas competências podem ser ampliadas e moldadas conforme o cenário prático de cada momento social.

Já a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, conforme determina a LGPD, após complementação dada pela Lei nº 13.853/2019, é de



competência da ANPD, conjuntamente à criação do Conselho Nacional de Proteção de Dados Pessoais e Privacidade, como um fórum permanente de comunicação em cooperação técnica com órgãos e entidades da Administração Pública advindos de setores econômicos e regulatórios diversos, também definindo as formas como a ANPD aplicará sanções, penas e multas, que conforme o artigo 52, § 5º da LGPD, os valores arrecadados serão destinados ao Fundo de Defesa dos Direitos Difusos – FDD, órgão vinculado ao Ministério da Justiça, justamente visando à reparação de danos por violações e à difusão de conteúdos didáticos.

2.5.4 A LGPD e o RGPD em perspectiva comparada

As normas e efeitos do RGPD, a exemplo, podem ter aplicabilidade para brasileiros quando: (I) as filiais ou subsidiárias de empresas europeias sediadas em território brasileiro executarem qualquer forma de tratamento de dados de cidadãos europeus que residam na Europa, pois lá foram coletados; (II) quando empresas brasileiras realizarem transações de envios ou recebimentos de dados pessoais com qualquer empresa sediada na Europa; (III) quando empresas brasileiras que tratarem dados pessoais de cidadãos europeus, ainda que estes não tenham sido coletados por empresas europeias; (IV) quando forem realizados em subsidiárias ou filiais no Brasil de empresas não europeias, quaisquer tratamentos de dados de europeus, ainda que indiretamente. Apesar de haver previsão no RGPD sobre a aplicação extraterritorial de suas penalidades e multas para infrações e vazamentos de dados pessoais, ainda se encontram em construção as diretrizes específicos sobre como os entes jurídicos deverão proceder, quando da necessidade de análise de tais procedimentos, como se propõe analisar no presente estudo.

A LGPD brasileira apresenta-se de maneira menos extensa do que o RGPD, com apenas 64 artigos (BRASIL, 2018), face aos 99 artigos e mais 173 parágrafos de considerações preambulares da legislação europeia (CUE, 2016). As similaridades entre institutos, princípios e objetivos fixados nas normas, permitem a percepção de transplante ao ordenamento jurídico brasileiro do modelo europeu, muito embora seja perceptível, também, o emprego de institutos jurídicos tipicamente brasileiros. Segundo Patrícia Peck Pinheiro (2018, p. 44 - 45), a similitude decorre das aproximações visadas entre os mercados, bem como aduz à facilitação da transferência de dados, com leis e regulamentos de compatibilização simplificada de forma a ser possível extrair a seguinte tabela comparativa:

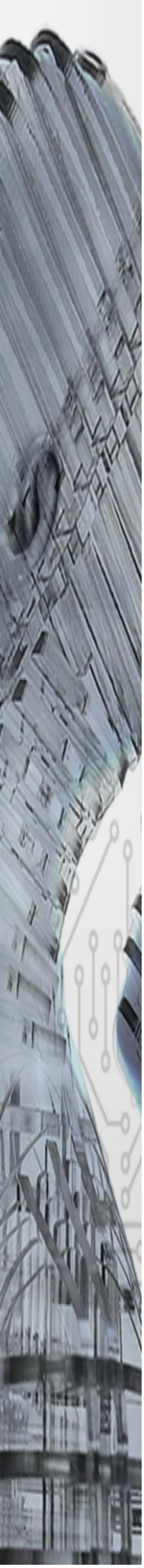
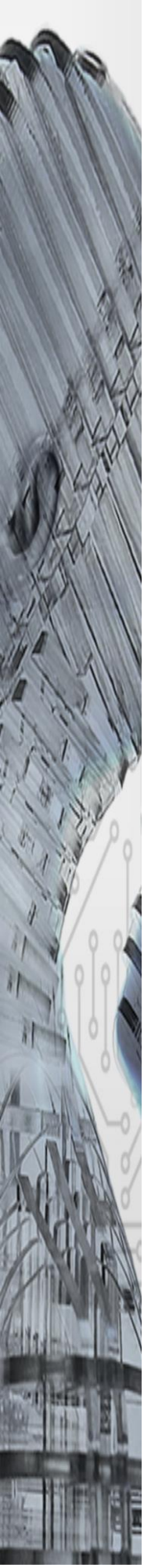


Tabela 4: Comparação entre dispositivos do RGPD e a LGPD.

RGPD	LGPGP
Objetivo da Lei - Art. 1.º	Objetivo da Lei - Art. 1.º
Aplicação territorial – Art. 2.º	Aplicação territorial – Art. 3º
Conceitos e definições – Art. 4.º	Conceitos e definições – Art. 4º
Princípios – Art. 5.º	Princípios – Art. 6º
Limitações do tratamento – Art. 6º	Limitações do tratamento – Art. 7º
Consentimento – Art. 7º	Consentimento – Art. 8º
Dados pessoais de crianças – Art. 8º, §1º	Dados pessoais de crianças – Art. 14, § 1º
Tratamento de dados sensíveis – Art. 9º, § 2º, "d" e "e".	Tratamento de dados sensíveis – Art. 11, II "b" e "g"
Dados anonimizados – Art. 11	Dados anonimizados – Art. 12
Formas de coleta – Art. 14	Formas de coleta – Art. 37
Direitos do titular – Art. 15	Direitos do titular – Arts. 17, 18 e 19
Direito ao esquecimento – Art. 17	Direito ao esquecimento – Art. 18, IV
Políticas de proteção de dados- Art. 24, § 2º	Políticas de proteção de dados – Art. 50
Representantes – Art. 27	Representantes – Art. 61
Controle e operação – Art. 28, § 3º	Controle e operação – Art. 39
Relatório de Impacto - Art. 35	Relatório de Impacto – Art. 38
Consulta prévia – Art. 36	Consulta prévia – Art. 36
Transferência internacional de dados – Art. 44 e seguintes.	Transferência internacional de dados – Art 33 e seguintes.
Segurança no tratamento – Art. 32	Segurança no tratamento – Art. 46
Encarregado de dados pessoais – Art. 37 a 39	Encarregado de dados pessoais – Art. 41
Conformidade – Art. 41	Conformidade – Art. 50 e 51
Comitê Europeu para Proteção de Dados – Art. 68 e seguintes.	Autoridade Nacional para Proteção de Dados – Art. 58 a 59 e MP 869/2018
Responsabilização de agentes – Art. 82	Responsabilização de agentes – Art. 42

Fonte: Elaboração própria.

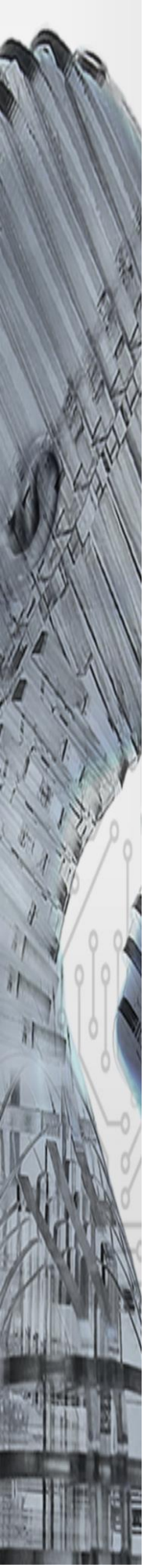


A complementação da LGPD, dada pela MP n° 869/2018 (BRASIL, 2018), convertida na Lei nº 13.853/2019 (BRASIL, 2019), aproximou ainda mais o contexto de proteção de dados do Brasil com a legislação do RGPD e da União Europeia. Um dos aspectos de maior relevância é a realização da Jurisdição transfronteiriça ou "jurisdição *crossborder"*, que está prevista em ambas as legislações em comento, de modo que estas sejam aplicáveis a empresas europeias sediadas no Brasil, empresas brasileiras sediadas na Europa, bem como de europeus residentes no Brasil ou brasileiros residentes em países integrantes da União Europeia, sendo utilizado para fins de fixação do critério de competência jurisdicional a nacionalidade do titular de dados, a legislação do local onde os dados foram colhidos/cedidos ou a legislação da sede da empresa que realizou o tratamento dos mesmos.

A privacidade, enquanto princípio que norteia o direito à proteção de dados pessoais, demonstra o risco envolvendo o tratamento de dados, o qual deve passar por um aumento nos padrões de segurança de empresas e organismos públicos, a fim de atender às exigências de ambas as normas, RGPD e LGPD, garantindo o respeito a outros princípios fundamentais, tais como a legalidade, a justiça, a responsabilidade, a não-discriminação, limitação de objetivos e a transparência no uso de dados pessoais.

Através do RGPD e da LGPD, estão normatizadas as transferências internacionais de dados, com restrições à transferência transfronteiriça de dados pessoais, devendo as mesmas ocorrerem segundo os critérios da minimização de dados, precisão, limitação de armazenamento e segurança, incluindo integridade e confidencialidade, de modo na vigência de tais normas, as transferências somente ocorreram entre países com um nível adequado de segurança (jurídica) para proteção de dados, ou mediante cláusulas contratuais cujos mecanismos prevejam a proteção de dados (BIONI, 2018, p. 122 - 126).

Em relação às sanções legais administrativas, a LGPD faz previsão no art. 52, de aplicação de multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil em seu último ano de exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Enquanto o RGPD prevê a aplicação de multas leves no valor máximo de até € 10.000.000 ou 2% do faturamento anual total da empresa em relação ao ano anterior, incluindo violações de privacidade por obrigações de projeto, falha em manter registros adequados e falha em atender aos requisitos de segurança (HAUNTS, 2018, p. 42); já para crimes mais severos, a multa máxima é de € 20.000.000 ou 4% do faturamento anual da empresa.



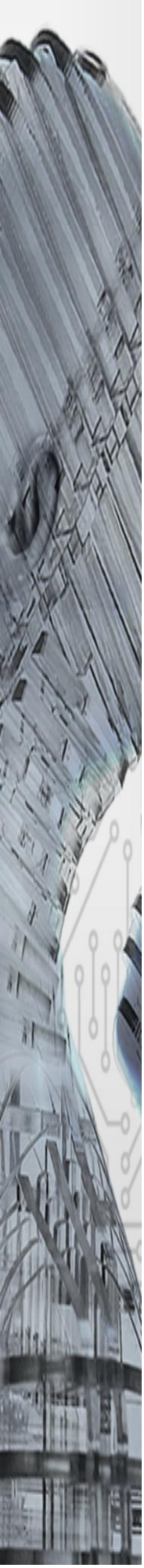
Enquanto o RGPD trabalha com prazos de 30 dias para prestação de dados solicitados por titulares (CUE, 2016), a LGPD segue o padrão geral do Código de Processo Civil brasileiro (BRASIL, 2016), concedendo 15 dias para o acesso à informação pessoal (BRASIL, 2018). Outrossim, a LGPD também introduziu no ordenamento jurídico do Brasil novos direitos, tais como o de portabilidade de dados pessoais e o apagamento dos mesmos, tido como o direito ao esquecimento (TEIXEIRA, 2018, p. 100 - 101), mas já existentes nas leis nacionais sobre privacidade e proteção de dados em alguns países europeus e na Diretiva 46 (CE, 1995).

O registro de impacto mantido pelo controlador de dados, ou DPO, e o mapeamento de dados, "apesar de excessivamente onerosos para as empresas, são capazes de permitir a mensuração do impacto causado por possíveis vazamentos de dados" (HAUNTS, 2018, p. 24), permitindo a organização de maior segurança conjuntamente a um planejamento melhor estruturado sobre segurança, de modo muito similar no RGPD e na LGPD. No mesmo sentido, qualquer intercorrência envolvendo vazamento de dados deve ser notificada à respectiva ANPD nacional ou ao Comitê Europeu para Proteção de Dados, bem como aos titulares afetados, a fim de que se apurem as extensões dos prejuízos e danos, conforme previsto em ambas as normas.

Assim sendo, é perceptível observar similitudes em grande quantidade, todavia guardadas as diferenças necessárias à aplicabilidade e à aquisição de eficácia legal em cada ambiente jurídico-normativo e geopolítico. Acima de tudo, o RGPD e a LGPD possuem um escopo complementar e visam à comunicação entre economias, mercados e governos.

2.6 A Transparência e a Privacidade à luz do Interesse Público

A transparência no acesso à informação pública e a proteção de dados pessoais, oportunizadas pela Lei de Acesso à Informação e LGPD, respectivamente, são elementos essenciais da vida democrática e constam como previsões de caráter fundamental constitucional, além de atuarem como instrumentos de participação dos cidadãos na Administração Pública, estando presentes nos ordenamentos jurídicos de muitos países (BLANKE; PERLINGEIRO, 2018, p. 6 - 17). A interação entre esses direitos (e suas normas correlatas) - ou seja, a maneira de lidar com o acesso público a documentos contendo dados pessoais - pode, no entanto, ser percebida como complicada, dadas as suas naturezas teoricamente antagônicas da publicidade e da privacidade.

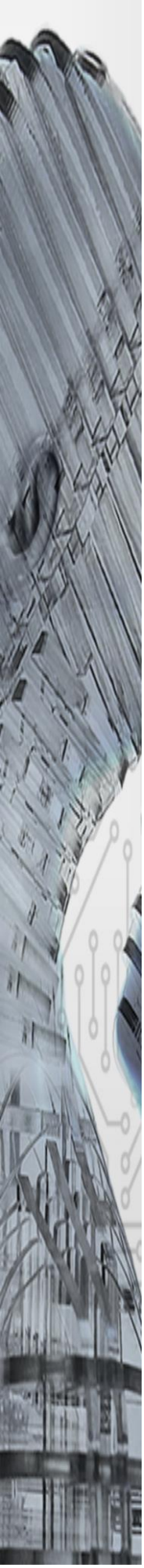


Como as legislações sobre a Liberdade de Acesso à Informação Pública são essenciais à sustentação de governos democráticos, abertos, socialmente responsáveis e comprometidos com a transparência e o combate à corrupção, estas costumam ser claras ao delimitarem o âmbito de sua aplicação somente aos assuntos e organismos administrativos públicos e aos atos de "autoridades públicas" (BLANKE; PERLINGEIRO, 2018, p. 18 - 19), realizados no exercício de suas funções, abrangendo os Poderes Executivo, Legislativo e Judiciário, tendo como base os Princípios da Democracia e do Estado de Direito, de modo que a publicidade é a regra e o sigilo é a exceção (BANDEIRA DE MELLO, 2015, p. 34 - 40).

As Leis de Proteção de Dados Pessoais se preocupam principalmente com "o consentimento, a confidencialidade e a segurança das informações" (BIONI, 2018, p. 115), enquanto "em termos de política legal, as demandas por acesso a documentos dos três setores (poderes) do Governo focam em transparência como um requisito da publicidade, democracia e uma sociedade civil "efetiva" (BLANKE; PERLINGEIRO, 208, p. 27)". Cabe então distinguir dados pessoais e informação pública. Neste sentido, dados pessoais podem ser compreendidos como aqueles personalíssimos e que "compõem parte integrante da vida individual de seu titular" (BIONI, 2018, p. 12). Já a informação pública se refere à disponibilização de todas as atividades da Administração Pública que devam ser ofertadas ao conhecimento geral, a fim de dar ciência sobre atos oficiais que os governos realizam, ainda que, para tanto, sejam utilizados dados pessoais, nos limites necessários para o cumprimento das finalidades (BLANKE; PERLINGEIRO, 2018, p. 33 - 40).

Os órgãos públicos têm o dever de ajudar as pessoas a obterem as informações que buscam, de modo que o procedimento correto para uma autoridade pública seguir ao responder a uma solicitação de informações, na maioria dos casos, pode ser observado em duas possibilidades nas quais as informações sobre indivíduos são prestadas em sede de direito de acesso à informação, sendo elas: (I) quando a informação não se qualifica como dados pessoais, porque a pessoa não é identificável ou sua identidade é inteiramente incidental ou; (II) quando a informação possui dados pessoais referentes ao(s) indivíduo (s), mas não ocorre a violação aos princípios de proteção de dados pessoais ao divulgá-la e o interesse público envolvido supera qualquer interesse individual em não divulgação.

Segundo a LGPD, os dados pessoais estão isentos de divulgação se de tal ato resultar violação de qualquer um dos princípios de proteção de dados (BRASIL, 2018). A transparência sob a LGPD está intimamente relacionada com os requisitos para o processamento de dados pessoais dos indivíduos (PINHEIRO, 2018, p. 104 - 112). Em um



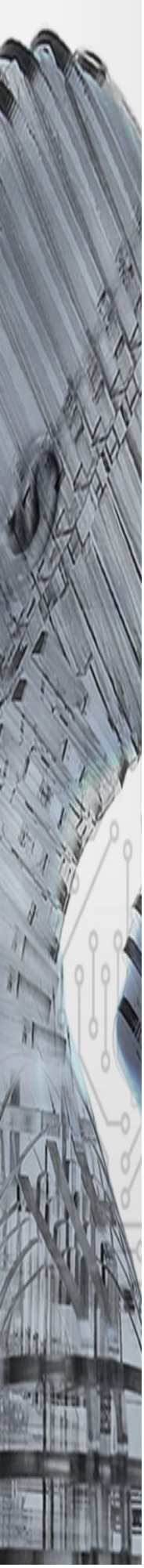
nível geral, requer que os controladores adotem uma abordagem aberta e futura para os indivíduos - permitindo acesso fácil e gratuito a informações claras sobre o processamento de dados pessoais e processos de implementação para facilitar o exercício dos direitos dos indivíduos.

Quando os dados se referem à pessoa que faz a solicitação, a isenção é absoluta Nesse caso, as informações não podem ser liberadas em resposta a uma solicitação de liberdade de informação, mas podem ser liberadas ao solicitante/titular como uma solicitação de acesso a dados pessoais, de acordo com a Lei de Proteção de Dados local e conforme os limites expressos no consentimento (BIONI, 2018, p. 156).

A distinção entre os pontos onde as legislações de proteção de dados pessoais e de acesso à informação pública se sobrepõem é tênue e nebulosa. Os profissionais da informação, particularmente no setor público, podem se tornar os mais prejudicados e culpabilizados, apenas por não alcançarem melhor compreensão a respeito da distinção entre ambos os limites de tratamento de dados, quando interconectados, bem como as restrições à divulgação sob as Leis de Acesso à Informação Pública locais, incluindo as circunstâncias em que uma solicitação deve ser recusada, a fim de proteger os dados pessoais.

Neste ponto, o interesse público e a proteção de dados colidem. Há isenção para uma ampla gama de assuntos onde o sigilo é primordial, ou onde a revelação da informação seria prejudicial à atividade, como: (I) segurança, defesa e relações internacionais; (II) aplicação da lei, auditorias e outras investigações; (III) informações sobre a economia e informações relativas à formulação de políticas governamentais, ou cuja divulgação seria prejudicial à condução efetiva dos assuntos públicos, mas não, em geral, à informação estatística. Aliás, as informações estatísticas e a *Big Data* representam duas fontes de informação que devem ser analisadas cuidadosamente, antes de compartilhadas entre a iniciativa privada e os setores públicos, a fim de se verificar a inexistência ou a total anonimização de dados pessoais antes da reutilização.

Ao lidar com esses casos, é imperativo que os funcionários e agentes públicos responsáveis façam um exame concreto e individual de documentos contendo dados pessoais (PINHEIRO, 2018, p. 75 - 76). Segundo ensinam Hermann-Josef Blanke e Ricardo Perlingeiro (2018, p. 42 - 43), em primeiro lugar, “a divulgação só pode ser recusada se a privacidade de um indivíduo estiver em jogo”; em segundo lugar, “o efeito negativo da divulgação de dados pessoais de alguém deve ser substancial” e, em terceiro lugar, “deve ser examinado se a legislação de proteção de dados permite a divulgação”.

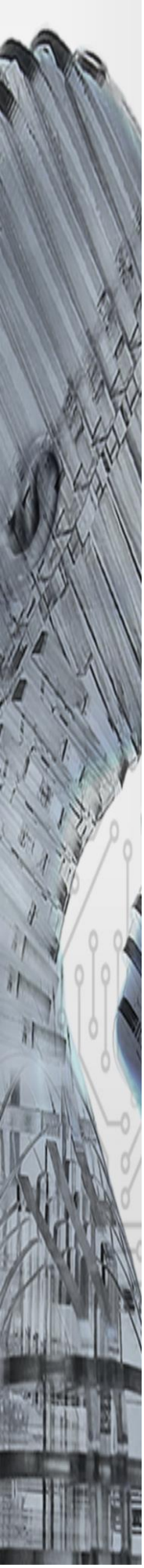


A ocorrência de situações nas quais a divulgação de informações contendo dados pessoais, à luz da Lei de Acesso à Informação (BRASIL, 2011), pode representar possíveis violações aos institutos propostos pela LGPD, devido à chamada supremacia do interesse público em tal divulgação, como defendido por doutrinadores como Celso Antônio Bandeira de Mello (2015), Hely Lopes (2000) e Maria Sylvia Di Pietro (2005), como um princípio fundamental do ordenamento jurídico administrativista brasileiro, implícito na criação e na execução das leis.

Celso Antônio Bandeira de Mello (2015, p. 186 - 194) defende a prevalência dos interesses da coletividade sobre os interesses dos particulares como pressuposto para a manutenção da estabilidade social e a execução de atos, leis e decisões judiciais, face à natureza burocrática dos órgãos da Administração Pública, muito mais dificultosos e demorados do que as resoluções particulares. Seguindo um posicionamento similar, Hely Lopes Meirelles (2000, p. 89 – 96) interpreta o princípio da supremacia do interesse público na dialética do direito administrativo, como característica de superioridade do poder público, com regime jurídico diferenciado das relações meramente particulares, pois representa os interesses coletivos, que têm primazia e exerce funções do poder de polícia, atuando também de forma limitadora quando as atividades privadas possam ameaçar interesses difusos ou coletivos.

Di Pietro (2005, p. 125 - 140), também traz lume à necessidade de valorizar tal princípio quando da elaboração da lei e na sua subsequente execução pela Administração Pública, de modo que todas as normas de Direito resguardem os interesses da coletividade e correspondam à própria manutenção da máquina estatal, como a pacificação social e o bem comum, ainda que se desenvolvam por sobre questões particulares, como a propriedade, relativizando, mitigando ou modulando hipóteses normativas nas quais os direitos individuais cedem diante do interesse público.

Marçal Justen Filho (2005, p. 152 - 187), por sua vez, se opõe à supremacia do interesse público, tendo em vista que o termo “interesse público”, enquanto matriz principiológica e conceitual pode ser amplamente interpretado e dar margem à atuação arbitrária e não-protetiva de agentes administrativos, excedendo os limites da legalidade e do próprio Estado Constitucional Democrático e os valores fundamentais a ele conexos, obstando o controle dos atos – e excessos – praticados pelo poder público (*Idem,* p. 197*)*, tendo em vista a incompatibilidade de se identificar interesse público, como sendo a manifestação do



interesse da maioria, dado o caráter metaindividual e multipolar das democracias constitucionais, que buscam fornecer proteção às minorias.

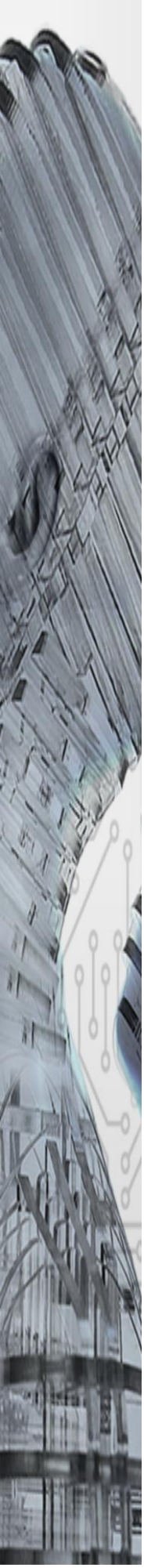
Logo, é difícil concentrar conteúdo exclusivo para definir conceitos de interesse público, tendo em vista as necessidades específicas de sociedades fragmentadas e plurais como as contemporâneas, nas quais não há um único interesse público, mas diversos e muitas vezes antagônicos interesses públicos, não permitindo que o benefício socioeconômico em favor do Estado ofereça maior baliza para a Jurisdição Administrativa (PERLINGEIRO, 2014, p. 79 - 82).

Se não é possível definir com precisão o que vem a ser o interesse público, como admitir que este possa prevalecer sobre os interesses dos particulares? A crescente necessidade de transparência na execução de atos que versam sobre interesses e recursos públicos, à luz dos direitos humanos e do cidadão, majoritariamente advindos da cobrança de taxas e impostos aos contribuintes face à ampliação do acesso a dados e informações provenientes de estudos pormenorizados, necessita organização continuada, para ser colocada à disposição (JELLINECK, 2015, p. 83 - 90).

No mesmo sentido, a atividade administrativa, e especialmente a Jurisdição Administrativa, devem ser orientadas não pelo princípio da supremacia, mas pela máxima realização de todo o conjunto de direitos fundamentais (PERLINGEIRO, 2014, p. 79 - 82), sejam estes de titularidade individual, coletiva ou difusa, onde o "Interesse Público deixa de ser a materialização do exercício de Poder Público, para se transformar numa categoria de prestação de serviços de importância capital no fomento à cidadania e participação popular[69]" (SARLET, 2018, p. 381).

De forma semelhante, as readequações experimentadas pela Administração Pública face à utilização de novas tecnologias eletrônicas propiciam mecanismos de governança voltados para o melhor aproveitamento das Tecnologias da Informação e da Comunicação em setores que realizam a análise de dados e a computação em nuvem, especificamente para melhor atender ao público e gerenciar seu banco de dados central (RAMOS *et al.*, 2014, p. 46 - 60). Conforme ensina Cândido Rangel Dinamarco, *in verbis*:

[69] Um bom exemplo de exercício adequado do Poder Público foi promovido por meio da Emenda Constitucional 45/2004. Com a criação do Conselho Nacional de Justiça (CNJ), em 2005, quando se tentou proporcionar uma maior agilidade ao Poder Judiciário bem como uma transparência em sua estrutura e funcionamento do sistema de poder, estabelecendo função correcional, dentre outras atribuições (BARROSO, 2019, p. 174). A partir de então, o Brasil passou a contabilizar, de forma sistemática, importantes números sobre a realidade jurídica do país (BARROSO, 2019, p. 180). O Judiciário, então visto como responsável pela resolução de conflitos e equilíbrio social começa a ser avaliado principalmente como um prestador de informações científicas e comunicador de dados e serviços à coletividade.



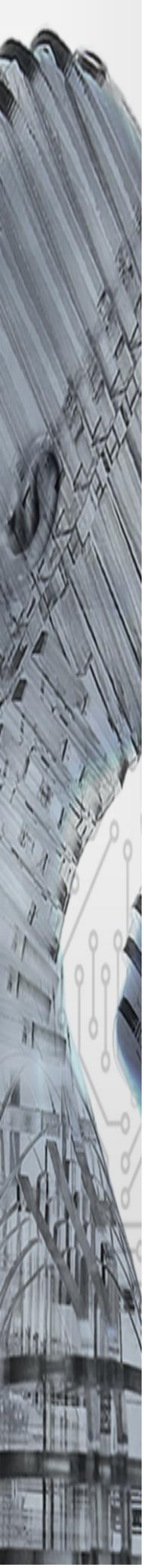
> [...] as técnicas procedimentais constituem o resultado de experiências multisseculares, às quais o legislador aporta as inovações e aperfeiçoamentos que na prática lhe pareçam úteis. As significativas revisitações aos institutos processuais, que se vêm fazendo ultimamente, vão produzindo também alterações nos procedimentos em si mesmos, como modo de adequar a técnica do processo às novas conquistas da ciência. (DINARMARCO, 2017, p. 139)

Deste modo, "a segurança de dados é de extrema importância para as agências públicas e privadas, e qualquer uso de informações privadas do consumidor é estritamente regulado e muitas vezes anonimizado, quando compartilhado com o público" (STAPLETON, 2014, p. 155). Em programas de parceria público-privada, portanto, as empresas privadas, frequentemente solicitadas pelos governos locais, "aplicam medidas contra ameaças cibernéticas controlando o acesso às informações de clientes, anonimizando completamente informações confidenciais dos clientes, como informações de cartão de crédito" (HUDAK, 2006, p. 36), e também controlando o acesso aos aplicativos baixados nos dispositivos móveis dos clientes, "sem dizer da possibilidade de dificultar ou, até mesmo, travar o funcionamento dos servidores das empresas e/ou dos computadores de usuários, impedindo o exercício de suas atividades", (TEIXEIRA, 2018, p. 64), como em ataques de *spam, hackers, malwares* e vírus.

A Administração Pública tem o direito de solicitar certas métricas relativas ao uso de produtos e serviços oferecidos pelas empresas privadas (MENDES, 2014), cujos dados produzidos têm o condão de auxiliar no melhor planejamento urbano, no transporte público[70], na segurança, gestão orçamentária e fiscal, e no bem-estar dos cidadãos, de modo a otimizar as ações futuras e a formulação de políticas públicas voltadas para setores onde as reais necessidades sejam conhecidas com maior clareza e profundidade, em decorrência do compartilhamento de dados privados e públicos (PRIVACY INTERNATIONAL, 2018, p. 32 - 38).

Os processos de parceria também podem se voltar para o compartilhamento de dados com o público em geral. Entre as informações compartilhadas com o governo, nem todas precisam ser disponibilizadas em acesso público (BIONI, 2018, p. 74- 79). No entanto, entre os que obtêm a exposição pública, o governo pode permitir ao público o acesso a dados para fins educacionais e de conscientização.

[70] Por exemplo, através de empresas de aplicativos de compartilhamento de carona (Uber, Lyft, 99 Taxi) e de descontos em hospedagem (Trivago, Decolar.com), nas quais os dados gerados por seus serviços, como número total de caronas, rotas de passeio mais populares, o horário de pico do dia e também o preço médio pago em um determinado passeio em um determinado distrito da cidade, podem ser utilizados para auxiliar cidadãos e gestores públicos a realizarem um melhor planejamento sobre os transportes públicos, o tráfego de veículos e pedestres, a melhoria de infraestruturas e também o planejamento do setor de turismo.



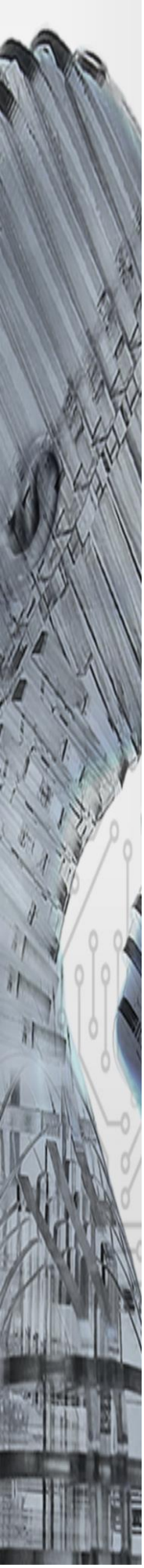
A cooperação público-privada para o compartilhamento de dados compreende também a proteção de dados e a privacidade dos usuários, incentivando "o papel das autoridades públicas para garantir o uso responsável dos dados e a utilização responsável de seu potencial para fins políticos e administrativos voltados para a melhoria da condição de vida dos cidadãos" (WALDFOGEL; PEITZ, 2016, p. 527), dando ao público mais controle sobre seus dados relacionados à mobilidade e quais estratégias podem ser apropriadas.

Mas, "a sensibilidade à proteção da privacidade varia globalmente, em um cenário marcado pelo ceticismo tanto dos tomadores de decisão, como do público em geral" (HAUNTS, 2018, p. 29). "A cooperação público-privada no espaço de dados está emergindo como uma tendência clara que promete benefícios mútuos" (GREGÓRIO, 2018, p. 52). Os dados privados advindos de empresas têm sido utilizados pelos governos, como o da Alemanha (MATTERN, 2008, p. 25), que "visa à abertura dos dados para o público e para o setor privado, com a crença de que resultados inovadores mais amplos se seguirão, não apenas estimulando a inovação, mas também economizando gastos públicos" (BECKER, 2018, p. 80), onde novas tecnologias podem aumentar a eficiência da prestação de serviços - por exemplo, a fusão de dados em *Big Data* de tráfego e dados meteorológicos específicos do local, voltados para a redução dos riscos de acidentes (BIONI, 2018, p. 39).

Embora existam histórias de sucesso, "a escala ilimitada, a fragmentação temática e a dispersão geográfica dessa cooperação destacam a falta de um quadro claro para a criação de colaboração baseada em dados entre os setores públicos e privados" (SCHOLZ, 2012, p. 55), aumentando os custos para o setor privado e reduzindo os benefícios potenciais do amplo compartilhamento de dados entre jurisdições de Estados distintos e setores públicos diversos (HAUNTS, 208, p. 30).

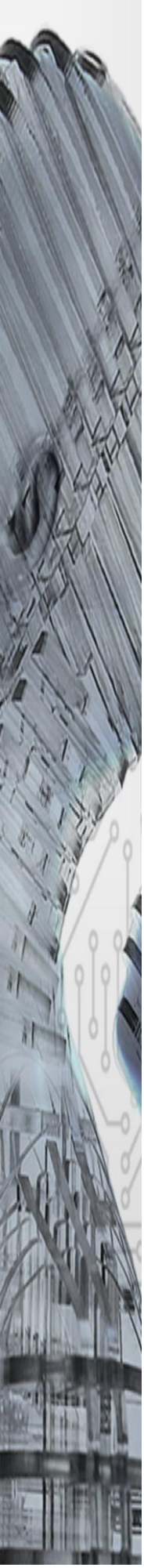
Com base nos resultados de uma avaliação de impacto (EUROPEAN COMISSION, 2015), a Comissão Europeia buscou a conformidade com o Regulamento Geral sobre a Proteção de Dados da EU, atualizando a Diretiva 833/2011, relativa aos dados abertos e à reutilização de Informações do Setor Público (ISP) - que podem abranger, por exemplo, desde dados pessoais tornados anônimos sobre o consumo de energia das famílias até informações gerais sobre os níveis nacionais de educação, no quadro que estabelece as condições em que os dados do setor público devem ser disponibilizados para reutilização, com especial destaque para os crescentes volumes de dados de valor elevado atualmente disponíveis.

Os benefícios estimados a partir desta atualização visam a propiciar adaptações do novo ambiente digital às normas em matéria de proteção da privacidade nas comunicações



eletrônicas de forma que grande parte do conteúdo do setor público possa ser acessado e gratuitamente reutilizado, permitindo que pequenas e médias empresas, como também jovens empresas possam participar de novos mercados no fornecimento de produtos e serviços baseados em dados (EUROPEAN COMISSION, 2015). Ademais, a abertura de dados públicos oferta à inciativa privada informações a respeito de dados de alto valor, como dados estatísticos ou geoespaciais, de transportes e serviços públicos.

Igualmente, as preocupações sobre o uso de dados comercialmente sensíveis, proteção de privacidade e segurança cibernética também requerem atenção. Para o setor público é importante o reconhecimento e a utilização de informações de *Big Data* e como um importante recurso para ganhos sociais e econômicos (BIONI, 2018, p. 40 - 41). Alguns governos entraram em cooperação com o setor privado para o compartilhamento de dados, incluindo programas de melhoria de sistemas e envolvendo indivíduos que competem pelo uso mais inovador e sustentável de dados (TEIXEIRA, 2018, p. 264 - 270). Assim, Hermann-Josef Blanke e Ricardo Perlingeiro advertem no seguinte sentido:



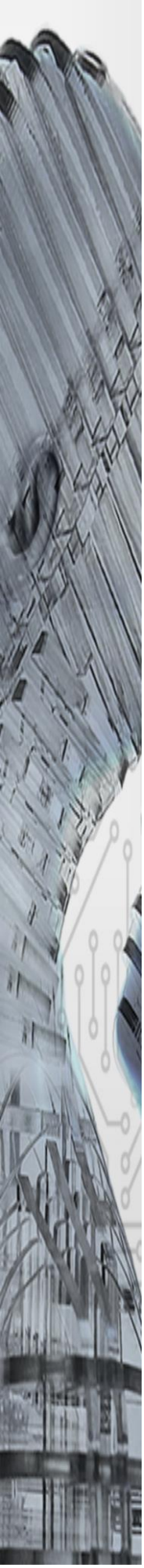
> Vale a pena pensar sobre até que ponto a eficácia das leis de acesso à informação está ligada às chances de sucesso dos cidadãos com reivindicações derivadas do acesso a informações de interesse geral. O sistema jurídico é adequadamente estruturado para atingir os objetivos dos "direitos" de acesso à informação em relação às suas dimensões sociais? Quais são, de fato, esses objetivos? Uma preocupação extremamente importante é verificar a conduta honesta por parte das autoridades públicas - pelo menos preventivamente - no combate à ilegalidade, especialmente a corrupção, em instituições governamentais e autoridades nacionais ou supranacionais. (BLANKE; PERLINGEIRO, 2018, p. 56, tradução nossa[71])

Sob tais espeques, o direito de acesso à informação como um dos Direitos Humanos Fundamentais (SARLET, 2018, p. 98), desponta na correlação entre o tratamento de dados públicos e a sua disponibilização aos cidadãos e terceiros interessados (*e.g.:* empresas, cidadãos estrangeiros, inteligências artificiais), mormente nos Estados Constitucionais Democráticos, cuja universalidade dos acessos a dados públicos representa o esteio de um sistema lastreado na transparência e na circulação de informações verídicas, as quais sustentam a opinião pública e encorajam o exercício de supervisão, cobranças e controles, por parte da população, aos agentes e administradores públicos, de modo conjunto e organizado (BLANKE; PERLINGEIRO, 2018, p. 50 - 56).

Outros dois pontos sensíveis no compartilhamento de dados públicos e privados se referem: (I) à falta de capacidade suficiente no setor público para lidar com a escala, o escopo e a velocidade de novas fontes de dados, posto que a ciência de dados normalmente não faz parte do conjunto de habilidades que as agências públicas buscam no currículo profissional de seus administradores, como também (II) à baixa contratação de cientistas de dados pela iniciativa pública, para analisar e quantificar dados e informações que ultrapassam a mera percepção orçamentária, a qual fica relegada à iniciativa científico-acadêmica para adquirir maior desenvolvimento. Ambos os fatores citados dificultam a capacidade dos órgãos públicos para realizar análises de alta qualidade dos dados que a Administração Pública coleta ou exige que o setor privado forneça.

A análise de *Big Data* também pode melhorar sobremaneira a capacidade do setor público para realizar políticas baseadas em evidências, "com base na possibilidade de enxergar o panorama completo ao invés de fazer estimativas a partir de uma pequena amostra coletada" (SCHOLZ, 2012, p. 87). Além disso, "usos específicos de *Big Data* podem

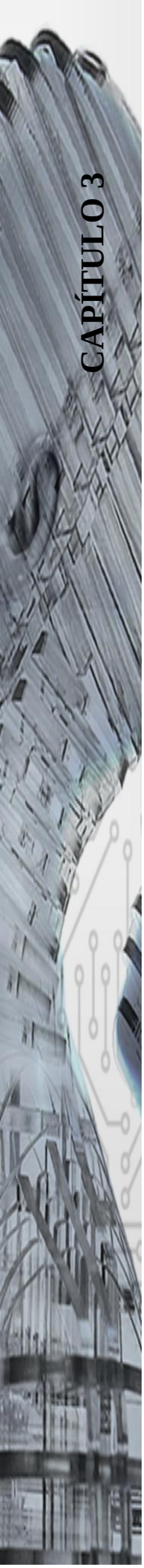
[71] Do original, em inglês: "*It is Worth thinking about the extent to which the effectiveness of information access laws is connected with the chances of success of citizens with claims that are derived from access to information of general interest. Is the legal system adequately structured to achieve the objectives of the "rights" of access to information with respect to its social dimensions? What in fact are those objectives? One extremely important concern is to check for honest conduct on the part of the public authorities - at least preventively – to combat illegality, especially corruption, in government institutions and national or supranational authorities*". *In: The Right of Acess to Public Information*, Springer, 2018.



possibilitar o surgimento de soluções inovadoras de transporte e mobilidade adaptadas, que em última análise são capazes de oferecer serviços públicos com níveis de melhoramento de conforto e conveniência" (LIBERT, 2014, p. 33).

O futuro desponta as parcerias público-privadas, à medida que mais empresas privadas se envolvam em áreas que influenciam ou lançam luz sobre as práticas do setor público e da forma como a população em geral consome produtos e serviços, cujos impactos tocam ambos os setores. Na senda da proteção de dados pessoais, face à transparência da informação pública, portanto, importa agir com ponderamento e bom senso na análise e publicação de informações capazes de causar danos morais ou pessoais irreversíveis a cidadão ou residente no país, bem como evitar demandas sob tais termos a qualquer setor, autoridade ou agente público, de modo que uma norma não se sobreponha à outra e diminuam parcialmente as suas eficácias, enquanto o Legislador não revê formas mais adequadas e juridicamente seguras para delimitar com maior clareza os diálogos entre ambas as fontes.

Deste modo, os horizontes e perspectivas das parcerias público-privadas envolvendo a proteção, o uso, a reciclagem e a reutilização de dados pessoais num meio ambiente economicamente e juridicamente sustentáveis, na tendência futura de expansão sob a moldura normativa dada pelas Leis de Proteção de Dados na maioria dos países, carecerá de abordagens cada vez mais abertas e colaborativas ao trabalhar com os governos locais, sincronizando plataformas tecnológicas para relatórios mais diretos e transparentes de dados, como também métodos cada vez mais seguros de armazenamento e compartilhamento de dados, em qualquer nível da Administração Pública e da jurisdição, quando esta última deverá produzir adaptações, jurisprudências e regulamentos administrativos capazes de harmonizar a Economia da Informação e os fenômenos dos mercados digitais com as regras nacionais e internacionais de proteção de dados pessoais, dentro de suas configurações jurídicas, porém preservando e reafirmando os direitos humanos e constitucionais conexos, em prol da melhoria social comum.



CAPÍTULO 3

A JUR0ISDIÇÃO NA PROTEÇÃO DE DADOS PESSOAIS

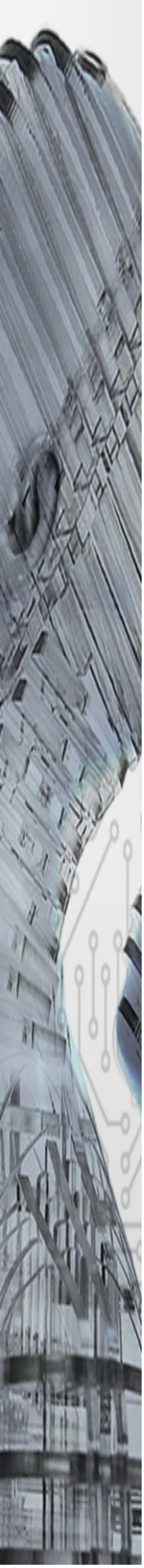
A Internet é "descentralizada e inerentemente amorfa; não é uma entidade física ou tangível" (STAPLETON, 2014, p. 33). Portanto, o ciberespaço existe em um "mundo virtual" onde os milhões de roteadores garantem que as informações cheguem ao seu destino. Ao contrário da rede telefônica na qual se baseia, ela tem a capacidade de localizar o servidor dentro ou fora da jurisdição, distinguindo a atividade da Internet de outras formas de interação. No entanto, a própria singularidade da Internet ameaça ser a sua fraqueza, conquanto induz ao aumento da exposição das partes às leis de outros países e aos tribunais de outras jurisdições, criando incertezas sobre garantias, direitos e reduzindo todo o potencial do comércio eletrônico.

Não obstante à ciência de tais fatos, as regras sobre a proteção de dados pessoais, para serem válidas e eficazes, precisam atingir o mundo real e o ciberespaço, exercendo a jurisdição tanto nos limites territoriais, quanto em outros Estados, além do nebuloso campo de regras aplicáveis ou moldáveis às relações no ciberespaço, "de modo que os tribunais possam exercer a tutela jurisdicional de maneira clara e juridicamente segura, em todas os campos onde as relações humanas sejam realizadas" (GLOBAL PARTNERS DIGITAL, 2018, p. 44).

Em um ambiente de construção de novas práticas judiciais, doutrinárias e de jurisprudência transnacional, as legislações sobre proteção de dados pessoais orgânicas dos Estados parecem mais voltadas para a proteção da população e das empresas públicas e privadas contra atos indevidos (de coleta, tratamento e armazenamento) ocorridos no exterior (TEIXEIRA, 2018, p. 533 - 534), do que direcionadas à criação de mecanismos capazes de evitar conflitos jurisdicionais com outros Estados.

Nessa perspectiva, a proteção de dados pessoais como direito humano inalienável e constitucional fundamental presente nas Cartas Magnas de muitos países, necessita desenvolver bases jurisdicionais mais adaptadas aos problemas legais provenientes do mercado internacional comum, numa perspectiva mais fluida em relação à forma como a jurisdição é tradicionalmente exercida e dialogando com os contextos práticos do Direito doméstico de Estados distintos (BIONI, 2018, p. 157 - 162) especialmente voltados para o exercício jurisdicional nacional e transfronteiriço.

Os instrumentos de cessão e de consentimento representam elementos fundamentais da proteção de dados pessoais e estão presentes nos contratos internacionais, explicados adiante, conforme introduzido pelas palavras de Nádia de Araújo:



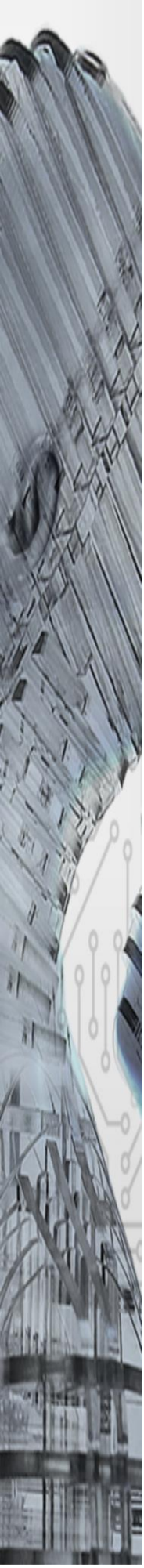
> O que caracteriza o contrato internacional é a presença de um elemento de estraneidade que o ligue a dois ou mais ordenamentos jurídicos nacionais. Por exemplo, basta que uma das partes seja domiciliada em um país estrangeiro ou que um contrato seja celebrado em um país, para ser cumprido em outro. Nesses casos, as partes podem procurar prever situações futuras, estabelecendo regras de direito substantivo no bojo do contrato, para resolver essas situações, e ainda procurar determinar onde e como o litígio dali decorrente será julgado através de cláusulas de foro e arbitragem. (ARAÚJO, 2009, p. 29)

Deste modo, o exercício jurisdicional carece de embasamento formal capaz de dialogar entre as normas de direito privado, público, consumerista, cível, penal, administrativo e constitucional (ARAÚJO, 2011, p. 30 - 32), enquanto observa as normas de proteção de dados nos "construtos jurídicos internacionais correlatos, tendo como foco a harmonização de interesses multipolares e transfronteiriços" (MCLEAN, 2010, p. 184), além do "fornecimento de informações sobre fenômenos jurídicos e impactos sociais para o desenvolvimento de regras sobre privacidade e proteção de dados pessoais em outras áreas da lei" (STRENGER, 2003, p. 42).

Neste ponto, Cândido Dinamarco e Bruno Lopes definem a jurisdição nos seguintes termos, *in verbis*:

> A jurisdição costuma ser conceituada com a tríplice qualificação com poder, como função e como atividade, mas essa assertiva merece uma retificação. Ela não é propriamente um poder, mas uma expressão do poder estatal, o qual é uno e não comporta qualquer ramificação em uma pluralidade de poderes diversificados – o Estado não tem mais de uma capacidade de decidir imperativamente e impor decisões. Essa capacidade é uma só, e o que diferencia seu exercício em variados setores da atuação do Estado é a função exercida em cada um deles. A função exercida na atividade legislativa é a de instituir normas de caráter geral e abstrato destinadas a reger no futuro a vida dos integrantes da sociedade (legislação). A função exercida na atividade administrativa é a de promover o bem comum mediante a oferta de serviços e segurança à população (administração). E a função exercida na atividade jurisdicional consiste na busca da pacificação de sujeitos ou grupos em conflito. É mais correto, portanto, qualificar a jurisdição como uma expressão do poder estatal exercida com a função de pacificar e mediante as atividades disciplinadas pela Constituição e pela lei. (DINAMARCO; LOPES, 2016, p. 77)

Não somente nas leis de proteção a dados, a jurisdição internacional é também suscitada em questões envolvendo direitos de nacionalidade e a condição jurídica do estrangeiro, no Processo Civil Internacional, nas coletas de provas em Estados diferentes, na Arbitragem Internacional, principalmente a respeito de contratos, no Direito de Família e Sucessões, em questões empresariais, tais como nos setores de energia, petrolíferas e de transferência de tecnologias, em questões de Direito Marítimo e em Tratados de Cooperação Econômica e Judiciária regionais, como ocorrem no Mercosul e na União Europeia (ARAÚJO, 2011; MCLEAN, 2010; VOIGT; BUSSCHE, 2018).



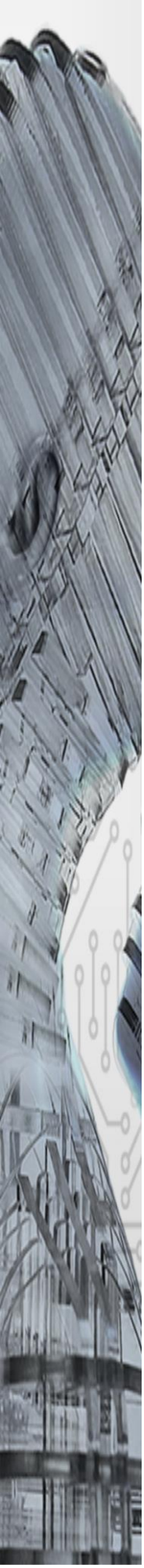
Entretanto, as leis de proteção a dados têm contato com a jurisdição internacional de forma bastante ampla, considerando a utilização de equipamentos e tecnologias conectadas à Internet, realizando contínua coleta e tratamento de dados, de forma a ser possível classifica-las como normas compostas por "disciplinas jurídicas interoperantes", com possível jurisdição concorrente. Neste sentido, Nádia Araújo aponta para as seguintes definições:

> A jurisdição é um dos elementos da soberania do Estado, e só a este compete determina-la. No Brasil é regulada pela Constituição, no capítulo do Poder Judiciário. No plano internacional constitui princípio assente que ao Estado, na esfera de sua jurisdição, cabe determinar a competência dos tribunais, assim como sua organização, as formas de processo, a execução das sentenças e os recursos contra as suas decisões. (ARAÚJO, 2011, p. 229)

Muito embora os princípios fundamentais para a aplicação das leis de proteção de dados pessoais sejam semelhantes entre regiões e sistemas jurídicos (KAZEMI, 2018; ASAI, 2018; DUGGAL, 2018; HAUNTS, 2018; PINHEIRO, 2018), as miríades a respeito do "exercício jurisdicional em demandas conexas, concorrentes ou sobrepostas são apresentadas em cada lei de maneira substancialmente diferente" (ARAÚJO, 2011, p. 84). Neste prisma, os dispositivos presentes nas leis de proteção de dados têm fundamentado juridicamente um número crescente de disputas jurisdicionais (PRIVACY INTERNATIONAL, 2018, p. 53 - 56), muitas delas lastreadas nas transações comerciais e contratos celebrados no ambiente virtual.

Em vista dos critérios sobre o exercício jurisdicional, suas extensões e formas são delimitadas não somente pelos escopos previstos nas leis de proteção de dados pessoais, como também mediante diálogo entre as normas, regras e princípios de fontes do Direito conexas a cada caso, seja de matriz pública ou privada, nacional ou internacional, seguindo seu aspecto geracional (ARAÚJO, 2009, p. 37 - 40). A partir do fato gerador de aplicação das leis de proteção de dados, como sendo as normas vigentes e mais adequadas à resolução de conflitos advindos de fatos, atos ou negócios jurídicos realizados no momento em que os dados pessoais são coletados e processados, "tais leis podem ser aplicadas a quase todas as operações realizadas no ambiente virtual, pois os conceitos e princípios da privacidade e da proteção de dados pessoais podem ser interpretados expansivamente" (BECKER, 2018, p. 66), de modo a ampliar o seu âmbito de competência e escopo. Nas palavras de Nádia de Araújo:

> Diante dessa pluralidade de sistemas jurídicos, ocorre o conflito de leis no qual a situação jurídica poderá ser regulada por mais de um ordenamento. As situações multiconectadas possuem características próprias e distintas das situações internas, necessitando de regulamentação específica. (ARAÚJO, 2011, p. 35)



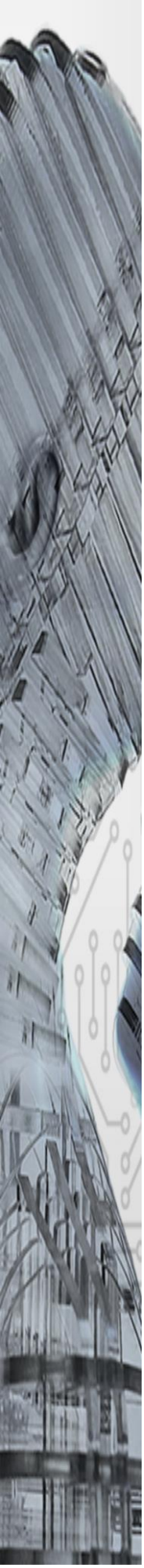
Deste modo, torna-se importante a análise mais aprofundada sobre as formas de jurisdição mais adequadas à prática jurisdicional comum, tendo por base o antagonismo fixado pela ineficiência *versus* a exorbitância sobre os princípios jurisdicionais, numa relação limitada pela jurisdição e pela finalidade de tutela e resolução dos conflitos. Para tanto, é importante compreender de quais formas as violações à privacidade e à proteção de dados pessoais poderão requerer a tutela jurisdicional, considerando um cenário de sobreposição de leis nacionais e internacionais. Outra importante análise advém dos critérios necessários para acolhimento e fixação de competência para julgar, tendo em vista a territorialidade como princípio presente nos instrumentos de cessão de dados pessoais; quais são os limites estabelecidos no novo CPC e nas legislações brasileiras para a adjudicação e processamento de pedidos lastreados em violações à proteção a dados pessoais, conforme a moldura normativa do ordenamento jurídico nacional e; de quais maneiras a LGPD pode se tornar um mecanismo de cooperação internacional e de fortalecimento dos Direitos Humanos e Constitucionais Fundamentais, no ambiente virtual.

3.1 Princípios para a formulação da jurisdição na proteção de dados

Os princípios e bases jurisdicionais onde se fundamentam as leis de proteção de dados delimitam também o conjunto de objetos jurídicos abrangidos pelas normas e fixam critérios capazes de permitir a aplicação das jurisdições dos Estados, na forma da atuação dos juízes, visando à consecução legal de maneira eficaz, adequada e segura e considerando os possíveis impactos advindos da execução de sentenças, em médio e longo prazos. Cândido Dinamarco e Bruno Lopes ensinam que:

> Não se fala hoje em tutela de direitos mas em tutela jurisdicional às pessoas, qualificada como o amparo que, por obra dos juízes, o Estado oferece a quem tem razão em uma causa posta em juízo. Tutela é ajuda, proteção. É jurisdicional a proteção outorgada mediante o exercício da jurisdição, para que o sujeito beneficiado por ela obtenha, na realidade da vida e das relações com as coisas ou com outras pessoas, uma situação mais favorável do que aquela em que antes se encontrava. Sabido que o escopo magno do processo civil é a pacificação de pessoas e a eliminação de conflitos segundo critérios de justiça, consistindo nisso a função estatal a que tradicionalmente se chama jurisdição, segue-se que compete aos órgãos jurisdicionais outorgar essa proteção aquele cuja pretensão seja merecedora dela. (DINAMARCO; LOPES, 2016, p. 22)

Como instituto de grande relevância, "o princípio da Territorialidade trata da competência do Estado-juiz, baseada nos atos jurídicos ocorridos no território do Estado em discussão" (MCLEAN, 2010, p. 57). Logo, bastaria ser considerado o local de ocorrência do ato para definir a competência para julgar. Todavia, as leis de proteção de dados observam o princípio da Territorialidade Objetiva, o qual analisa "o ato em questão quando este for



iniciado no exterior, mas completado no território do Estado" (DINAMARCO; LOPES, 2016, p. 23), ou que "um elemento constitutivo do comportamento ocorra no território nacional – tendo em vista a dificuldade de se precisar o local de realização de uma ocorrência" (BANDEIRA DE MELLO, 2015, p. 67) em ambiente virtual.

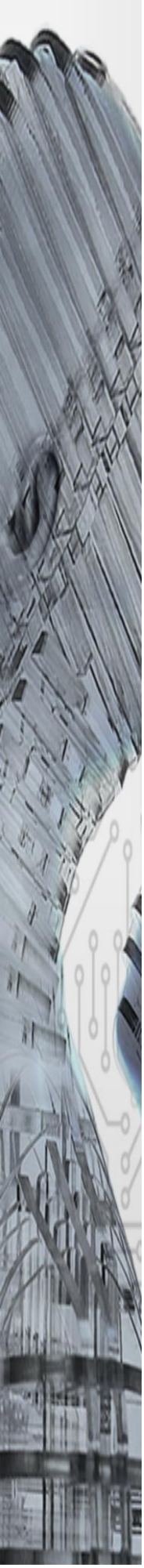
Para tanto, o princípio da territorialidade objetiva em privacidade e proteção de dados pessoais "tende a considerar o local da coleta dos dados físicos ou o local de utilização do equipamento eletroeletrônico" (BIONI, 2018, p. 96) utilizados para coletar ou ceder dados pessoais, como território titular da competência jurisdicional. No plano do Direito Internacional Privado, Nádia Araújo leciona nos seguintes termos:

> Responder à questão relativa à competência internacional é o primeiro passo para abordar uma hipótese multiconectada. Sua resposta deve preceder o questionamento sobre a lei aplicável, em função não só da lógica, como também da cronologia. Enquanto o conflito de jurisdições diz respeito à determinação do *locus* em que a prestação jurisdicional terá lugar, o conflito de leis no espaço pertine ao coração do Direito Internacional Privado. O juiz da causa precisa determinar primeiro sua competência, e em seguida utilizar o método conflitual para determinar a lei aplicável ao caso concreto. (ARAÚJO, 2011, p. 226)

O princípio da Personalidade, sob o prisma da jurisdição exercida em dados pessoais, pode ser fixado como base na nacionalidade do agente causador do dano (princípio da personalidade ativa) ou da vítima (princípio da personalidade passiva) (MENDES; BRANCO; COELHO, 2018, p. 182 - 183). "Embora o princípio da personalidade seja usado principalmente no direito penal, também existem exemplos de aplicação no direito civil" (BANDEIRA DE MELLO, 2015, p. 68). O princípio da personalidade passiva tem sido criticado, mas o princípio da personalidade ativa ainda é usado como base para a jurisdição em várias áreas, tais como tributação, direito a voto e proteção diplomática (ARAÚJO, 2011, p. 77 - 79).

Desta forma, o princípio da Personalidade na lei de proteção de dados, em correlação com o princípio da Territorialidade, pode ser aplicado de forma extensiva também à jurisdição administrativa exercida por Agências ou Autoridades de Proteção de Dados nacionais, em face de controladores de dados fora do Estado de residência de titulares, que processaram dados sobre estes últimos, de forma a basear a jurisdição na nacionalidade do titular dos dados.

O princípio da Responsabilidade imputa ao coletor primário da informação pessoal a responsabilidade pela conformidade com o quadro de privacidade original, aplicado quando e onde os dados foram coletados, independentemente das outras organizações ou países para os quais são posteriormente transferidos e armazenados os dados pessoais (MCLEAN, 2010, p.



79 - 85). Sob tal interpretação, o princípio da Responsabilidade parece assegurar que as proteções da lei nacional onde os dados foram originalmente coletados, prossigam permanentemente com os dados (BECKER, 2018, p. 32 - 35) e continuem a ser aplicáveis, inclusive quando estes possam vir a ser transferidos para o exterior, "mesmo que prevista a sua reutilização/reciclagem, com a possiblidade de responsabilização do controlador original dos dados pelo processamento subsequente em outro país por um terceiro, de forma prejudicial à privacidade do titular" (KAZEMI, 2018, p. 135).

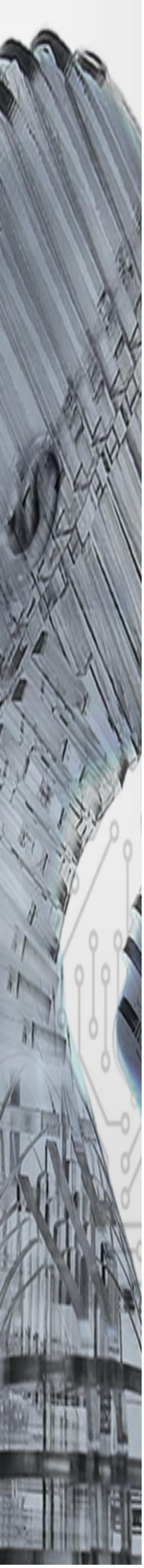
O princípio de Proteção, no esteio das legislações de proteção de dados pessoais, atua de maneira voltada à proteção de um Estado e em diálogo com o Princípio da Segurança Nacional, "utilizando dados digitalizados – sigilosos ou não, realizados em território estrangeiro, capazes de colocar em risco a segurança jurídica e a sua soberania do Estado, perante a comunidade internacional" (BECKER, 2018, p. 88), sendo geralmente limitada ao direito penal e às graves violações à segurança do Estado, que anteriormente não incluíam violações de proteção de dados, mas precisam se adaptar às novas modalidades de ameaças virtuais e de uso de dados em matéria de contra inteligência e espionagem, por exemplo. Nas lições do professor Adilson Pires:

> No debate sobre integração, não se pode deixar de abordar o problema da soberania, consequência natura dos processos de compatibilização das políticas estatais isoladas. O estudo do Direito Internacional Público não pode prescindir de conhecimentos sobre a origem e a evolução do conceito de soberania, ao qual está diretamente relacionado. O próprio conceito tradicional, exposto por Jean Bodin como poder absoluto e perpétuo, há que ser rediscutido, tendo em vista novas modalidades de cooperação entre os Estados. (PIRES, *in* GOMES, 2010, p. 39)

Além disso, sob o princípio da Proteção, o foco exclusivamente voltado para a proteção do Estado, também passa a proteger os indivíduos conforme a moldura jurídica das leis de proteção de dados pessoais (BECKER, 2018), quando a interpretação do princípio da proteção volta-se para o contexto das questões de segurança, de modo a assemelhar-se a uma aplicação da territorialidade objetiva (HAUNTS, 2018, p. 25 - 33), ou da doutrina dos efeitos (GEIST, 2015, p. 186 - 199).

3.2 A jurisdição territorial e a jurisdição extraterritorial na proteção de dados

A jurisdição territorial denota a assunção e o exercício de autoridade judicial sobre demandas (e demandados) que estão fisicamente além dos limites do Estado demandante, mas cujas atividades estão sendo julgadas dentro dele (TRINDADE, 2002, p. 25 - 33). "A fixação jurisdicional resultante da atividade transfronteiriça tradicionalmente exigida pela presença física" (DINAMARCO; LOPES, 2016, p. 75), foi substituída ou relativizada em decorrência da proliferação de recursos tecnológicos capazes de permitir comunicações mais ágeis, tais



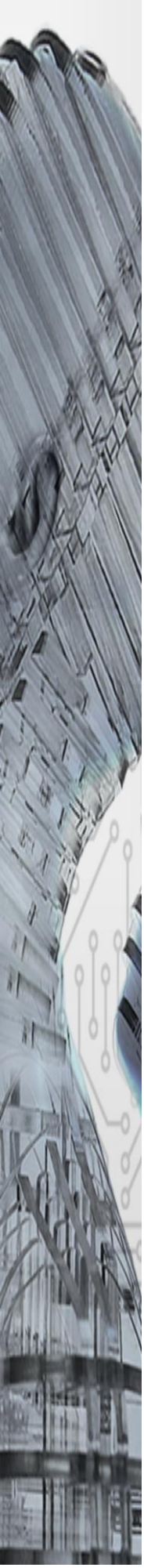
como os e-mails e os aplicativos de mensagens automáticas, as vídeo-chamadas, telefonia via satélite e digitalização de documentos e obras literárias (TEIXEIRA, 2018, p. 80 - 83).

Enquanto a Internet revolucionou os meios de comunicação e a digitalização transformou o produto e a natureza da atividade comercial, a jurisdição em proteção de dados pessoais fez surgir algumas anomalias do ponto de vista jurídico. Talvez a questão crucial seja a jurisdição em proteção de dados depender da natureza do produto, localização das partes ou o método de comunicação. Para Nadia de Araújo (2011, p. 89), "quando ambos os litigantes estão dentro do território do foro de competência onde a lei se aplica, a jurisdição dos tribunais locais dificilmente pode ser contestada". Todavia, podem existir ou devem haver diferenças para as formas como cada solicitação de usuários pode ser tratada no ponto de recebimento ou redirecionadas para o processamento de dados pessoais, à luz da privacidade.

Perante tais circunstâncias, "em transações virtuais, a jurisdição pode ser fixada em decorrência do local onde está sediado o servidor utilizado" (VOIGT; BUSSCHE, 2018, p. 43), o qual pode estar instalado fora da jurisdição onde ocorreu o fato gerador da demanda, refletindo a natureza de muitas das atividades de matriz cibernética. Todavia, a importância das legislações nacionais sobre a proteção de dados pessoais, no mercado de transações de produtos e serviços comercializados em ambiente virtual, bem como o processamento de dados pessoais armazenados por empresas em dispositivos conectados à rede mundial de computadores, indicam que "os Estados devem estar juridicamente desenvolvidos para assumir uma presumível jurisdição e proteger os cidadãos" (HAUNTS, 2018, p 35).

No mundo real, "a identidade e a localização geográfica dos participantes e as ferramentas utilizadas são facilmente rastreáveis em um território específico" (TEIXEIRA, 2018, p. 27 - 31). Todavia, o direito internacional proíbe o ato de um Estado realizar investigações e atividades de inteligência sem prévia autorização, no território de outro Estado, havendo raras permissões somente a funcionários vinculados à Administração Pública local (em oposição a indivíduos particulares) (TRINDADE, 2002, p. 94 - 102). Assim, por exemplo, um Estado não pode realizar uma investigação em outro Estado, se o objetivo for aplicar a sua própria lei administrativa, penal ou fiscal. As violações desta regra, incluindo aquelas realizadas remotamente usando a Internet, podem ensejar anátemas diplomáticos entre os Estados envolvidos, posto que ferem a soberania local (DINAMARCO; LOPES, 2016, p. 97 - 98).

Neste ponto da discussão, a análise também se desdobra por sobre a jurisdição extraterritorial, cuja ocorrência "se perfaz quando o Estado exerce a sua jurisdição sobre atos,



fatos e negócios jurídicos ocorridos fora do seu território" (MORAIS *in* GOMES, 2010, p. 172). Vários são os critérios capazes de justificar a jurisdição extraterritorial e fixar como uma demanda deverá ser resolvida, conforme expostos adiante.

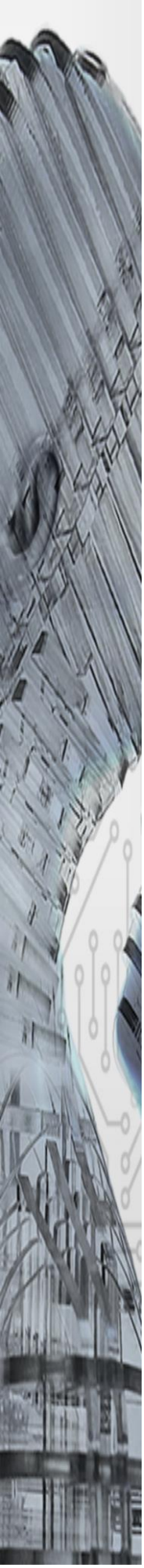
A Convenção de Bruxelas de 1968, relativa à Competência Jurisdicional e à Execução de Decisões em matéria civil e comercial (CUE, 1968), elenca três princípios básicos estabelecidos nos artigos de 1 a 5 e de 13 a 17.

Em primeiro lugar, a Convenção é restrita a "questões cíveis e comerciais"; as matérias fiscais, aduaneiras e administrativas, bem como as questões relativas à falência, à liquidação de empresas, à segurança social e à arbitragem estão excluídas (*Ibidem*).

Em segundo lugar, a jurisdição pessoal baseia-se no domicílio e na convenção das partes; que permite às empresas escolher os tribunais de um Estado-Membro para resolver qualquer litígio que possa surgir em relação a uma relação jurídica específica. Na ausência de uma escolha estipulada, o artigo 2 (CUE, 1968) favorece o demandado e prevê a competência geral, permitindo que qualquer pessoa domiciliada em um Estado-Membro seja demandada no país onde reside. Em outros casos, a Convenção também estabelece jurisdição específica, por contrato e ato ilícito (*Ibidem)*. Nos contratos, uma pessoa domiciliada num Estado-Membro pode ser demandada perante os tribunais de outro Estado-Membro, se tiver a execução da obrigação em questão determinada por referência ao desempenho da obrigação principal (ARAÚJO, 2009). No delito, a jurisdição é apropriada para os tribunais do lugar onde o evento prejudicial ocorreu, ou onde há "uma ameaça ou um risco real" de ocorrer algum dano. Conforme ensina a professora Fabíola Morais, *in verbis:*

> Há ainda dificuldade de interpretação, em certos casos, de algumas expressões previstas nas diretivas, bem como o problema da utilização, pelas diretivas, de termos abstratos, vagos, que acarretam para o legislador nacional um poder discricionário bastante amplo no ato de transposição.
> Além disso, as diretivas fragmentam os direitos nacionais dos contratos, uma vez que o legislador nacional muitas vezes prefere simplesmente transpor uma determinada diretiva para a ordem jurídica interna a enfrentar os problemas que decorrem da dificuldade de adaptar o sistema jurídico nacional à diretiva. (MORAIS, *in* GOMES, 2010, p. 173).

Em terceiro lugar, aplicam-se regras especiais nos contratos de consumo e de emprego (ARAÚJO, 2009). Contratos de consumo são contratos fora do comércio ou da profissão do contratante e consistem em instrumentos formais para a venda de bens em prestações, empréstimos reembolsáveis em parcelas ou contratos para o fornecimento de bens ou serviços, quando o contrato foi precedido por um convite específico para o consumidor ou a publicidade e o consumidor tomaram nesse Estado as medidas necessárias para celebrar o contrato (CUE, 1968).



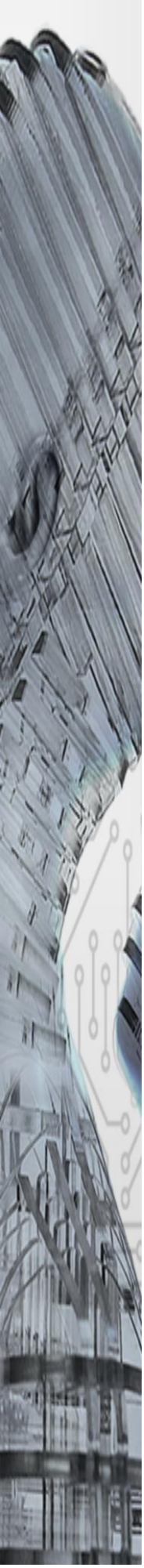
A jurisdição também pode ser evocada no desenvolvimento de uma Justiça Administrativa sadia, nos países onde o sistema judicial é misto, conforme prevê o Regulamento de Bruxelas (CUE, 1968), sobre o desenvolvimento de atividades de "*e-commerce*, cujo enfoque é atualizar e substituir o atual regime de fixação da competência territorial, pela jurisdição e execução de decisões judiciais no âmbito do Tribunal Europeu" (BECKER, 2018, p. 75), por exemplo. A revisão retém o domicílio do réu como base de jurisdição pessoal, mas oferece fundamentos jurisdicionais alternativos onde existe um "vínculo estreito" entre o tribunal e a ação ou onde a "boa administração da justiça" seria facilitada (ARAÚJO, 2009, p. 76 - 80).

No entanto, "as autoridades europeias de proteção de dados também buscaram a possibilidade de realizar auditorias de aplicação de processadores de dados em outros países" (HAUNTS, 2018, p. 29), de forma que as cláusulas do RGPD (CUE, 2016) capazes de obrigar os importadores de dados fora da UE a aceitarem auditorias a pedido dos exportadores de dados e, quando aplicável, em acordo com a autoridade de proteção de dados, bem como a submissão geral à jurisdição demandante e ao Tribunal de Justiça da UE, também foram incorporadas em dois conjuntos de cláusulas contratuais padrão para transferências de dados fora da EU, aprovadas pela Comissão Europeia, conforme aponta Becker (2018, p. 121 - 123).

Tais situações levantam questionamentos acerca de saber se a Internet deve ser governada por um sistema autônomo de leis e instituições ou se a governança do mundo real deve ser adaptada para a Internet, indo desde o estabelecimento de esquemas de autorregulação[72], como medida temporária, até a criação de "novas" leis e instituições legais que operem no ciberespaço de forma internacional.

Portanto, a questão representa uma escolha entre um sistema "novo" e o já "existente", refletindo sobre princípios tradicionais em diferentes jurisdições e explorando o aperfeiçoamento de regras comuns, quando estas já existam e sejam aplicáveis a disputas cibernéticas. Neste prisma, até que um sistema universal esteja em vigor, os reclamantes continuarão demandando mediante ingresso dos pleitos nos tribunais locais.

[72] A autorregulação poderia surgir dos operadores de sistema que publicam códigos de conduta na Internet e convidam aos comentários operadores e usuários, antes que uma norma seja adotada. Como as regras planejadas são a vontade comum de seus membros, que aderem voluntariamente, a conformidade será compatível com a atividade comercial dos membros do esquema. Os operadores dos sistemas locais conhecem o ambiente de trabalho e decretam os seus próprios termos de acesso, mas enquanto os operadores do sistema podem impor sanções ao infrator, na prática, não conseguem oferecer uma solução eficaz para o queixoso.



3.2.1. A Territorialidade sob a perspectiva da Doutrina dos Efeitos

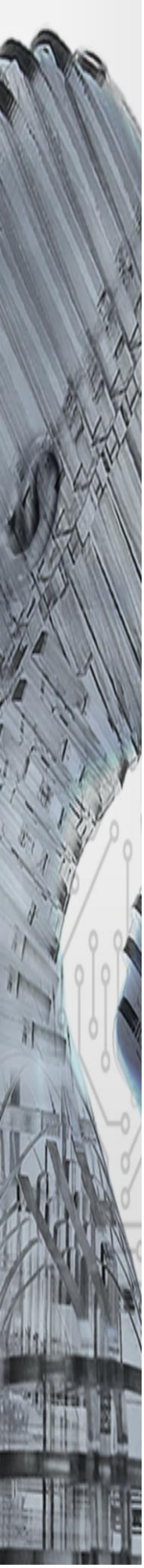
Sob o corolário de uma jurisdição universal e fluida que faça dialogar, através de seus princípios, as legislações nacionais sobre a proteção de dados pessoais e a privacidade, o direito internacional apresenta a "Doutrina de efeitos" como uma extensão do princípio da Territorialidade (TRINDADE, 2002; STRENGER, 2003; ARAÚJO, 2009; MECLEAN, 2010).

A Doutrina dos Efeitos, amplamente empregada nos Estados Unidos e em países de tradição consuetudinária, faculta aos Estados nacionais declararem competência territorial e titularidade jurisdicional para julgar atos praticados por empresas fora de seu território, desde que tais atos causem efeitos nocivos no interior de seu território (DORR; WEAVER, 2014; BANDEIRA DE MELLO, 2015).

A Doutrina dos Efeitos tem sido veementemente criticada (FEILER, 2012; BAMBERGER; MULLINGAN, 2015; GEIST, 2015); em relação à proteção de dados pessoais e a privacidade, "mas parece ter se difundido, pelo menos no que diz respeito às afirmações de jurisdição sobre conduta no ambiente virtual" (DORR; WEAVER, 2014, p. 88). As discussões partem da percepção de que a Doutrina dos Efeitos tem interpretação bastante aberta, uma vez que a economia globalizada produz contextos jurídico-econômicos sobrepostos em muitas áreas, apenas mediante a ocorrência de um fato isolado.

O segundo ponto de discussão diz respeito ao alargamento do alcance das regras jurisdicionais baseadas no efeito, refletindo-se num alargamento do hiato entre motivos razoáveis para a jurisdição e a necessidade de aplicação da lei, em um ambiente no qual estão dispostas reclamações de titulares de dados/vítimas com motivos razoáveis para o reconhecimento e a execução de sentenças estrangeiras no outro lado da questão (MCLEAN, 2010, p. 91 - 104).

Por consequência, a Doutrina dos Efeitos é uma ferramenta complementar para a compreensão e a fixação da jurisdição com base no princípio da Territorialidade. Todavia sua interpretação não pacífica pode trazer insegurança à resolução de demandas transfronteiriças e oportunizar debates diplomáticos, restando a sua aplicação a controvérsias nas quais os princípios e tratados internacionais, bem como os textos constitucionais não subsidiem entabulação jurisdicional mais cristalina e estruturada.



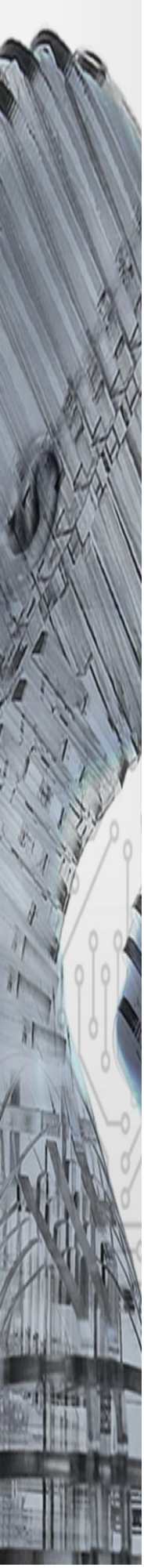
3.3. A jurisdição em dados pessoais no Direito Público e no Direito Privado

Muito embora "a distinção entre o direito público e o direito privado possa encontrar-se lastreada de forma bastante simplificada na diferença dos interesses tutelados e insculpidos em normas direcionadas para o âmbito das relações entre particulares" (MORAIS *in* GOMES, 2010, p. 174), como nas relações sobre indivíduos (pessoas físicas ou jurídicas de natureza privada) que habitem ou exercitem atividades fora de seus respectivos Estados, ou com viés administrativo do Estado em relação aos demais entes e órgãos afetos (*Ibidem*), os contornos das leis de proteção de dados pessoais dificultam a clara definição quanto a se tratarem de normas atraídas para os sistemas de Direito Internacional Público ou Direito Internacional Privado, quando da necessidade de tribunais superiores (não) aplicarem a lei pública de jurisdições estrangeiras.

Desta forma, caso a privacidade em proteção de dados pessoais seja "considerada como norma de direito público, o tribunal ou autoridade de proteção de dados, no âmbito de seu exercício jurisdicional, poderia aplicar tão somente a própria lei nacional" (BECKER, 2018, p. 188) e renegar o diálogo com a fonte normativa estrangeira, ainda que, conforme explica Nadia de Araújo (2011, p. 73), "segundo o princípio da Territorialidade, o objeto da discussão que desencadeou o ajuizamento de uma ação judicial tenha ocorrido em outro Estado".

Ademais, a classificação como questão de direito público ou de direito privado "pode ser importante para determinar se certos instrumentos jurisdicionais relevantes, como os Tratados Internacionais do quais os países envolvidos na lide possam ser signatários" (MCLEAN, 2010, p. 227), deveriam ser recepcionados no ordenamento normativo onde a jurisdição é exercida, como também se seriam capazes de promover uma solução mais adequada à contenda (TRINDADE, 2002, p. 45 - 49), por apresentar mecanismos mais eficazes do que as leis nacionais de proteção de dados dos Estados contrapostos. A respeito dos Tratados Internacionais, o professor Adilson Rodrigues Pires, explica o seguinte:

> O tratado que cria o organismo regional, em regra, tem força de indução no sentido de promover a harmonização da legislação interna, o que se costuma chamar de harmonização positiva. Noutros termos, se a legislação interna de cada país for responsável pelo delineamento da legislação dos países signatários, diz-se que a harmonização é negativa, entendendo-se esta como a supressão dos antagonismos e das distorções contidas nas leis internas dos Estados contratantes. (PIRES, *in* GOMES, 2010, p. 37)



Visando expandir o escopo e abarcar contextos privados e públicos, na perspectiva da coleta, tratamento e armazenamento de dados como sendo realizados tanto por pessoas jurídicas de direito privado, quanto por entes, órgãos e agentes públicos atuando no interesse da Administração Pública, as leis de proteção de dados não podem ser categorizadas como abrangendo totalmente a lei privada ou a lei pública, mas se apresentando de uma maneira mista, pois são derivadas de uma variedade de fontes legais, como as leis de defesa do consumidor, as leis sobre direitos humanos, a privacidade como regra constitucional, dentre outras.

Logo, "a legislação relativa à proteção de dados incluirá normalmente disposições de natureza de direito público, relativas a uma autoridade e aos seus deveres e decisões" (WALTERS; TRAKMAN; ZELLER, 2019, p. 88). Mas, "a lei também incluirá provisões de lei civil, normalmente sobre responsabilidade por violações de proteção de dados" (*Ibidem*). Assim sendo, torna-se mais confortável modular a natureza da lei de proteção de dados não apenas de direito público ou de direito privado, mas de forma conexa à atividade ou ao objeto da demanda. Desta forma, caso uma decisão seja tomada por uma autoridade de proteção de dados (por exemplo, uma ação de execução ou uma auditoria), tal ato pode ser considerado como uma questão de direito público.

Todavia, caso uma ação seja tomada por um ator privado (como a assinatura de um acordo de transferência de dados com outra parte privada), então deve ser considerado um ato de direito privado, embora com um forte elemento regulador (MCLEAN, 2010, p. 66). Conforme explica Irineu Strenger (2003, p. 51), haverá "muitas situações em que a natureza pública e privada da lei de proteção de dados se entrelaça, podendo requerer análise minuciosa a fim de fixar os critérios de distinção empregados em cada caso particular".

As disposições da legislação em matéria de proteção de dados podem, por conseguinte, ser qualificadas como pertencentes a diferentes áreas do direito, às quais são atribuídos diferentes critérios de conexão relevantes. Seguindo o método tradicional, "diferentes aspectos de um caso podem então ter de ser decididos por diferentes normas de direito interno, externo e internacional, o que pode facilmente levar a distorções das decisões" (PIRES *in* GOMES, 2010, p. 38) e a uma elevada temeridade fundada na insegurança jurídica e na livre escolha do Estado-juiz para fundamentar uma decisão que não pode ser antevista apenas com base na linearidade legal específica da matéria (DINAMARCO; LOPES, 2016, p. 102 - 113), uma vez que "a legislação é concebida como um todo orgânico, em que as

diferentes disposições apoiam uma solução adequada" (BANDEIRA DE MELLO, 2015, p. 229).

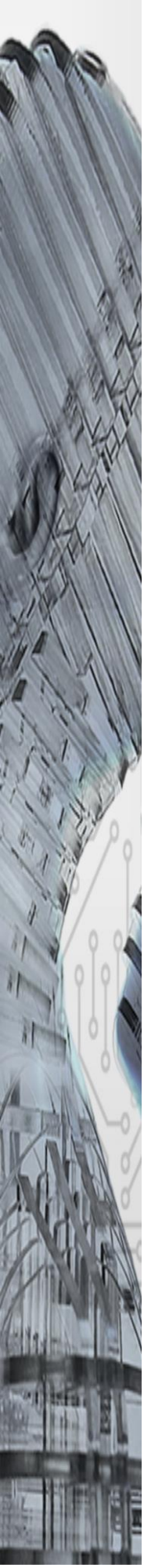
Assim sendo, não parece profícuo ao processo, à jurisdição e à tutela jurisdicional, a fixação de critérios capazes de determinar se a lei de proteção de dados e os direitos das partes, especialmente em uma disputa internacional, devam ser discriminados com referência aos controversos mistérios da distinção entre direito privado e direito público. Outrossim, sobrevêm relevantes motivos para "promover a análise de uma ampla senda de ramificações do Direito, ao se tratar das bases jurisdicionais para a lei de proteção de dados" (BLUM, 2018, p. 34), "incluindo a consideração de princípios que tradicionalmente estariam classificados como pertencentes a diferentes áreas de direito público e privado" (BIONI, 208, p. 227).

Logo, parece preferível analisar os vários princípios jurisdicionais baseados no grau de contato que eles exigem entre as partes e a jurisprudência do tribunal julgador, ao invés de ser realizada a mera exclusão de tópicos da discussão, no caso concreto, apenas por tradicionalmente se tratar de matéria analisada no contexto de exclusão recíproca de uma área particular do direito em face de outra preterida.

3.3.1 Regras Jurisdicionais da proteção de dados no Direito Internacional

A "Jurisdição" no plano do direito internacional público pode ser definida como "o direito do Estado no direito internacional de regular a conduta em assuntos não exclusivamente internos" (ARAÚJO, 2011, p. 144), e assume características contrastantes com a "escolha da lei" ou a "legislação aplicável", as quais podem ser consignadas para melhor definir qual lei ou leis devem ser aplicadas em um determinado caso (STRENGER, 2003, p. 82 - 99). Para McLean:

> No contexto dos procedimentos cíveis, a cooperação internacional está primariamente preocupada com o serviço de documentos, "processo" de um tipo ou outro, mas também documentos extrajudiciais significativos e a obtenção de provas. A assistência pós-julgamento, sob a forma de execução das sentenças e ordens, é tradicionalmente tratada como um tema (principal) de direito próprio.
> Como ficará mais claro, cada estado pode ter seus próprios mecanismos, permitindo que seus tribunais autorizem o serviço do processo ou a obtenção de provas fora de sua jurisdição territorial; pode haver também medidas de coerção disponíveis contra pessoas dentro da jurisdição que permitam efetivamente que o tribunal obtenha provas ou informações, mesmo que as principais fontes de informação estejam no exterior. Mais tipicamente, no entanto, o envolvimento ativo das autoridades do estado estrangeiro relevante será necessário (especialmente se as atitudes dessas



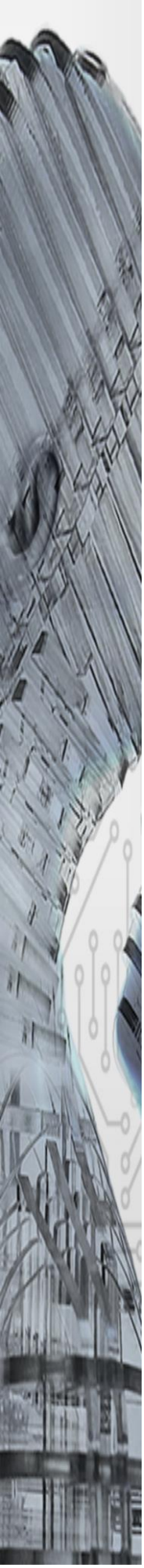
> autoridades derivarem da tradição do direito civil) ou, pelo menos, desejável. (MCLEAN, 2010, p. 4, *tradução nossa*[73])

No contexto das leis de proteção de dados, "a escolha das regras sobre a jurisdição aplicável se baseia também nos princípios de privacidade, cujas origens estão nos direitos humanos" (BECKER, 2018, p. 102). Muito embora a sobreposição de legislações na moldura jurídica de cada Estado possa causar confusão a respeito da escolha da lei que melhor se amolda a cada caso, "é importante aos legisladores, aos tribunais e às autoridades de proteção de dados mensurarem os possíveis impactos advindos da falta de normas e regras" (HAUNTS, 2018, p. 26 - 27) capazes de garantir que os dados pessoais não sejam privados da proteção de sua legislação nacional, na hipótese de transferência internacional (BIONI, 2018, p. 77 - 83).

Em um microambiente de demandas envolvendo dados pessoais, as ações judiciais cujas execuções das sentenças normalmente não possam ser tomadas contra a entidade que processa os dados, quando estes forem transferidos para um país estrangeiro, poderão rever a jurisdição à luz das regras fixadas pela autoridade de proteção de dados (como agência independente ou órgão subordinado à Administração Federal) (PINHEIRO, 2018, p. 44 - 49), a qual pode ter (e necessita) o condão de estabelecer que o processamento no exterior deva ser conduzido sob a lei nacional que balizou o momento da coleta e armazenamento de dados, mesmo que haja pouca ou nenhuma chance da lei ser aplicada.

Nesta perspectiva, a aplicação da lei nacional para o processamento de dados transferidos para o exterior permite a afirmação da competência regulatória da autoridade nacional de proteção de dados, sem que seja possível ao sujeito processado a escolha de lei nacional ou estrangeira mais benéfica, mas visando a proteção do titular dos dados com base na sua legislação nacional como critério para a fixação da jurisdição (HAUNTS, 2018; MCLEAN, 2010; TEIXEIRA, 2018). Assim sendo, torna-se possível às autoridades nacionais de proteção de dados aplicarem sua legislação local ao processamento de dados no exterior ou reivindicarem a jurisdição nacional sobre tais processamentos, geralmente sem realizar a distinção corrente entre as duas situações, mas apenas utilizando os princípios comuns do

[73] Do original na língua inglesa: "*In the context of civil preceedings, international co-operation is primarily concerned with the service of documents, "process" of one sort or another but also extrajudicial documents of significance, and the taking of evidence. Post-trial assistance, in the form of the enforcement of the judgements and orders, is tradicionally treated as a (major) topic in itz own right.*
As will become clearer, each state may have its own mechanisms enabling its courts to authorize the service of process or the taking of evidence outside its territorial jurisdiction; there may also be measures of compulsion avaiable against persons within the jurisdiction wich enable the court effectively to secure evidence or information even though the primary sources of informatin are abroad. More tipically, however, the active involvement of the authorities of the relevant foreign state will be required (especially if the attitudes of those authorities derive from the civil law tradition) or at least desirable"(MCLEAN, 2010, p. 4).



Direito Internacional que atraem a competência de análise judicial para a jurisdição do território onde ocorreu a coleta dos dados pessoais.

A delimitação quanto ao alcance da lei e a utilização de nomenclaturas jurídico-econômicas, tais como "coleta", "armazenagem", "privacidade", "proteção", "dados pessoais" e "tratamento", possuem ampla interpretação objetiva, axiológica e deontológica, demonstrando como a lei de proteção de dados detém o condão de abarcar amplamente as variáveis interpretativas quanto ao processamento de dados pessoais, além de também aumentar a chance de conflitos jurisdicionais, "pois representam um conjunto de direitos violados diariamente" (BIONI, 2018, p. 32) e tutelados pela legalidade das regras de jurisdição internacional dada a natureza global da Internet, de modo a impulsionar formas de interpretação da jurisdição doméstica em harmonia com as normas de Estados estrangeiros e de Direito Internacional, embasadas também pelos princípios dos Direitos Humanos.

Deste modo, o Direito Internacional, segundo as formas de exercício da jurisdição, pode ser subdividido em: (I) Jurisdição Prescritiva; (II) Jurisdição Judicativa e; (III) Jurisdição Executiva, as quais são explicadas por Ramalho nos seguintes termos:

> Ora, a jurisdição, noção também polissémica por natureza, tende a ser dividida na literatura anglo-saxónica nas vertentes prescritiva, judicativa e executiva. Grosso modo, a primeira refere-se ao poder de determinar ordens jurídicas ou autorizações vinculativas perante os indivíduos do Estado respectivo, *maxime* determinando condutas criminalmente relevantes e determinando o âmbito de aplicação das normas; a segunda refere-se ao poder de definir juridicamente situações concretas através de decisões que aplicam e interpretam vinculativamente as normas aplicáveis; e, por fim, a jurisdição executiva traduz-se no poder de assegurar, com recurso a meios coercivos, que as normas e imposições jurídicas são cumpridas ou para punir o seu incumprimento. (RAMALHO, 2017, p. 36).

No contexto das leis de proteção de dados, a Jurisdição Prescritiva pode ser concorrente e não exclusiva[74].

A Jurisdição Judicativa, indicando "o poder dos tribunais de um Estado para julgar casos envolvendo um elemento estrangeiro, pode representar não só o alcance territorial e extraterritorial da lei de proteção de dados" (MCLEAN, 2010, p. 157), como também os critérios de acolhimento das demandas levadas à análise do Estado-juiz ou da autoridade de proteção de dados. Deste modo, caso a lei de proteção de dados em análise permita a

[74] *E.g.:* a aplicação da lei de proteção de dados da UE a um site com sede nos Estados Unidos da América, mas que utiliza *cookies* para processar dados pessoais de indivíduos localizados na UE (HAUNTS, 2018, p. 33).

definição do objeto da discussão como proveniente do "direito público", a jurisdição adjudicativa será equivalente à jurisdição legislativa[75].

A Jurisdição Executiva na lei de proteção de dados pessoais, por sua vez, retrata o "poder de um Estado para realizar atos no território de outro Estado, desde que haja previsão legal para tal e sobrevenha acordo de cooperação mútua entre os Estados envolvidos no caso em discussão" (RAMALHO, 2017, p. 88), estando a legalidade da jurisdição correlacionada à jurisdição prescritiva e à jurisdição judicante, quanto ao alcance, limitações e alcances concomitantes de cada uma das formas citadas (MCLEAN, 2010, p. 98)[76].

O reconhecimento no âmbito do direito internacional público de que um Estado não pode aplicar diretamente sua lei além de suas fronteiras, mas aplicá-la a condutas que transcendem suas fronteiras é amplamente permissível, desde que haja bases legais reconhecidas para isso (ARAÚJO, 2011, p. 132 - 134), ilustrando a "existência de limitações na jurisdição de execução, as quais se tornaram universalmente aceitas" (DINAMARCO; LOPES, 2016, p. 80).

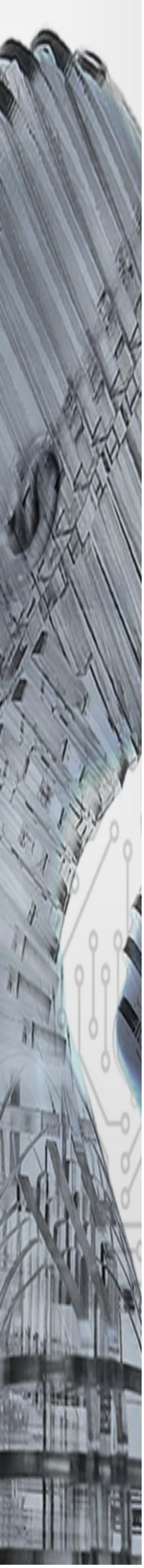
De início, os princípios fundamentais da soberania e da não interferência do Estado parecem requerer tais limitações. No entanto, ainda não existe nenhum instrumento sob a lei internacional pública de aplicação global (e não apenas regional) contendo regras jurisdicionais para as leis de proteção de dados.

3.4 Adequações do modelo clássico da jurisdição ao panorama de dados pessoais

Quando a abrangência jurisdicional de uma lei é muito ampla, sobrevém o risco de diminuição da observância e do respeito à norma, diminuindo a sua aplicabilidade e, por conseguinte a sua eficácia no ordenamento jurídico (BANDEIRA DE MELLO, 2015, p. 183 - 185). De forma semelhante, as lacunas entre o cumprimento e a aplicação das leis de proteção de dados podem se tornar consideravelmente grandes, tendo em vista a dificuldade de monitorar todos os milhões ou bilhões de ocorrências em tratamentos de dados. Logo, o alcance jurisdicional das leis de proteção de dados também pode atuar de modo didático, nas

[75] Um exemplo dado é aquele de uma autoridade europeia em matéria de proteção de dados, que decidisse uma queixa apresentada por um indivíduo localizado na EU, com base no tratamento dos seus dados pessoais por uma entidade situada fora da EU (VOIGT; BUSSCHE, 2018).

[76] Esta modalidade de exercício jurisdicional pode ser ilustrada pela realização de uma auditoria por uma autoridade europeia em matéria de proteção de dados na sede de uma entidade (pública ou privada) situada em país não integrante da UE (HAUNTS, 2018, p. 23).



sendas da política, da legislação, da administração pública e da conscientização da população a respeito de seus direitos e deveres.

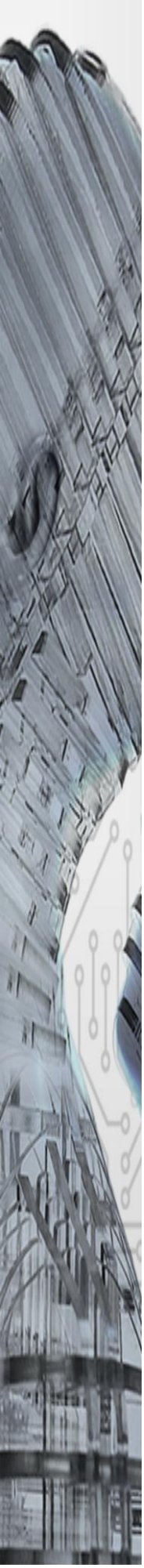
A superação regulatória, onde as regras são expressas de forma geral e não discriminatória, "permite aplicações diversificadas, de modo que a delimitação da jurisdição em casos de adjudicação e disputas em tribunais ou em sede administrativa, através das autoridades reguladoras nacionais, não representam possibilidades puramente teóricas" (ARAÚJO, 2011, p. 122 - 129) devendo, para tanto, contar com uma moldura normativa capaz de assegurar o Estado Constitucional e a execução das decisões judiciais e administrativas de forma clara, em um enquadramento jurídico mais hermético (BANDEIRA DE MELLO, 2015, p. 145 - 158).

As incertezas jurisdicionais sobre a proteção de dados pessoais tratados no ambiente virtual têm lastro em possíveis situações, tais como: (I) os conflitos envolvendo afirmações unilaterais de jurisdição dos Estados na Internet, tal como ocorre em outras áreas do Direito; (II) o manuseio de tecnologias (como programas de transferência de IP e a geolocalização) permitindo que entidades reclamem amparo jurisdicional, com base na exposição legal à territorialidade escolhida (III) a escolha de fixação da sede de empresas em Estados nos quais as jurisdições não são capazes de produzir medidas de execução, ou contra pessoas físicas ou jurídicas e bens do réu dentro do Estado; e (IV) a lacuna sobre a conscientização a respeito das formas de fixação da jurisdição em atividades realizadas no ambiente virtual.

O amplo escopo jurisdicional das leis de proteção de dados também esbarra em questões *interna corporis* advindas da governança corporativa e de *compliance*, seja na instituição de regimentos internos e a fiscalização, seja na aplicação de sanções em casos de violação a tais regras privadas e à legislação.

Sob a perspectiva da abordagem clássica (MCLEAN, 2010; TRINDADE, 2002; STRENGER, 2003) para avaliar a propriedade de uma base jurisdicional, "é possível utilizar o domínio do sítio eletrônico para determinar o local da conexão" (BIONI, 2018, p. 53), sob a égide da territorialidade, podendo tal relação ser justificada mediante a definição da "sede de uma relação legal", do "centro de gravidade" ou a "conexão mais próxima". Por este ponto de vista, a jurisdição pode ser fixada de maneira concorrente, tornando-se preventa a autoridade judiciária que primeiro conheceu a demanda[77], em decorrência da competência originária (DINAMARCO; LOPES, 2016, p. 105).

[77] Por exemplo o local de estabelecimento do controlador de dados, quando a empresa A é estabelecida no Estado X e oferece serviços pela Internet que processam dados pessoais. A maioria de seus clientes e ativos também está localizada no Estado X.



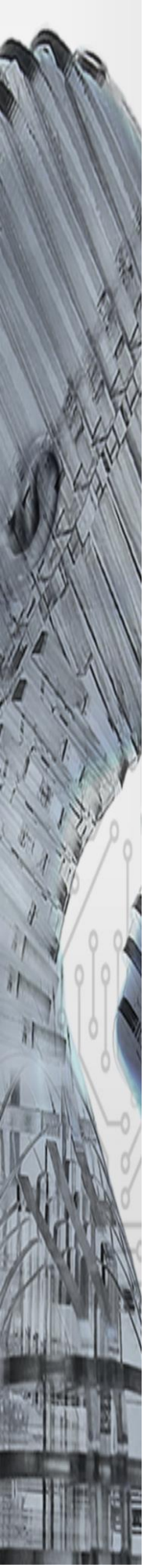
Outro ponto de inflexão por sobre a necessidade de "armazenamento em locais físicos de dados pessoais processados na Internet é a dificuldade para determinar o local de tratamento" (HAUNTS, 2018, p. 28), considerando cenários como a computação em nuvem, onde processamento de dados pessoais e metadados podem ocorrer em vários Estados simultaneamente.

Assim, a questão é se, na era da computação em nuvem, faz sentido falar que os dados estão "localizados" em um lugar específico, mesmo considerando a utilização dos processadores físicos em *data centers*. Nesta perspectiva, pode ser mais adequado selecionar a jurisdição com base na residência do titular de dados ou o local onde o ato ilícito produziu os efeitos finais, a fim de dar a máxima proteção ao indivíduo.

Também pode ser possível, para facilitar a declaração da jurisdição competente, em casos de conflitos entre Estados, a "criação de um Tratado Internacional definindo a continuidade da aplicação das leis endêmicas do Estado onde o contrato foi firmado" (MORAIS *in* GOMES, 2010, p. 172) e os dados consequentemente coletados, de modo que o titular conheça a própria legislação nacional e a lei do território de transferência passe a conviver com o fator limitador de se adequar aos paradigmas normativos da relação matriz (ARAÚJO, 2009, p. 133 - 140).

Em alguns casos isso pode ser sustentado por acordos entre as partes na transferência de dados, tal como os modelos de contratos da UE (VOIGT; BUSSCHE, 2018), que exigem que a parte no país de importação de dados continue aplicando a lei do país de exportação de dados ao processamento, exigindo que essa parte se submeta à jurisdição das autoridades reguladoras do país de exportação.

Tais afirmações de jurisdição "são tentativas compreensíveis de proteger os dados pessoais de cidadãos e residentes, não importando onde no mundo eles são processados" (BECKER, 2018, p. 155). Todavia, os Tratados Internacionais e as legislações nacionais encontram dificuldade de aplicação e eficácia no ordenamento jurídico interno, pois segundo o professor Adilson Pires:



> Apesar de considerado norma primária pelo direito internacional, não se pode afirmar que o tratado tenha o condão de desencadear modificações na legislação interna dos países que integram um organismo internacional. Em contrapartida também não se pode dizer que a legislação interna dos Estados contratantes é capaz de induzir os negociadores do acordo a fazerem convergir para a lei maior do organismo o conjunto de leis internas de cada país.
> Em resumo, nem a legislação interna nem o tratado internacional têm força suficiente para promover as modificações necessárias à boa e harmônica convivência doméstica internacional. Ocorre, em verdade, uma tensão contínua entre ambos, o que se faz com que permanentemente um, o ordenamento interno, e outro, o tratado, convirjam para a conciliação. (PIRES, *in* GOMES, 2010, p. 38)

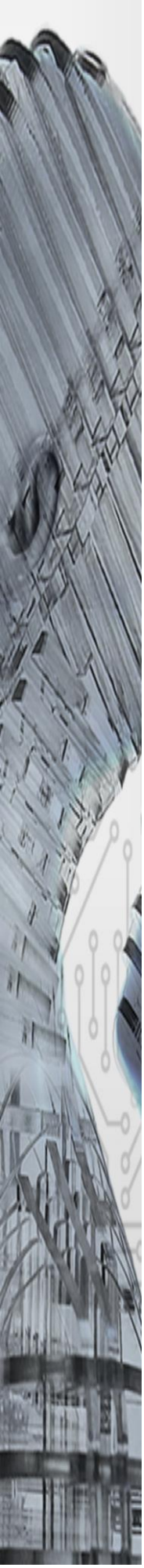
As múltiplas adaptações às legislações regionais ou nacionais decorridas de Tratados Internacionais são abrangentes e objetivam se adequar a todas as possíveis situações jurisdicionais. Também é provável que seja inútil supor que cada base jurídica para a proteção de dados poderia ser exclusiva, havendo sempre um local de jurisdição para a exclusão de todos os outros. Assim sendo, uma das alternativas seria encontrar um método para permitir que tais afirmações jurisdicionais múltiplas coexistam, encontrando uma maneira inovadora de medir e fixar a sua legalidade no plano internacional.

3.4.1 O juízo de admissibilidade na jurisdição sobre dados pessoais

O juízo de admissibilidade na jurisdição sobre dados pessoais inicia-se quando a parte autora submete à apreciação do Estado-juiz ou da autoridade administrativa com competência para julgar, uma reivindicação sobre um direito amparado por legislação nacional ou internacional (DINAMARCO; LOPES, 2016, p. 179).

Deste modo, importa que a autoridade julgadora interprete antecipadamente os impactos adjuntos à recepção ou ao não acolhimento do pleito, sopesando as características individuais tanto da parte autora, quanto da parte ré, “visando o equilíbrio da disputa e todas as garantias processuais e éticas à defesa, principalmente quando a parte ré se localizar em país estrangeiro”. (ARAÚJO, 2011, p. 55)

Assim sendo, a realização de qualquer tratamento de dados pessoais fora da jurisdição pode ser permitida, preferencialmente “mediante a previsão contratual que preveja a escolha de uma eventual forma alternativa de solução de conflitos (mediação, conciliação ou arbitragem), a adoção de lei específica ou a determinação do foro de jurisdição competente”



(MORAIS *in* GOMES, 2010, p. 77) para dirimir quaisquer conflitos, em comum acordo entre as partes contratantes e o *pacta sunt servanda*[78] a reger as relações privadas.

Embora as regras possam permitir o serviço fora da jurisdição, o reclamante eventualmente precisará "demonstrar a relevância da questão a ser julgada e deixar claro o fundamento legal capaz de definir determinado tribunal ou autoridade administrativa como apropriado(a)[79] para conhecer e julgar seu pleito" (MCLEAN, 2010, p. 189). Ao decidir se a ação tem a conexão mais real e substancial, o tribunal ou a autoridade administrativa também poderá considerar fatores como: (I) a nacionalidade e a residência das partes e das testemunhas e onde elas estão localizadas; (II) as cláusulas contratuais facultativas e impeditivas da absorção jurisdicional; (III) a natureza e o valor do litígio, incluindo eventuais dificuldades jurídicas ou práticas.

Outros fatores a serem considerados versam quanto à submissão do réu à jurisdição: (I) a conduta do réu e sua conexão com o Estado do foro; (II) a inconveniência de defender um processo naquele foro; (III) o interesse do Estado do foro em julgar a disputa; (IV) o interesse do requerente em obter alívio adequado e efetivo; (V) o interesse do sistema judiciário interestadual (ou internacional) na resolução eficiente de conflitos transfronteiriços e; (VI) o interesse compartilhado dos Estados em promover políticas sociais substantivas.

A jurisdição sobre dados pessoais, uma vez baseada na cidadania, consentimento ou presença do réu, também pode se basear em duas investigações. Em primeiro lugar, "a jurisdição pessoal conferida pelo Estado do foro" (STRENGER, 2003, p. 157) e, em segundo lugar, "caso tal jurisdição exista, se o seu exercício seria consistente com as limitações do devido processo constitucional" (CANOTILHO, 2002, p. 224).

Além disso, quando o réu não é nacional, as políticas processuais e substantivas de outros estados, bem como as relações externas do Estado onde o processo judicial ou administrativo é instaurado, podem ser levadas em consideração antes de assumir a jurisdição, de modo a reconhecer uma escala de atividade que consiste em três categorias: sítios eletrônicos interativos, passivos e intermediários (FARIA; SILVEIRA; MONTEIRO, 2018).

Em um extremo do espectro, um sítio eletrônico passivo meramente fornecendo informações poderia ser equiparado a um anúncio e possivelmente não justificaria o exercício da jurisdição em dados pessoais (HAUNTS, 2018, p. 28 - 33). No outro extremo da escala, os sites comerciais que celebram contratos e captação de dados em ambiente virtual,

[78] A expressão *Pacta sunt servanda* é um brocardo jurídico de matriz latina cuja sentido expressa a máxima de que "acordos devem ser mantidos", refletindo a força de manutenção e cumprimento das cláusulas previstas em pactos, acordos, convenções, contratos e demais instrumentos onde duas partes, ou mais, ajustem termos entre si.
[79] Apropriado(a), neste sentido, pode ser compreendido como suficientemente (jurisdicionalmente) competente.

possivelmente submeteriam o titular de dados à jurisdição do Estado do foro (*Ibidem*), onde a empresa ou o organismo da Administração Pública está fisicamente sediado.

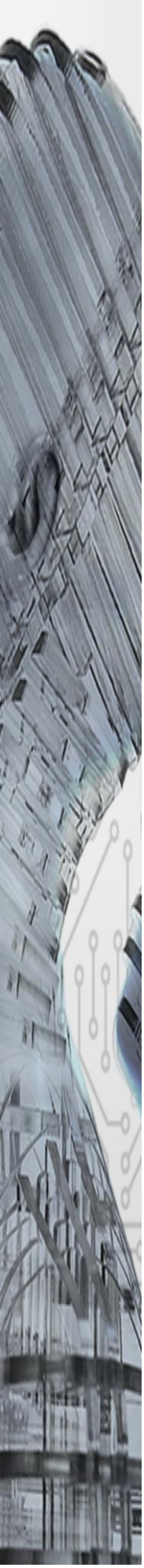
A incerteza está no meio termo, onde a interação entre o *site* e o usuário fica aquém de um contrato real, mas um usuário pode trocar informações com o computador ou uma inteligência artificial, contribuindo para que o exercício da jurisdição dependa do nível de atividades realizadas (quantidade) e da natureza comercial das trocas de informações ocorridas no sítio eletrônico em análise, conforme o caso concreto (*Ibidem*).

No entanto, a carga que recai sobre o réu, em busca de "contestar a competência do foro eleito para exercer a jurisdição não é apenas demonstrá-lo como não adequado segundo o princípio da territorialidade, mas para estabelecer que existe outro foro disponível" (ARAÚJO, 2011, p. 142) que é clara ou distintamente mais apropriado do que o foro acionado inicialmente. Neste prisma, a discrição judicial deve ser exercida à luz da cortesia internacional que exige que o tribunal tenha um interesse ou conexão suficiente com o assunto em questão. A hipossuficiência da parte afetada (vítima), no caso concreto, também deve ser analisada, pois há possibilidade de que incidentes e ilícitos ocorram também nas relações entre Administração Pública e empresas ou entre duas ou mais empresas, quando uma destas realização captação e tratamento de dados e outra somente armazena os mesmos, configurando variáveis onde é provável haver disparidade financeira e, inclusive, de capacidade postulatória de advogados, quando do desenrolar processual.

3.4.2 A Jurisdição Exorbitante

Os princípios do direito internacional privado determinam a questão da jurisdição enfatizando a "multiplicidade de ligações entre as partes, o objeto da ação e o local do acontecimento da ação em discussão ou o Estado do foro" (STRENGER, 2003, p. 55). A jurisdição exorbitante, na prática, pode ser estabelecida com base na localização geográfica dos tribunais que a exercem e nas previsões em convenções internacionais (MCLEAN, 2010, p. 180).

A aplicação principal da jurisdição exorbitante em relação à Internet, tem sido minimizar as consequências negativas da execução de sentenças, quando estas produzem resultados em outros Estados, de modo que os tribunais possam ocasionalmente atrair para a sua jurisdição a maior parte possível das obrigações fixadas na decisão, visando garantir segurança jurídica e proximidade com os atos executórios (ARAÚJO, 2009; MCLEAN,



2010), "além de evitar danos e anátemas diplomáticos, políticos e econômicos no ordenamento jurídico de outro Estado" (VENOSA, 2016, p. 92).

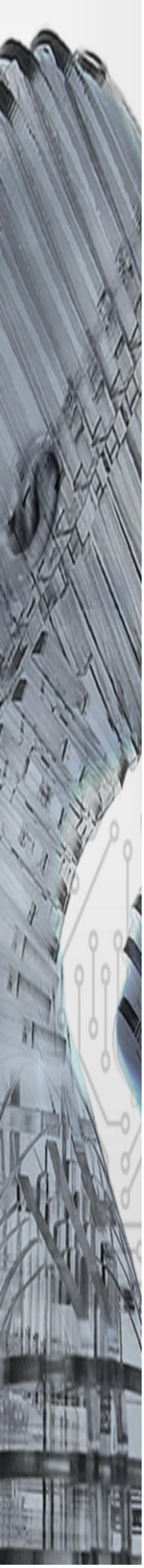
Ao assumir a jurisdição, o julgador pode desconsiderar o meio da Internet como essencialmente irrelevante e rejeitar pontos de uma eventual contestação jurisdicional, "avaliando os atos reclamados fisicamente ocorridos em sua jurisdição, embora esteja ciente das possibilidades de impactos ocorridos em locais diversos" (WALTERS; TRAKMAN; ZELLER, 2019, p. 135).

As ocorrências de jurisdição consideradas impróprias ou excessivas podem ser percebidas em "situações nas quais a jurisdição extraterritorial é exercida em tentativas de regular e solver disputas judiciais transnacionais por meio de legislação nacional, adjudicação ou execução, fixando obrigações a pessoas" (MCLEAN, 2010, p. 181), sobre bens ou atos além de suas fronteiras que produzem efeitos em outro Estado, somente quando não houver dispositivo de direito internacional prevendo tal possibilidade entre ambos os países (DINAMARCO; LOPES, 2016, p. 214 - 218).

A jurisdição exorbitante pode afetar somente a réus não residentes no país onde a demanda judicial é instaurada; não sobrevindo nenhum problema quando o réu é residente dentro da jurisdição, mesmo se a atividade reclamada tiver seu efeito fora do estado do foro (RAMALHO, 2017, p. 57 - 63). Ademais, o direito privado permite que contratos celebrados por empresas reduzam as possibilidades de problemas nas relações comerciais e de prestação de serviços transfronteiriços envolvendo dados pessoais[80], como um ato de responsabilidade que supera a essência contratual e se aproxima dos Direitos Humanos, ao visar a proteção da relação e a sua durabilidade em um cenário de integridade e respeito mútuo.

A jurisdição exorbitante no contexto das leis de proteção de dados pessoais traz alguns pontos de reflexão, sendo eles: (I) a competência jurisdicional de um tribunal tanto para julgar questões de privacidade e proteção a dados, quanto para exarar decisões a serem cumpridas via carta rogatória, em jurisdição estrangeira; (II) no caso de ser competente o tribunal, qual seria a legislação aplicável mais justa para a resolução da disputa e; (III) constituída a sentença, qual tribunal (nacional ou estrangeiro) poderá executá-la?

[80] Além disso, o desempenho no exterior de funções ligadas ao Poder Executivo (como auditorias) por autoridades de proteção de dados, também não encontra grande respaldo à luz do direito internacional e das condutas de boas práticas mercadológicas, principalmente à luz da incorporação de cláusulas em contratos-modelo adesivos, não apenas excedendo os limites do que é considerado consentimento válido (MORAIS in GOMES, 2010), mas também ignorando o fato de que o consentimento exigido não é da entidade que processa os dados, mas do Estado sob cuja jurisdição se encontra.



Apesar das relações econômicas e comerciais internacionais considerarem um mercado comum globalizado, o desenvolvimento de regras internacionais costuma ser mais lento (TEIXEIRA, 2018, p. 310 - 318), em comparação com a formulação de dispositivos estatutários de direito interno, em contraste com as regras que regem os litígios internacionais, decretadas somente quando estiverem de acordo com os adendos da regulamentação interna conexa[81](ARAÚJO, 2009, 187 - 190). No mesmo contexto, a ausência de regras universais é mais simples de entender; pois as preocupações tradicionais sobre a soberania levaram os Estados a restringirem suas leis e jurisdição aos seus respectivos territórios.

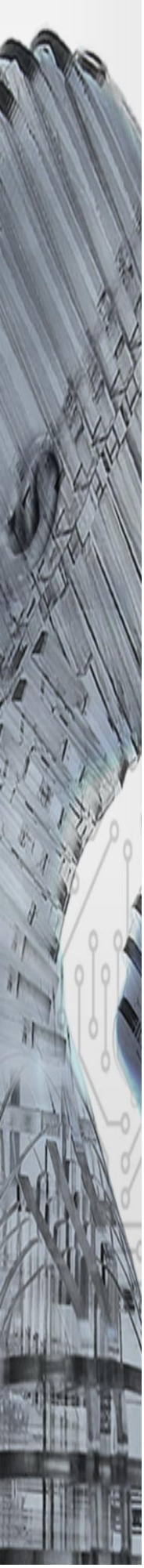
Fundamentos jurisdicionais como a localização do controlador de dados, o local do demandado e do demandante e o local onde um *e-mail* publicitário é recebido, são baseados em fatores como territorialidade, proteção e outros princípios e direitos amplamente aceitos (STRENGER, 2003, p. 78 - 85).

Outros fundamentos de jurisdição parecem mais questionáveis, em relação a uma oportunidade ensejada pela aplicação da lógica jurídica, a qual torna possível imaginar que os Estados lidem mais facilmente com o processamento de dados pessoais de seus residentes, do que pessoas de outras regiões, ainda que mediante o cumprimento de certos requisitos e padrões similares em outras leis (RAMALHO, 2017; BLUM, 2018); mas em relação próxima à função protetora da Administração Pública, bem estabelecida em várias formas jurisdicionais, tal como na doutrina dos efeitos e no princípio da personalidade.

Entretanto, a jurisdição protetora não dispensa a exigência de conexão substancial entre o foro e as partes e/ou a controvérsia, tampouco o critério de "uso de equipamentos" traduz a clareza e a segurança jurídicas suficientemente capazes de fundir um elo de jurisdição, de forma a persistirem os critérios de fixação acostados a opções complementares, mais explicitamente ligados à salvaguarda dos direitos de proteção de dados pessoais, tal como a territorialidade onde se realizou qualquer ato de cessão de dados, por via expressa ou mediante a mera requisição.

3.4.3 Desdobramentos da jurisdição transfronteiriça ou jurisdição *cross-border*

[81] Por exemplo, ao abrigo do Regulamento de Bruxelas, alguns fundamentos de competência reconhecidos como exorbitantes são excluídos em processos contra demandados domiciliados num Estado-Membro da UE. O Protocolo Complementar à Convenção de Haia sobre o Reconhecimento e Execução de Decisões Estrangeiras em Matéria Civil e Comercial também exclui do reconhecimento de sentenças estrangeiras com base em vários fundamentos jurisdicionais. O anteprojeto de convenção relativa à competência e decisões estrangeiras em matéria civil e comercial, elaborado pela Conferência da Haia de Direito Internacional Privado, que nunca foi promulgada, continha um catálogo de fundamentos de jurisdição proibidos.



As transferências internacionais de dados têm sido reguladas pelas leis de proteção de dados, cujas semelhanças entre si têm como escopo o estabelecimento de um padrão ou nível de segurança adequado à realização de atividades jurídicas, financeiras e comerciais no ciberespaço (GREENLEAF, 2014; GEIST, 2015; MAGRANI, 2017; DUGGAL, 2018; KAZEMI, 2018). Os "fluxos de dados transfronteiriços referem-se ao movimento ou transferência de informações entre servidores através das fronteiras do país" (HAUNTS, 2018, p. 34). Os dados precisam ser capazes de circular livremente, de modo que, não importa onde o tratamento ocorra, o titular de dados e o agente responsável terão acesso às informações e aos serviços (BIONI, 2018, p. 178 - 179).

Segundo Nick Bostrom (2014, p. 64), "todos, de indivíduos a grandes corporações, dependem da transferência de dados", de forma que este vínculo impacta também a todas as organizações envolvidas em transferências de dados transfronteiriços[82]. Portanto, algumas medidas de minimização de risco podem ser apropriadas, tal como a possibilidade de o provedor de conteúdo restringir o acesso a determinada jurisdição ou, no mínimo, tornar óbvio que o conteúdo exibido não se encontra amparado por uma determinada jurisdição ou legislação similar à do local de acesso[83].

Esta situação cria uma incerteza jurídica significativa e a arquitetura legal internacional pode dificultar a cooperação necessária para combater ilicitudes, considerando a falta de mecanismos claros para o acesso transfronteiriço a provas eletrônicas, como incentivo à introdução de requisitos obrigatórios de localização de dados (STAPLETON, 2014, p. 182 - 189).

Além de questões técnicas de viabilidade significativas, a generalização dessa abordagem pode representar grandes barreiras para os atores econômicos menores, e pôr em perigo a natureza transfronteiriça da Internet, "sendo que, neste ambiente virtual, as relações de consumo tomam uma proporção ainda maior, tanto em volume de negócios como em problemas jurídicos" (TEIXEIRA, 2018, p. 312).

Dentro de cada país, as modalidades de investigações previstas em lei e o acesso a evidências eletrônicas são regulados de acordo com procedimentos nacionais rigorosos, mas

[82] Por exemplo, as organizações que utilizam serviços de TI em linha, armazenamentos e processamentos realizados em nuvens e bancos de dados sediados em país estrangeiro ou serviços de acesso, dentre outros, muitas vezes precisam implementar mecanismos legais de transferência de dados (HAUNTS, 2018, p. 38).

[83] Quando o conteúdo é direcionado a um determinado território, os provedores devem se esforçar para estarem melhor ajustados tanto à jurisdição quanto às leis aplicáveis à relação e preferencialmente com antecedência a qualquer discussão judicial, uma vez que a disputa tenha surgido (BOFF; FORTES; FREITAS, 2018). Desta forma, os provedores de internet e as empresas que realizam o tratamento de dados pessoais, podem evitar litígios por difamação, verificando os fatos antes da publicação ou expressando o conteúdo como uma opinião e não como um fato (MAGRANI, 2018).

com diferenças locais significativas (ARAÚJO, 2009, p. 78 - 81). Um desafio comum para todos os atores é, portanto, desenvolver mecanismos que permitam solicitações transnacionais a provedores de acesso e a evidências eletrônicas baseadas em altos padrões do "devido processo legal" e proteção dos Direitos Humanos (BLUM, 2018; PINHEIRO, 2018; TEIXEIRA, 2018).

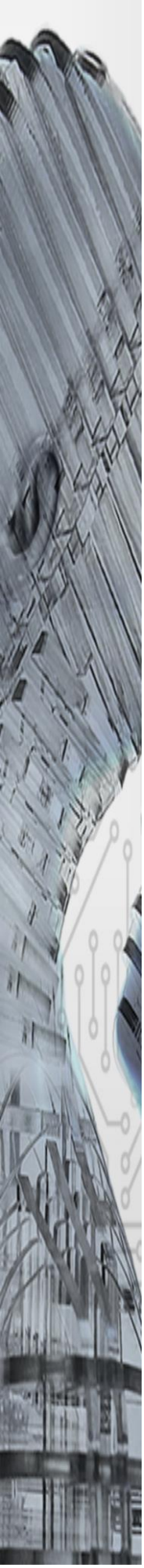
O cumprimento de sentenças estrangeiras também pode ser revisto à luz das leis de proteção de dados pessoais, tendo em vista a fluidez das relações, como percebido pela repercussão de determinadas decisões judiciais sobre casos envolvendo grandes empresas de tecnologia e provedores de conteúdo[84], sediadas em diversos países. "No âmbito da Internet, no caso específico da captação de dados, sua comercialização e o envio de mensagens eletrônicas, é possível perceber que há um aparente conflito de direitos constitucionais" (TEIXEIRA, 2018, p. 89), que "favoreceram a criação de um novo sistema legal e instituições para governar a atividade virtual, ou o exercício de autorregulação como um precursor das Convenções Internacionais" (ARAÚJO, 2011, p. 57). Logo, ações descoordenadas para enfrentar os desafios da jurisdição *crossborder* podem ter consequências não intencionais, incluindo aumento de conflitos de leis.

No escopo de minimizar conflitos entre jurisdições e esclarecer direitos oponíveis com força legal suficiente para sua positivação, o pensamento inovador se faz necessário para além dos quadros existentes, oportunizando o surgimento de mecanismos de cooperação transfronteiriça que protejam totalmente os direitos e a privacidade dos cidadãos, levando em conta os cenários legais estabelecidos sobre a proteção de dados pessoais, os procedimentos de investigação e as diferenças no tamanho, natureza e capacidade das partes interessadas, principalmente considerando a desigualdade de combate jurídico entre o indivíduo e uma grande empresa internacional ou entre o indivíduo e a Administração Pública de um Estado.

3.5 Perspectivas em jurisdição e positivação da proteção em dados à luz da Lei nº 13.709/2018

O panorama legislativo do Brasil republicano produziu um sistema com nuances naturalmente peculiares e, por sua vez, possuidora de semelhanças e distinções em relação aos também variados contextos jurídicos dos demais Estados (MORAES, 2018, p. 20 - 38),

[84] Tais como nos processos envolvendo empresas de tecnologia, como a Microsoft, Google, Youtube, Whatsapp, Facebook e Twitter, a respeito da retirada de conteúdos ofensivos, informações inverídicas, vazamentos de dados pessoais e pedidos de indenização.



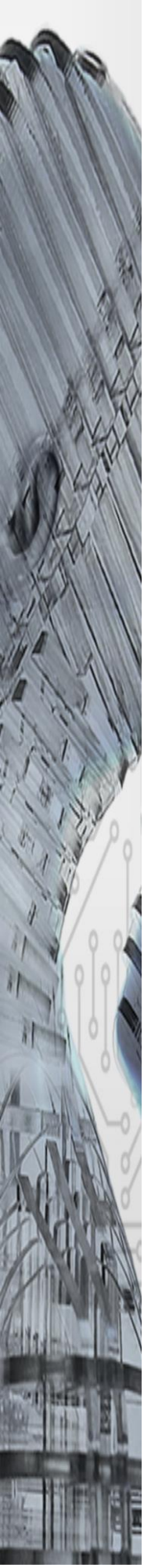
adeptos tanto da *civil law*, ou modelo romano-germânico, quanto da *commom law*, em arcabouços normativos variados (PERLINGEIRO, 2014, p. 79 -82). Esta natureza adaptável da construção do Direito Brasileiro aduz a uma significativa facilidade para a ocorrência do transplante de modelos legais estrangeiros à ordem jurídica nacional, "bem como aproxima os diálogos de fontes normativas, seja de matriz interna, seja no campo internacional" (NADER, 2017, p. 258).

À luz da LGPD (BRASIL, 2018) complementada pela MP nº 869/2018 (BRASIL, 2018) que foi convertida na Lei nº 13.853/2019 (BRASIL, 2019), a competência e a jurisdição em dados pessoais, no Brasil, podem ser exercidas tanto pela via judicial, quanto em patamar administrativo, através das funções, condições e limitações previstas para a ANPD.(BIONI, 2018; BLUM, 2018; PINHEIRO, 2018).

A exigência do devido processo legal representa no Brasil - e em outros países, a faculdade do Estado de fazer e aplicar a justiça, ou seja, de exercer a jurisdição através de juízes ou de tribunais (PERLINGEIRO, 2014, p. 79 - 82), "dentro de um processo, para solucionar um litígio entre partes" (FÜHRER, 2017, p. 55). Assim sendo, a privacidade como direito fundamental reconhecido pela Constituição da República Federativa do Brasil de 1988 (BRASIL, 2018), permitiu a discussão judicial acerca dos direitos sobre a personalidade, e a proteção de dados pessoais (BLUM, 2018, p. 20 - 28).

A inserção da LGPD (BRASIL, 2018) no ordenamento jurídico brasileiro de jurisdição unitária (onde somente as decisões do Poder Judiciário produzem coisa julgada exequível), fortalece a privacidade nacionalmente como um direito fundamental, ao passo que também "ilustra o transplante e a adaptação do RGPD (UE, 2016) europeu para o sistema normativo nacional" (BLUM, 2018). Apesar da jurisdição brasileira ser unitária e o Judiciário ser o titular do *decisium* em qualquer matéria submetida à tutela jurisdicional (PERLINGEIRO, 2014, p. 79 - 82), é pouco prudente dissociar a compreensão da LGPD de seus aspectos geracionais, lastreados em norma regional para o bloco europeu, o qual integra-se majoritariamente por países de jurisdição mista (compreendida entre a Jurisdição Judiciária e a Jurisdição Administrativa).

Portanto, as circunstâncias determinantes para a definição de competência de um tribunal brasileiro, no caso de procedimentos envolvendo dados pessoais, face ao descumprimento de qualquer dispositivo da LGPD (BRASIL, 2018), podem considerar como polo ativo o titular dos dados, as personalidades jurídicas de direito privado que realizam



tratamento de dados pessoais em geral e os setores dos Poderes Executivo, Legislativo e Judiciário (e organismos da Administração Pública).

Já no polo passivo, podem figurar as seguinte personalidades de direito: (I) as empresas brasileiras; (II) as empresas estrangeiras (com filiais no Brasil ou não); (III) municípios; (IV) estados; (V) União (VI) empresas públicas, fundações, autarquias, sociedades de economia mista (VII) órgãos dos Poderes Executivo, Legislativo e Judiciário que realizem tratamento de dados pessoais (VIII) empresas do terceiro setor (IX) pessoas físicas que realizem tratamento de dados pessoais e; (X) nos demais casos em que um tribunal pode exercer jurisdição[85] sobre um réu estrangeiro acusado de ter cometido um ilícito cível, criminal ou administrativo, conforme os mecanismos da jurisdição *cross-border* presentes nas leis brasileiras.

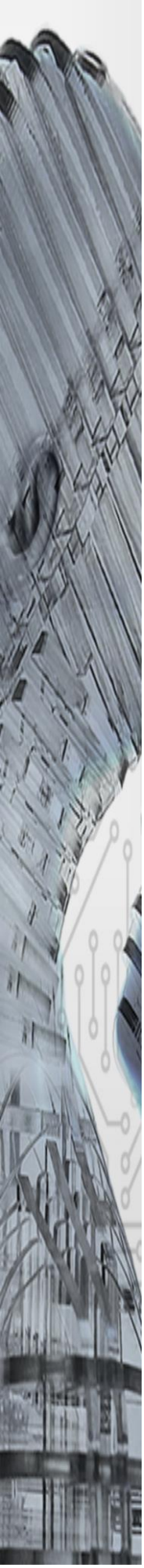
Também é possível que uma empresa tomadora de dados (física ou virtual "empresa.com") ou entidade governamental, colete, trate e armazene informações e dados pessoais ou sensíveis em algum *data center* pertencente a uma terceira empresa, revelando a possibilidade de procedimentos envolvendo personalidades jurídicas públicas ou privadas (em litisconsórcio) face à empresa depositária de dados, de modo concorrente, sob a perspectiva da responsabilidade civil.

Conforme já exposto, será competente a Justiça Brasileira quando o local de cumprimento das obrigações ocorrer em território brasileiro (NADER, 2017, p. 155 - 156); "nas situações nas quais a obrigação principal tiver de ser cumprida no Brasil" (SARLET, 2018, p. 44), sendo vedado às partes dispor sobre a competência internacional concorrente por força das normas fundadas na soberania nacional, não suscetíveis à vontade dos interessados (TRINDADE, 2002, p. 132 - 134).

3.6 Competência e jurisdição em dados pessoais tratados por empresas nacionais

À luz da LGPD (BRASIL, 2018), a relação entre o cliente como pessoa física e a empresa nacional responsável pela coleta, armazenamento e tratamento de dados, pode encontrar definição facilitada pelo disposto no art. 53, inc. III, alínea "a", do Código de Processo Civil (BRASIL, 2016), onde é comportada a competência em razão do foro, para a sede da empresa, em ação nas quais figurem como parte ré alguma pessoa jurídica.

[85] Outro fator capaz de modular e facilitar a delimitação da jurisdição se refere à utilização das TICs pelos Tribunais nacionais (TEIXEIRA, 2018, p. 567 - 620), os quais têm adotado o sistema de protocolo integrado, propiciando a realização de atos processuais sem a necessidade de deslocamentos constantes para partes e seus procuradores até suas sedes físicas.

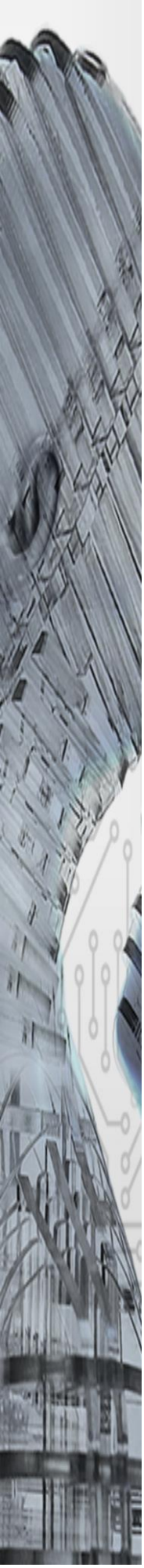


As relações cíveis envolvendo a cessão de dados pessoais dos titulares/consumidores para empresas nacionais, sob o prisma da jurisdição, se enquadram em um sistema amplo, com fontes materiais e processuais multidisciplinares e sobrepostas ou concorrentes, todavia herméticas e mergulhadas nas balizas legais nacionais, de modo a permitir um enquadramento de aplicação da tutela jurisdicional local, capaz de sanar a controvérsia e executar decisões legalmente eficazes (MENDES; SARLET; COELHO, 2015).

Um ponto chave para as relações entre titulares e controladores de dados está fundamentado nas cláusulas que compõem o contrato adesivo ou instrumento de cessão usualmente requisitado por empresas, como mecanismo jurídico de obtenção do consentimento, conforme previsto pelos arts. 5º, inc. XII e 7º, inc. I, ambos da LGPD (BRASIL, 2018). A concessão e a retirada do consentimento sobre tratamento de dados do titular para o controlador são dispostas de forma simplificada e maleável, na configuração instituída pelo art. 8º, também da LGPD (*Ibidem*). Neste sentido, qualquer atividade não definida nos termos de cessão ou consentimento, gera vício e torna o ato anulável.

Na perspectiva prática da jurisdição, esta relação entre o cessionário de dados, como titular de dados e, por vezes, consumidor, em face de uma pessoa jurídica de direito privado, caracterizada como prestadora de um serviço ou produto, com a finalidade de auferir lucros ao mesmo tempo em que coleta e trata dados pessoais de clientes, aduz para si as tutelas previstas no Código de Defesa do Consumidor (BRASIL, 1990), as quais se apresentam de forma contígua à LGPD (BRASIL, 2018), ao Direito e ao Processo Civil, mecanismos capazes de fundamentar possíveis adjudicações, lastreados nos construtos apresentados pelos artigos 6º, VIII, e 101, I, do CDC, permitindo a distribuição do processo judicial no foro de domicílio do autor.

Tendo em vista a possibilidade de a atividade comercial atingir nichos de consumo variados, principalmente quando empresas oferecem produtos e serviços, como também realizam anúncios publicitários com alcance nacional (TEIXEIRA, 2018, p. 290), a competência relativa em razão do foro decorre da responsabilidade fortuita do fornecedor em arcar com os custos e riscos da atividade por ele exercida (BENJAMIN; MARQUES; BESSA, 2017, p. 157 - 166), conglobando os vícios em seus produtos e serviços, como uma das possíveis consequências absorvidas face ao lucro almejado. No mesmo jaez, caso seja a ação proposta pelo fornecedor em face do consumidor, a competência será fixada no domicílio deste, não podendo o fornecedor optar pelo foro do seu domicílio (MARQUES, 2007, p. 69 - 71).



O artigo 6º, inc. VIII, do CDC (BRASIL, 1990) dialoga com o art. 8º, § 2º, da LGPD (BRASIL, 2018). Enquanto o CDC assegura a facilitação da defesa dos direitos do consumidor, facultando a inversão do ônus da prova (BENJAMIN; MARQUES; BESSA, 2017, p. 170 - 174), a LGPD institui como "cabível ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o fixado nos demais dispositivos da própria LGPD" (BIONI, 2018, p. 182).

Muito embora o instrumento (contrato ou autorização expressa, através do qual as limitações da cessão de dados pessoais estarão fixadas e o titular irá conhecer das finalidades sobre a utilização de suas informações particulares), possa vir a possuir cláusula de eleição do foro competente para julgar as questões envolvendo extrapolação do avençado, esta não poderá afastar o direito do consumidor de optar pela propositura da demanda no foro de seu domicílio, conforme preceitua o art. 101, inc. I, do CDC (BRASIL, 1990), configurando-se nula de pleno direito, pois coloca o consumidor em abismal desvantagem e vulnerabilidade frente ao fornecedor/tratador de dados, conforme expõe o art. 51, inc. IV, do CDC (*Ibidem*).

Portanto, os instrumentos de cessão de dados pessoais, tão logo tenham a adesão expressa de seus titulares, devem permanecer disponibilizados aos polos da relação e não serem modificados sem expressa autorização das partes (BENJAMIN; MARQUES; BESSA, 2017, p. 198 - 210), "sendo possível a utilização de meios alternativos de solução de conflitos também" (DI PIETRO, 2016, p. 88), permanecendo o foro para ingresso da ação como sendo o domicílio do consumidor (TEIXEIRA, 2018, p. 260 - 281), na qualidade de titular de dados.

3.7 Jurisdição em dados pessoais tratados por empresas transnacionais no Brasil

Ao se tratar da competência e da fixação da jurisdição entre pessoas físicas/titulares de dados e empresas transnacionais, mas com sede no Brasil, é possível traçar dois panoramas distintos que, vinculados às cláusulas do instrumento de cessão de dados, determinarão a forma como o poder Judiciário se norteará para prestar a tutela jurisdicional, sendo possível vislumbrar as possibilidades de: (I) ocorrer o tratamento e armazenamento de dados somente no Brasil ou; (II) ocorrer tratamento, armazenamento e transferência de dados em bases de dados sediadas em país estrangeiro, não configurando necessariamente a sede da empresa.

Na hipótese de empresa transnacional se limitar a realizar atividades em tratamento de dados pessoais de brasileiros somente na sucursal sediada no território nacional, com cláusula prevista no instrumento de adesão, a jurisdição pode ser fixada de maneira similar

àquela aplicável às empresas nacionais (BENJAMIN; MARQUES; BESSA, 2017, p. 204 - 205), com base na Súmula nº 363, do Supremo Tribunal Federal (BRASIL, 2017), a qual dispõe que "a pessoa jurídica de direito privado pode ser demandada no domicílio da agência ou estabelecimento em que praticou o ato".

Quando a requerida se tratar de empresa estrangeira que detenha sucursal brasileira, portanto, deve ser demandada, em regra, na Comarca do domicílio desta (BENJAMIN; MARQUES; BESSA, 2017, p. 204 - 205), nos termos do artigo 21, inciso I e parágrafo único c/c o artigo 53, inciso III, a e b, ambos do Código de Processo Civil – CPC (BRASIL, 2016).

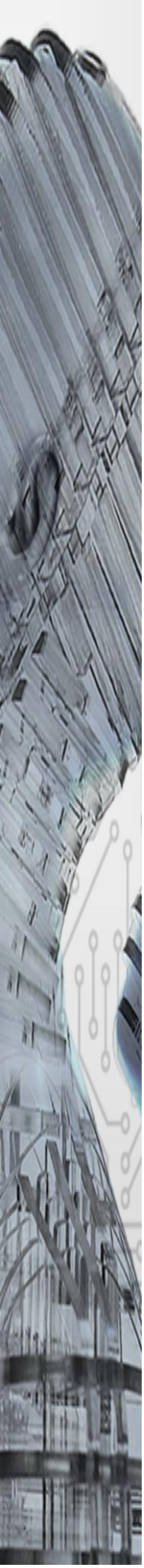
Na hipótese de ocorrerem o tratamento, o armazenamento e a transferência de dados a bases de dados sediadas em país estrangeiro, não configurando necessariamente a sede da empresa, haverá manifesta pluralidade de domicílios (BLUM, 2018, p. 79), sendo um deles no Brasil e possivelmente ou certamente tendo nele ocorrido a cessão dos dados pessoais, nos moldes do art. 3º, § 1º, da LGPD (BRASIL, 2018), aplica-se a jurisdição territorial nacional, também conforme preceitua o disposto no inciso II, do art. 75, § 2º, do CC/2002 (BRASIL, 2019), considerando a universalidade do fato em detrimento das unidades sucursais que viabilizam a realização das atividades empresariais (BENJAMIN; MARQUES; BESSA, 2017, p. 204 - 205).

3.8 Jurisdição administrativa na atuação da ANPD

Outro ponto de especial atenção trata das competências atribuídas à Autoridade Nacional de Proteção de Dados – ANPD, de modo a perfazer uma comparação em relação à Lei da Transparência e à LGPD (BRASIL, 2018), no tocante às formas de efetivação de suas previsões, considerando a competência para o exercício da jurisdição administrativa, conferida por ambas as leis, ainda que dentro de uma moldura normativa monista, onde o Poder Judiciário exerce soberana decisão, no ordenamento pátrio.

A LGPD (BRASIL, 2018) passou a apresentar dentre muitas características específicas, três de maior relevância para o estudo do exercício da jurisdição, sendo elas: (I) a criação de uma autoridade nacional de proteção de dados[86] (ANPD) com a função precípua de

[86] A criação da ANPD estava prevista no texto aprovado da LGPD, sendo vetada pelo então Presidente da República Michel Temer, sob a justificativa de vício de consentimento, por dever se tratar a criação desta agência de ato privativo do Poder Executivo e não uma ação proveniente do Poder Legislativo. Tal questão somente foi sanada pela publicação da Medida Provisória nº 869/2018 (BRASIL, 2018) e a sua conversão na Lei nº 13.853/2019 (BRASIL, 2019), que esclareceu a forma e o escopo da criação da ANPD, complementando o texto da LGPD.



supervisão (poder de polícia e o *enforcement* legal para que a lei tenha eficácia) – art.55-A ao 55-K; (II) a função de *ombudsman* – art. 55-C, inc. IV e; (III) a função didática de orientação de agentes e consumidores acerca da interpretação da própria LGPD, conforme o art. 58-B, inc. V.

A ANPD também é competente para elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade (BRASIL, 2019), ou seja, poderá criar diretrizes comuns aplicáveis a entidades públicas e privadas, como também poderá fiscalizar e aplicar sanções, conforme previsão dos arts. 52 a 54, da LGPG (BRASIL, 2018). A competência regulatória da ANPD possui jurisdição nacional, atuando e fiscalizando agentes econômicos, empresas nacionais e transnacionais, como também órgãos, autarquias, empresas públicas e de capital misto, além de demais setores vinculados aos governos municipais, estaduais e da administração federal.

A atuação da Administração Pública Federal na criação da ANPD, conforme previsão do art. 55-A, da LGPD (BRASIL, 2018) vinculou esta última ao Poder Executivo Federal, ou seja, a subsumiu ao controle direto da Presidência da República, competente para criar o Conselho Diretor, indicado pelo Presidente da República, com mandatos de quatro anos, como também o colegiado que compõem o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, vinculado à ANPD, composto por 23 titulares, com mandatos de dois anos não remunerados, sendo composto por: seis representantes do Executivo Federal; um representante indicado pelo Senado Federal; um representante indicado pela Câmara dos Deputados; um representante indicado pelo Conselho Nacional de Justiça; um representante indicado pelo Conselho Nacional do Ministério Público; um representante indicado pelo Comitê Gestor da Internet no Brasil; quatro representantes da sociedade civil com atuação comprovada em proteção de dados pessoais; quatro representantes de instituição científica, tecnológica e de inovação; e quatro representantes de entidade representativa do setor empresarial ligado à área de tratamento de dados pessoais.

Em que pese não haver uma jurisdição especializada do contencioso administrativo no Brasil, formado por tribunais exclusivamente voltados para o julgamento de demandas onde algum ente da Administração Pública figure como o polo que tenha cometido ou sofrido infração ou ilícito de natureza cível, criminal e, logicamente, administrativa (PERLINGEIRO, 2014, 79 - 82), além dos demais órgãos do Poder Judiciário, voltados para a solução dos demais litígios exclusivamente privados, a LGPD (BRASIL, 2018) e a Lei de Acesso à Informação (BRASIL, 2011) apresentam uma característica em comum: a competência de

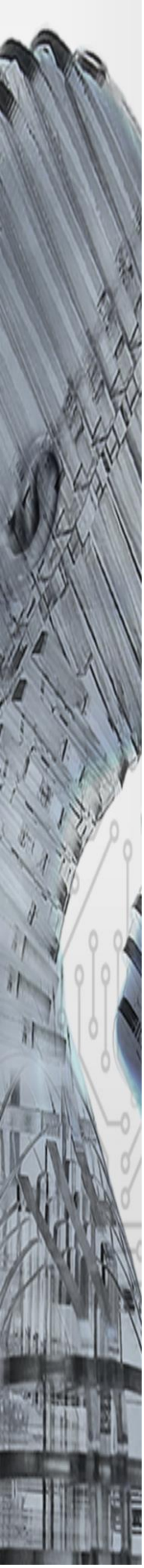
órgãos da Administração Pública para fiscalizar, realizar procedimentos e decidir questões a eles submetidas, dentro de suas molduras jurídicas (DI PIETRO, 2015; JUSTEN FILHO, 2005; VENOSA, 2016). Sobre a possibilidade de instauração de procedimento administrativo, Ricardo Perlingeiro comenta o seguinte, *in verbis:*

> Em outra perspectiva, sobre as decisões administrativas proferidas em virtude de uma solicitação do interessado, hoje tem sido considerada uma faculdade dele esgotar os recursos na via administrativa extrajudicial ou valer-se diretamente do processo judicial. Com efeito, essa faculdade não corresponde a uma adequada organização estatal: ou o recurso administrativo extrajudicial é instransponível, ou deve ser descartado.
> Por outro lado, com uma perspectiva mais rígida, afirmar ser necessário o recurso administrativo prévio, sob o fundamento de que é exclusividade das autoridades a oportunidade de rever suas decisões, é confundir o poder de autotutela na concepção do século XIX com a solução de causas administrativas na concepção atual. A indispensabilidade do processo prévio (recurso administrativo extrajudicial) deve ser proporcional à sua efetividade e, consequentemente, aos limites cognitivos de uma eventual e posterior revisão judicial. (PERLINGEIRO, 2014, p. 128 – 129)

O poder de polícia conferido à ANPD tem por objetivo fiscalizar ambas, as iniciativas privada e pública (incluindo o terceiro setor e pessoas físicas), conhecendo e determinando os mecanismos em segurança, a fim de assegurar a privacidade e a proteção de dados pessoais, sob a responsabilidade de qualquer espécie de entidade que realize o tratamento dos mesmos (BLUM, 2018, p. 157 - 159).

McLean (2010, p. 220 - 235) sugere formas de exercício da Jurisdição Administrativa, capazes de trazer soluções simplificadas, reunir provas e informações, além de promover a investigação de ilicitudes, mediante ações do poder Executivo, no plano de cooperação nacional ou internacional, baseadas no auxílio mútuo entre órgãos e entidades governamentais tais como: (I) a utilização da via Diplomática; (II) o apoio (direto) dos Consulados; (III) a ação consular indireta e preventiva; (IV) ações conjuntas entre Ministérios da Justiça de Estados distintos; (V) os diálogos e auxílios entre Autoridades Nacionais de proteção de dados de Estados distintos; (VI) a cooperação entre Ministérios da Justiça e Autoridades Nacionais de proteção de dados; (VII) A facilitação do acesso do demandante à requisição de providências junto às Autoridades Nacionais de proteção de dados (pedido de apuração e função de *ombudsman*).

O diálogo entre as fontes do Direito Público e do Direito Privado estão presentes na moldura normativa da LGPD (BRASIL, 2018) e nas demais normas reguladoras conexas. Muito embora a Administração Pública também colete, trate, armazene e possa vir a realizar transferências de dados entre entes federativos ou para endereços físicos e virtuais sediados em país estrangeiro (PINHEIRO, 2018, p. 188 - 196), estes devem respeitar os limites



traçados pela LGPD, nos moldes dos arts. 23 a 30, de forma a assegurar principalmente a distinção entre a informação pública, tutelada pela Lei de Acesso à Informação (ou Lei da Transparência) (BRASIL, 2011) e a informação lastreada em dados pessoais, tratados pela Administração Pública[87].

Os perfis de proteção de dados e os conceitos firmados na LGPD (BRASIL, 2018), aplicados à economia digital, à *Big Data* e à Administração Pública, representam um contexto de elevado valor econômico, político e social que, com a proliferação da utilização de equipamentos eletroeletrônicos com acesso à Internet, oportunizam a integração de legislações nacionais e internacionais capazes de dialogar entre si (BIONI, 2018; HAUNTS, 2018; PINHEIRO, 2018), ao passo em que oferecem a segurança jurídica em nível regional para a manutenção da privacidade, o fortalecimento do mercado, a soberania do Estado Constitucional Democrático, a realização da dignidade da pessoa e o exercício da atividade jurisdicional de maneira eficaz, contribuindo também para o fortalecimento e ampliação dos Direitos Humanos.

A natureza desmaterializada de muitas das atividades realizadas através de aparatos tecnológicos, com emprego e tratamento em plataformas e bases de dados conectados à Internet e ao ciberespaço, carecem de contínua divulgação, a fim de tornarem-se conhecidas pela população, por agentes públicos e atores empresariais, com vista à compreensão comum das formas a partir das quais surgem as disputas envolvendo dados públicos e pessoais.

Para tanto, importa à ANPD esta divulgação, bem como a fiscalização contínua de entidades privadas e órgãos da Administração Pública, monitorando setores onde reclamações e processos judiciais sejam instaurados em maior volume, inclusive retrocedendo a análise a períodos anteriores à vigência da norma, cuja criação e previsão também buscou solucionar problemáticas já existentes e anteriormente debatidas em Tribunais com outras roupagens jurídicas.

A atuação da ANPD voltada para a definição de categorias especiais para o funcionamento dos *sites*, também pode vir a facilitar a prestação de orientações concretas sobre o que significa uma "violação" de dados, para fins do devido processo (BIONI, 2018, p. 189). No tocante aos litígios envolvendo contratos e cessão de dados pessoais, em ambiente físico ou na Internet, importa que o titular esteja ciente dos limites, finalidades e duração da cessão de dados (BLUM, 2018; TEIXEIRA, 2018), bem como sejam promovidos os

[87] *E.g.:* dados pessoais sobre: (I) aposentadorias e benefícios junto ao Instituto Nacional da Seguridade Social; (II) informações sobre imposto de renda que contenham dados sobre patrimônio, endereço profissional e residencial; (III) operações financeiras junto a instituições bancárias de direito público, dentre outros.

elementos-chave de jurisdição pessoal tão enraizada no sistema nacional de jurisprudências, a fim de que a cessão realmente obedeça à transparência e aos conceitos relacionados à boa-fé, "incluindo a determinação de um nexo físico ou territorial que respalde qualquer necessidade ou forma de contato entre o titular de dados pessoais e a entidade que realiza o tratamento dos mesmos" (HAUNTS, 2018, p. 36), mediante o apoio de uma autoridade nacional de proteção autônoma e atuante.

3.9 Conflitos de Competência e Jurisdição no Poder Judiciário

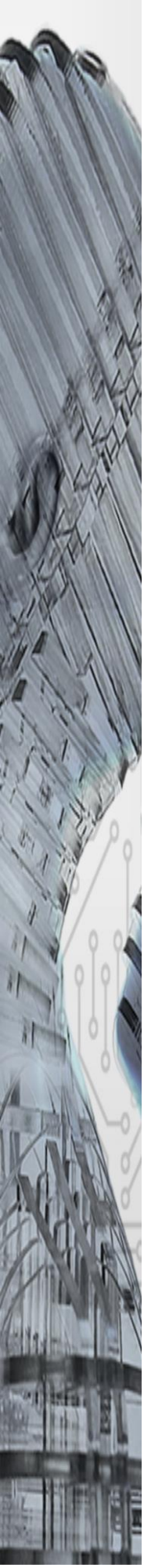
O engajamento judicial, tecnicamente instrumentalizado pelo processo como garantidor do Estado Constitucional Democrático, da autoridade estatal e do exercício jurisdicional, representa nas lições de Cândido Rangel Dinamarco (2003, p. 55 - 68), os escopos sociais, políticos e jurídicos norteadores das condutas dos agentes estatais.

De mesmo modo, a atuação do Estado-juiz, ao presidir um processo, pode tocar quatro perspectivas distintas e juridicamente concorrentes, sendo elas: (I) a competência do tribunal estadual onde os dados foram colhidos e tratados (art. 3º, da LGPD- art. 22, incs I, "b" e III, do CPC/2015) com base no princípio da territorialidade; (II) a competência com base na sede do ente público (art. 52 § único, do CPC/ 2015); (III) a competência da Justiça Federal (art. 109, da CF/88 *versus* art. 51, § único, do CPC/2015) ou; (IV) os litígios entre União, Estado, Distrito Federal e territórios, inclusive entidades de sua administração indireta, os quais serão resolvidos pelo STF (art. 102, I, "f" da CF/88[88]).

A regra apresentada pelo art. 102, I, "f" da Constituição Federal de 1988 (BRASIL, 2018), todavia, pode apresentar interpretação conflituosa, por força da mais recente jurisprudência da Corte Constitucional, devendo ocorrer a exata distinção entre o "conflito federativo" e o "conflito entre entes federados", cuja explicação[89] foi exposta no ACO 1.295 AgR-segundo (STF, 2010), esclarecendo que apenas os conflitos federativos competirão ao STF.

[88] Art. 102. Compete ao Supremo Tribunal Federal, precipuamente, a guarda da Constituição, cabendo-lhe:
I - processar e julgar, originariamente:
f) as causas e os conflitos entre a União e os Estados, a União e o Distrito Federal, ou entre uns e outros, inclusive as respectivas entidades da administração indireta;

[89] "[...] 3. Diferença entre conflito entre entes federados e conflito federativo: enquanto no primeiro, pelo prisma subjetivo, observa-se a litigância judicial promovida pelos membros da Federação, no segundo, para além da participação desses na lida, a conflituosidade da causa importa em potencial desestabilização do próprio pacto federativo. Há, portanto, distinção de magnitude nas hipóteses aventadas, sendo que o legislador nacional constitucional restringiu a atuação da Corte à última delas, nos moldes fixados pelo Texto magno, e não incluiu os litígios e as causas envolvendo municípios como ensejadores de conflito federativo apto a exigir a competência originária da Corte." (*In:* ACO 1.295 AgR-segundo. Rel. Min. Dias Toffoli. Brasília: STF, 2010)

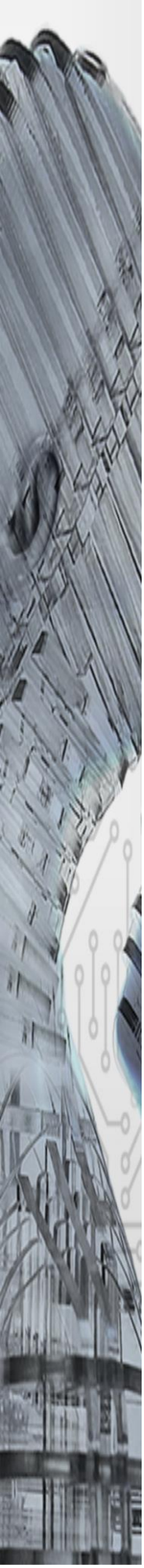


Logo, a construção jurisprudencial firmou entendimento no sentido de que a competência originária do STF estará configurada em casos nos quais for necessário julgar "as causas e os conflitos entre a União e os Estados, a União e o Distrito Federal, ou entre uns e outros, inclusive as respectivas entidades da administração indireta" (art. 102, I, f, da CF/88). Assim sendo, a posição da Suprema Corte atraiu para si o julgamento de causas em que a União figure como um dos polos, bem como excluiu de sua competência a análise de causas e conflitos entre Estados da Federação ou entre Estados e Municípios.

Quando houver litígio entre os entes da Federação, que não se qualificam como conflitos federativos, a competência originária é idêntica àquela ajustada para a natureza do conflito, tornando competente *prima facie* o STJ (ex.: art. 105, I, "g" da CF/88) ou a Justiça Federal (art. 109, I da CF/88). Como explica Luís Roberto Barroso (2019, p. 122), também deverão "estar explícitas questões de ordem subjetiva, tais como haver valor econômico relevante ou situação que ameace a manutenção do pacto federativo". Sob o prisma da LGPD (BRASIL, 2018), a competência para julgar ações envolvendo a proteção de dados pessoais também precisa representar conflito federativo, para ser apreciada pelo STF.

Já os conflitos internacionais (ou interfederativos), representados por disputas entre Estados diversos ou entre o Estado (nacional ou estrangeiro) e organismos internacionais, não produzem conflitos federativos, mas sim de natureza internacional, podendo adquirir ou não contornos interfederativos (MORAES, 2018, p. 43 - 56). Em qualquer subárea do Direito, mas com enfoque na privacidade na proteção de dados pessoais, a competência para julgar tais casos, será: (I) da Justiça Federal de primeira instância, quando a parte (demandante ou demanda) possuir domicílio, sede ou residência no Brasil, como nos casos onde um Município componha algum dos polos da lide (art. 109, II da CF/88), sendo cabível a utilização de Recurso Ordinário Constitucional para o STJ, nos termos do art. 105, II, c da CR/88, contra decisão de juiz federal de primeira instância, em substituição à peça de Apelação; (II) do STF, quando envolver os entes federativos, (União, Estados-membros ou o Distrito Federal), nos moldes do art. 102, I, "e" da CF/88 (BRASIL, 2018).

Neste ponto, importa destacar a possibilidade de ocorrerem conflitos de competência jurisdicional também entre Tribunais, ou entre Tribunais e juízes que primeiro conheceram da causa, de modo que a competência pode ser fixada conforme as previsões constitucionais específicas, tais como: (I) a competência do STF delimitada pelo art. 102, I, "o", da CF/88; (II) a competência do STJ proposta no art. 105, I, "d" da CF/88 e; (III) a competência dos TRF's, trazida no art. 108, I, "e", da CF/88.



A jurisprudência do STF, através do ACO 1342 AgRg/RJ (STF, 2010) esclareceu a respeito da não consideração de Municípios como entes federativos, tendo em vista não estar equiparado como "ente federado", por não possuírem os requisitos subjetivos (valor econômico relevante ou situação que ameace a manutenção do pacto federativo) (BARROSO, 2019), muito embora possam ser os municípios considerados "entes federativos de terceiro grau" (MENDES; BRANCO; COELHO, 2018; MORAES, 2018).

Neste espeque, o entendimento da Corte Constitucional trazido à inteligência do ACO 1342 AgRg/RJ (STF, 2010), delimita a competência da Justiça Federal em causas envolvendo os municípios, quando presentes em algum dos polos da ação a União, suas autarquias, fundações e empresas públicas federais. A competência da Justiça Federal também será fixada quando algum Estado-membro figurar como parte, exceto na superveniência de motivo capaz de aduzir a competência de outro órgão do Poder Judiciário, como a Territorialidade ou a continência.

Outro ponto de circunflexão se reflete pela previsibilidade de confecção de normas estaduais sobre proteção de dados pessoais e suas respectivas Autoridades de Proteção. A competência legislativa estadual pode ensejar um conflito infralegal de normas, quando a decisão recorrida julgar válida lei local contestada em face de lei federal (MORAES, 2018, p. 67 - 71), tendo em vista a essência constitucional da privacidade como direito fundamental e o patamar federal da LGPD, o que atrairia a competência do STJ, como "intérprete da legislação infraconstitucional federal" (BARROSO, 2019, p. 34).

Todavia, é possível a caracterização do "conflito federativo", cuja análise compete à Corte Constitucional, de forma originária ou em sede de recurso extraordinário e/ou especial, conforme as alterações realizadas pela Emenda Constitucional nº 45/2004, no art. 102, III, "d", da CF/88 (BRASIL, 2018) e pelos dispositivos trazidos no Código de Processo Civil de 2015 (BRASIL, 2016).

À luz do CPC/2015 (BRASIL, 2016), a competência internacional concorrente foi delimitada em ações de cunho consumerista e em causas nas quais as partes, expressa ou tacitamente, optem pela submissão à jurisdição nacional. Tendo por base o "sistema de ingresso multiportas", os defeitos de produtos e os ilícitos ocorridos nas relações consumeristas se enquadram nas regras de competência internacional concorrente. Todavia, caso o contrato ou instrumento jurídico firmado para garantir a relação entre as partes

contenha cláusula de eleição de foro estrangeiro, nos temos do art. 25, do CPC/2015[90], a competência da justiça nacional será afastada, contrariando o entendimento jurisprudencial do STF, firmado no Conflito de Competência 41728 (STJ, 2005), o qual anteriormente considerava nula a cláusula de eleição de foro diverso do domicílio do consumidor, por dificultar a defesa da parte hipossuficiente (BENJAMIN; MARQUES; BESSA, 2017, p. 220 - 234).

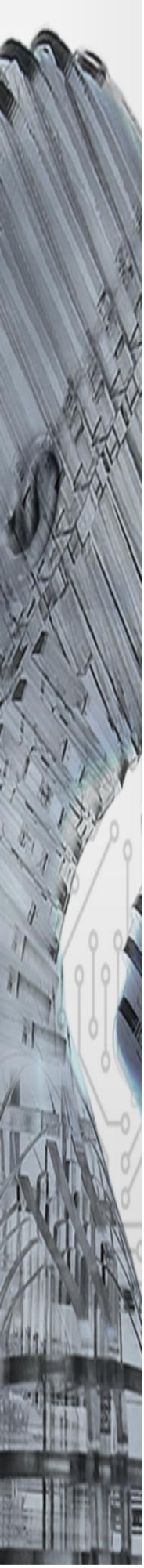
O CPC/2015 (BRASIL, 2016) trata da litispendência em casos de competência internacional concorrente, conforme a redação dada aos artigos 21, 22 e 23, todos do CPC/2015, de modo que a previsão da litispendência e da conexão internacional podem ser inseridas em tratado internacional e acordo bilateral. Igualmente, a impetração de demanda em foro de Estado estrangeiro induz à litispendência e à conexão, nos termos do art. 24, *caput,* do CPC/2015. Assim sendo, a existência em Tribunal estrangeiro de ação judicial não obsta à iniciação de processo com a identidade de partes, causa de pedir e objeto do pedido idênticos no Judiciário brasileiro, ainda que sobrevenha sentença estrangeira, a qual pode ou não ser homologada pelo Superior Tribunal de Justiça (art. 105, I, "*i*", da CF/88), para então adquirir eficácia executiva nacional (MENDES; BRANCO; COELHO, 2018, p. 47).

Na perspectiva da privacidade e da proteção a dados pessoais, a previsão de cooperação internacional possibilita a alegação de litispendência e conexão, seja mediante aplicação subsidiária de dispositivo insculpido em Tratado Internacional ou Acordo Bilateral, seja quando houver cláusula de eleição de foro estrangeiro em contrato ou instrumento de cessão de dados, que não exclua a jurisdição nacional.

Os conflitos decorrentes da relação contratual podem ser dirimidos tendo por base a previsão do art. 23, do CPC/2015, fixando a competência exclusiva nacional ou aplicação do art. 63, também do CPC/2015, o qual possibilita a modificação da competência em razão do valor e do território, face à cláusula de eleição do foro. Ambas as opções tem por escopo diminuir controvérsias e fixar, desde o início da relação de consumo, o foro competente para julgar a lide, nas hipóteses de competência internacional concorrente.

Em nível nacional, os diálogos entre Tribunais (e a ANPD) irão requerer aperfeiçoamentos contínuos, quando da criação e alteração das leis de proteção de dados em nível estadual e em relação às formas como as suas aplicações e adjudicações ocorrerão, bem

[90] Art. 25. Não compete à autoridade judiciária brasileira o processamento e o julgamento da ação quando houver cláusula de eleição de foro exclusivo estrangeiro em contrato internacional, arguida pelo réu na contestação.
§ 1o Não se aplica o disposto no caput às hipóteses de competência internacional exclusiva previstas neste Capítulo.
§ 2o Aplica-se à hipótese do caput o art. 63, §§ 1o a 4o.



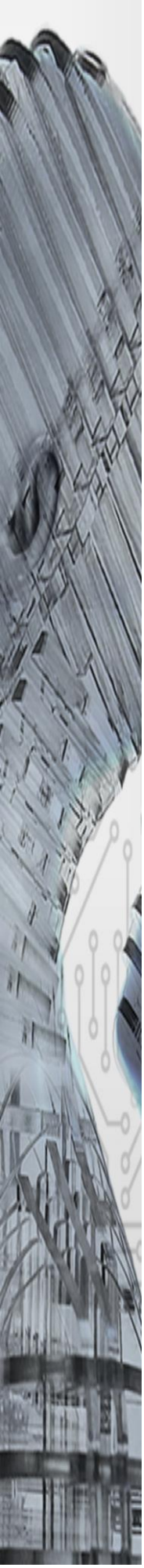
como as produções jurisprudenciais se encaminharão, tendo em vista a existência de 91 tribunais, de competência comum ou especializada, sendo: 61 tribunais na esfera federal, com 1 supremo tribunal, 4 tribunais superiores; os 27 tribunais regionais eleitorais (um em cada unidade federativa); os 24 tribunais regionais do trabalho (um por unidade federativa, exceto São Paulo, que tem dois - um na capital e outro em Campinas - e Acre, Roraima, Amapá e Tocantins, que estão sob a jurisdição dos tribunais baseados em Rondônia, Pará, Amazonas e DF, respectivamente) e; 5 tribunais regionais federais, além dos 30 tribunais estaduais, sendo: os 27 tribunais de justiça (um por unidade federativa) e três tribunais de justiça militar estaduais (apenas São Paulo, Minas Gerais e Rio Grande do Sul possuem tribunais de justiça militar estaduais) (CNJ, 2018).

Sob o prisma da privacidade e da proteção de dados, a harmonização de jurisprudências e acórdãos de tribunais diferentes, mantendo maior congruência e afastando (na medida do possível) os posicionamentos distintos entre si, mormente entre os Tribunais Estaduais e os Tribunais Superiores, tem por fito promover maior segurança jurídica e ampliar a eficácia pretendida pela LGPD (BRASIL, 2018) e as normativas advindas da ANPD, considerando um cenário onde os julgamentos têm a capacidade de promover significativa modulação das normas nacionais e internacionais, criando uma roupagem específica, porém com impactos duradouros, tendo em vista a juventude da LGPD no ordenamento jurídico nacional.

Sob tal espeque, importa aos Tribunais emitirem opiniões e produzirem suas jurisprudências sobre o assunto, com base em minuciosa análise e na ampla compreensão de contextos técnicos, econômicos e normativos, quando da oportunidade de decidirem sobre as questões relativas aos direitos à privacidade e à proteção de dados pessoais na jurisdição brasileira e no ambiente da Internet, com foco em estabilizar - antes de qualquer ato, os contornos jurisdicionais, considerando o padrão de *Due Process of Law* aplicados à perspectiva global onde ocorrem os atos, fatos e negócios jurídicos tuteláveis pela LGPD, tratados pela Administração Pública e por empresas, em localidade geograficamente conhecida, ou no ciberespaço.

3.10 A LGPD como mecanismo de cooperação

A busca por maior aproximação entre leis, sejam as estaduais face às federais, sejam as leis nacionais ou supranacionais (regionais ou de blocos econômicos), pode proporcionar a



edificação de um sistema com princípios e regras mais semelhantes, de modo que a aplicação das leis de proteção de dados entre entes administrativos diversos se encontrem mais pareados (BIONI, 2018 p. 199).

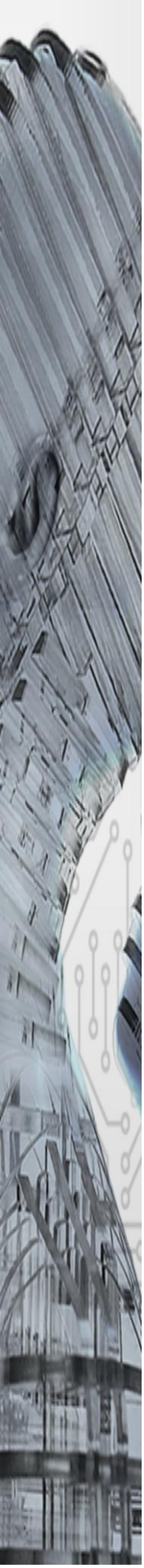
Tendo em vista que as leis de proteção de dados nacionais são desenvolvidas com base nas fontes de direito externo, na moldura normativa nacional e em valores culturais e jurídicos característicos de cada localidade, "a equiparação de todas as legislações de uma forma abrangente apresenta uma perspectiva pouco provável de ocorrer em curto prazo" (HAUNTS, 2018, p. 35), mesmo havendo a utilização do ciberespaço, como ambiente comercial e de tráfego de informações internacionalmente comuns.

Neste sentido, a cooperação entre autoridades reguladoras internacionais e nacionais, segundo McLean (2010, p. 225) "desponta como alternativa viável às adaptações legais de uma norma cujo escopo pode ser menos rígido e mais fluído, tendo em vista o contínuo aperfeiçoamento das leis", em atenção à proliferação de novas tecnologias para uso particular, empresarial e governamental.

Este viés congloba não somente a formalização da compreensão de conceitos e princípios comuns das leis de proteção de dados (como "dados pessoais", "controlador de dados" e "tratamento de dados"), como também delimita com maior clareza aspectos da legislação aplicáveis em relações de hipossuficiência, tais como as ocorridas entre o indivíduo e o Estado ou entre o indivíduo e empresas e corporações (BENJAMIN; MARQUES; BESSA, 2017; PINHEIRO, 2018; TEIXEIRA, 2018).

De forma semelhante, "os diálogos entre autoridades reguladoras também podem criar acordos multisetoriais e multilaterais capazes de reduzir o escopo e o impacto dos conflitos jurisdicionais (MCLEAN, 2010, p. 229), coordenando as "ações e posições de execução em questões jurídicas substantivas e de alcance regional ou internacional" (ARAÚJO, 2011, p. 157), além de reduzir a lacuna entre a não fiscalização e a efetiva aplicação da lei de proteção de dados, dando maiores possibilidades de execução da sentença em face de entidades nacionais ou transnacionais, de modo efetivo, dinâmico e cooperativo.

Tanto nos países de *civil law*, quanto nos de *commom law*, a jurisdição consubstancia regras voltadas para "a segurança jurídica lastreada na soberania de um Estado capaz de promover a tutela jurisdicional aos cidadãos e demais indivíduos em seu território, seguindo a legislação de forma flexibilizada e modulada às características de cada caso concreto" ((DINAMARCO; LOPES, 2016 ;DIDIER JR. ZANETI JR., 2017). Assim sendo, a jurisdição em proteção de dados pessoais também pode ser desenvolvida e aplicada tendo por critério a

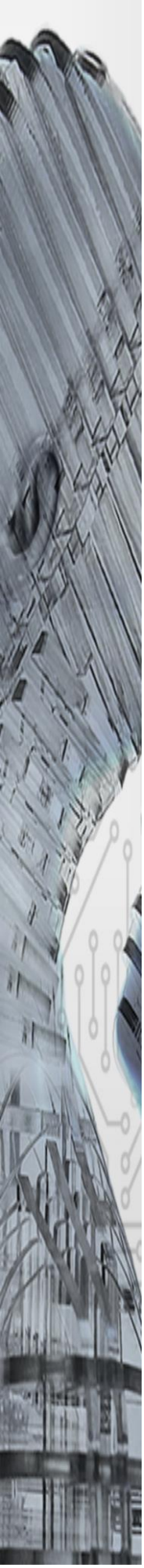


cooperação entre autoridades e jurisdições internacionais, permitindo que a competência seja definida de maneira a dar uma solução célere e adequada, elevando o grau aceitável de segurança jurídica buscada pela inserção das leis de proteção de dados nos ordenamentos jurídicos.

A jurisdição em proteção de dados pessoais, especialmente no ambiente do ciberespaço e da Internet, pode ser desenvolvida de maneira voltada para superar os meros interesses políticos, econômicos, comerciais ou sociais (PINHEIRO, 2018), de modo que os indivíduos se beneficiem da proteção das leis nacionais de proteção de dados e da supervisão das autoridades nacionais de proteção de dados nos casos em que tais amparos sejam necessários e quando exista um grau razoável de executoriedade para situações transfronteiriças (ARAÚJO, 2002; STRENGER, 2003; VENOSA, 2016). Estes elementos podem proporcionar uma maior interação entre a jurisdição e os sistemas normativos de proteção de dados, garantindo mais ampla segurança jurídica também para empresas e para o desenvolvimento da economia local, tradicional ou virtual.

O regime jurídico proposto na LGPD retrata também o fortalecimento e a reafirmação dos direitos humanos inalienáveis e constitucionais fundamentais, de modo que as produções normativas, regulamentares e jurisprudenciais também devam estar atentas aos princípios basilares da privacidade e da proteção aos titulares de dados pessoais, durante suas confecções, em vistas a fortalecer o Estado Democrático Constitucional, os diálogos internacionais, outrossim construindo um conjunto de direitos complementares, assegurados nacionalmente e internacionalmente.

Através de todos os dispositivos trazidos a comento durante o transcurso desta seção, buscou-se condensar uma estrutura de conhecimentos críticos e científicos, no intuito de pavimentar um pequeno trecho inicial dos caminhos por onde a LGPD começa a sua atuação protetiva, tendo no estudo da Jurisdição a sua consubstanciação mais prática, para as primeiras interpretações e formas de processamento, considerando os aspectos interdisciplinares e "transnormativos" desta nova Lei do Direito Brasileiro e o seu potencial contributivo para o desenvolvimento de uma sociedade mais ética e humanizada.

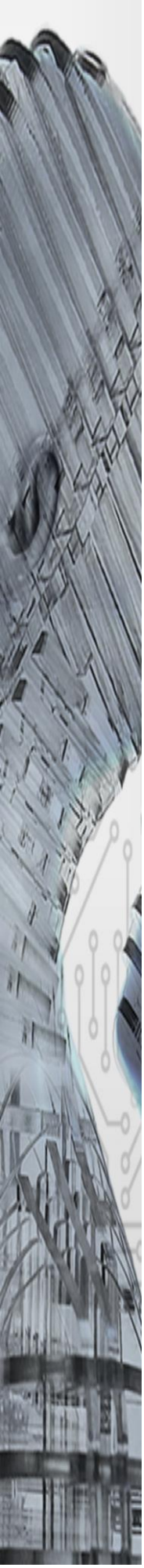


CONCLUSÃO

A presente pesquisa iniciou-se pela observação dos fatores objetivos e subjetivos que compõem a proteção de dados pessoais, considerando o estudo técnico de terminologias e nomenclaturas da Ciência da Computação, da Informática e das TICs, para garantir melhor compreensão contextual de eventos corriqueiros das atividades desenvolvidas no ciberespaço, com desdobramentos no cenário jurídico. Deste modo, foi possível perceber a paulatina incorporação de tais termos para o corpo de leis nacionais e estrangeiras, o que aponta o aumento da correlação entre o Direito e as Tecnologias de computação, informática e comunicação, pela aproximação semântica e suas predeterminadas repercussões na prática jurídica.

O mapeamento do cenário envolvendo a proteção de dados pessoais também convergiu os estudos para a análise de setores econômicos, sociais, administrativos e mercadológicos afetos à economia digital baseada na circulação globalizada de informações produtos, serviços e mercadorias, em formas físicas e digitais, e na consequente captação de dados pessoais, além de suas formas de utilização, reutilização, finalidades e capacidade de serem comercializados como bem ou ativo financeiro entre, governos ou empresas, integrando a formação de *BigData* à reunião de demais dados advindos de fontes públicas e privadas. O contexto delineado apontou para relativa liberdade normativa do comércio virtual e das amplas possibilidades de (má) utilização de dados pessoais, em decorrência da relativa ausência de mecanismos de regulamentação, tributação e limitação. Igualmente, foi possível perceber a migração da economia tradicional para o setor virtual, de forma a tornar necessária a revisão de muitas normas de direito civil, penal, administrativo e consumerista, a fim de promover um arcabouço legislativo mais atualizado, aperfeiçoado e capaz de fortalecer as leis de proteção a dados pessoais, à privacidade, à segurança digital, à intimidade e à liberdade de pensamento, expressão e associação, como Direitos Humanos e Constitucionais Fundamentais.

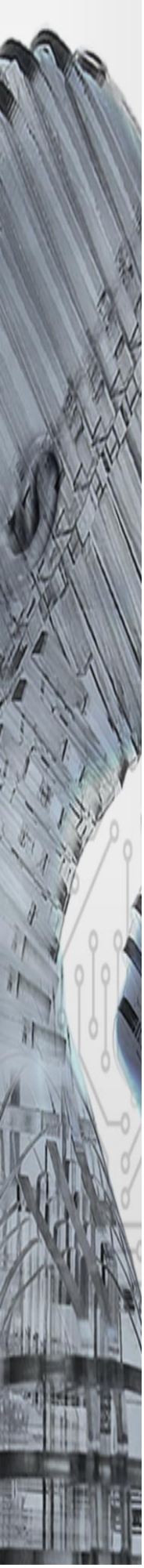
Após a compreensão da taxonomia e do *campus* onde podem se desenvolver as possíveis demandas envolvendo violação à proteção de dados pessoais, também foi analisado e compreendido o arcabouço normativo de maior relevância para o desenvolvimento do Regime Jurídico das Leis de Proteção de Dados Pessoais internacionais e a influência exercida na confecção das normas, princípios e regras (re) produzidas no âmbito da LGPD. A



partir de tais perspectivas, foi possível utilizar uma metodologia comparativa que culminou com a visualização de sistemas normativos distintos se encaminhando, desde a década de 1990, para o fortalecimento da soberania e do Estado de Direito, mediante a proteção por parte da Administração Pública aos dados pessoais de cidadãos e residentes em seu território.

De maneira especial, os estudos voltados para as leis brasileiras selecionadas como objetos de análise, demonstraram a caminhada dos Poderes da República, seus órgãos e entidades, na esteira da absorção de novas tecnologias nos serviços públicos, bem como a entrada em vigor da Constituição Federal de 1988, que trouxe princípios norteadores e direitos fundamentais, como a privacidade, dentre outros, os quais foram ampliados e reafirmados com o advento da Lei de Acesso à Informação, do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais. Logo, foi possível perceber os mecanismos de diálogo, sobreposição e integração entre normas, visando uniformizar o acesso às informações públicas, controlar a utilização de dados pessoais e a utilização sadia da Internet e do ciberespaço, além de fortalecer o Direito Virtual e Eletrônico como uma seara jurídica em franco crescimento, e aproximação também aos Direitos Humanos e Constitucionais Fundamentais, como fontes capazes de harmonizar o Regime Jurídico nacional com normas estrangeiras e internacionais. Neste sentido, o estudo também desenvolveu considerações críticas à sobreposição de tais normas, face à privacidade como direito fundamental e o interesse público, como ponto doutrinariamente controvertido, no que tange à sua primazia por sobre a proteção de interesses particulares. Todavia, é de se esperar que a positivação de tais direitos possa aumentar a proteção à pessoa como titular de seus dados e parte hipossuficiente – porém detentora de direitos de primazia protetiva inalienáveis e suficientemente capazes de caracterizar o "interesse público", como um direito de proteção à privacidade, à intimidade, à segurança e à autodeterminação informativa, colocando os interesses de Governos e empresas em uma posição de relativa inferioridade ou de preponderância mitigada, face aos direitos das pessoas, como cidadãs e titulares.

Com todo este cenário já investigado e sintetizado, a pesquisa se voltou para a análise da Jurisdição nas Leis de Proteção de Dados pessoais. A partir de então, foram desenvolvidas duas perspectivas críticas sobre a temática, onde num primeiro momento foi analisada a Jurisdição em suas bases principiológicas e normativas, com base nas regras comuns de direito internacional público e privado e, na segunda fase, foram explorados os critérios e entendimentos sobre Jurisdição à luz da LGPD e sua recepção no ordenamento jurídico brasileiro, considerando outras fontes de Direito, como o Civil, Processual Civil,



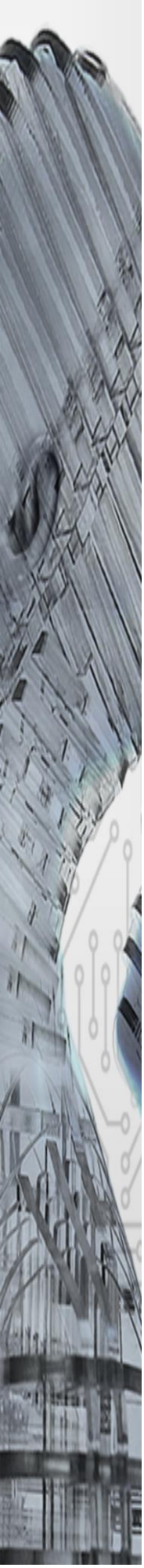
Constitucional, além de Súmulas e Jurisprudências de Tribunais Superiores. A construção de tais conhecimentos, dentro do recorte temático propugnado, objetivaram entabular um diálogo suficientemente capaz de elucidar a competência para julgar de Tribunais nacionais em demandas envolvendo a proteção de dados pessoais, conforme a legislação doméstica indica na vigência da LGPD.

Os resultados obtidos durante a pesquisa, abarcando os atuais cenários, permitem o vislumbre de diversas formas de aperfeiçoamento do direito à proteção de dados pessoais, tais como a construção de jurisprudências, de julgados e o exercício boas práticas forenses, voltadas para discussões de teses e análises das variáveis processuais, com o objetivo de pavimentar um caminho de segurança na prestação da atividade judiciária. A produção de orientações por parte da ANPD e a pesquisa científica e acadêmica, também poderão em muito contribuir para a divulgação e a ampliação da consciência de direitos e deveres em proteção de dados pessoais, voltada para a disseminação de tais saberes para a sociedade em geral, bem como fortalecendo e valorizando cada vez mais a positivação das regras, normas e princípios defendidos pelos Direitos Humanos, Constitucionais e todas as demais normas e políticas públicas de proteção dos direitos do cidadão.

A novidade do tema e a pouca profundidade dedicada às discussões sobre a jurisdição em leis de proteção de dados na literatura científica nacional, fazem com que a difusão de novos direitos à população e as limitações legais a eles conexas ainda não estejam intimamente conhecidas pela maioria dos residentes no Brasil e, especialmente, pelos reguladores de proteção de dados, cujo entendimento superficial das questões de jurisdição nacional e sua sobreposição em questões envolvendo entidades transnacionais podem ensejar contendas judiciais, facilmente evitáveis pelo aprofundamento de normas nacionais conexas à LGPD.

Assim sendo, os estudos envolvendo a LGPD, num cenário de migração da economia dos mercados tradicionais para os virtuais e a “facilitação do acesso”, pela Internet, à realização de atividades de consumo, como também de fiscalização popular da transparência de atos realizados pela Administração Pública, como a consultas a informações orçamentárias e de agentes públicos, representam novas formas de compreensão do processo judicial no Brasil, que também já se encontra em fase eletrônica.

Dentre os conflitos de interesses jurídicos e econômicos, resta a matriz do problema, que é a (má) utilização dos dados de pessoais, muitas vezes reduzidos à condição de “ativos” financeiros a serem mercantilizados para atender às necessidades do capital empresarial, sem

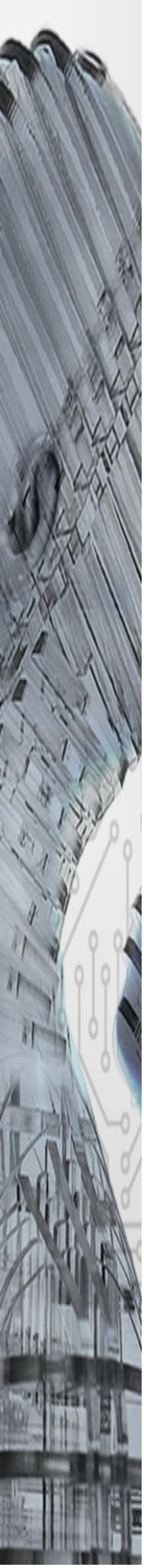


a devida ética e o respeito à dignidade da pessoa humana. Este quadro de descompromisso com a preservação da incolumidade particular de indivíduos, fica ainda mais comprometido quando a destinação dos dados pessoais é definida por inteligências artificiais, algoritmos com definições pré-formuladas (reduzindo o poder de escolha de usuários ou cruzando dados para finalidades diferentes daquelas avençadas no momento da cessão) e *BigData,* que tira a característica da individualidade, da personalidade e da pessoalidade, para compor dados massificados e quantitativos numéricos capazes de excluir a essência de humanidade de onde é proveniente em muitas circunstâncias.

Logo, é possível perceber que as leis de proteção de dados pessoais, muito embora tenham aplicação extraterritorial ou atraiam para si a jurisdição em questões judiciais, por seu próprio aspecto geracional, não estipulam mecanismos capazes de fixação clara da base jurisdicional e da competência para julgar. Esta ausência de definição expressa reduz a amplitude protetiva, quando as leis de proteção de dados pessoais são consideradas “a pedra angular dos direitos humanos na era digital”.

As empresas, particularmente no setor de tecnologia, são mais reativas que proativas em privacidade de dados. Para que a privacidade do consumidor realmente chegue ao primeiro plano, é provável que os governos, através de suas Autoridades e Agências Nacionais de Proteção de Dados, também tenham que desempenhar um papel de proteção - especialmente nos casos em que os consumidores sequer conseguem optar de maneira realmente consciente sobre os termos e condições de usos (como instrumentos de cessão e consentimento) de produtos e serviços desenvolvidos (ou não) com base nos critérios e princípios gerais da proteção de dados pessoais e da privacidade - por ainda não se encontrarem difundidas as ferramentas didáticas que promovam a autodeterminação informativa e coerção em face de empresas que utilizam brechas legais para manter práticas pouco alinhadas à afirmação dos direitos inalienáveis e fundamentais à proteção de dados pessoais.

Assim sendo, a assimilação da jurisdição em proteção de dados pessoais, em questões cujos polos representem personalidades de direito nacional (público ou privado), ou concorram com a jurisdição de Estados estrangeiros, requer estudo e adaptações contínuas, para haver certa condição de administração e garantia da segurança jurídica por parte dos tribunais nacionais e das ANPDs, de modo a satisfazer direitos e garantias fundamentais, bem como para formular um padrão mais flexível de jurisdição doméstica, abrangendo novas



tecnologias em projeção a cenários futuros, de forma autônoma e integrada à realidade nacional e à eficiência da Administração Pública.

Portanto, esta pequena contribuição teve por objetivo proporcionar a facilitação da compreensão a respeito da proteção de dados pessoais como proveniente do direito fundamental à privacidade, tanto para operadores do Direito, quanto para interessados em melhor compreender a constelação científica por detrás da LGPD aplicada ao cotidiano social, o qual se apresenta de forma cada vez mais atrelada à cessão de dados pessoais para a realização de atividades, de cunhos público e privado, mediante utilização de equipamentos eletroeletrônicos conectados à Internet.

Os impactos advindos da LGPD somente estarão claramente mensuráveis após alguns anos de vigência da referida lei, da adaptação de empresas às suas imposições e dos julgamentos de demandas envolvendo questões tuteladas pela proteção de dados. Assim, a compreensão aprofundada das bases técnicas, econômicas, sociais, político-diplomáticas de Jurisdição, nos prismas nacionais e internacionais, permitem a previsão dos possíveis desdobramentos sobre o (des)cumprimento das leis e resoluções sobre proteção de dados, permitindo o aperfeiçoamento desta área, com estratégias lúcidas e voltadas ao fortalecimento do Estado Constitucional de Direito e a promoção dos Direitos Humanos, com a proteção da dignidade da vida humana, da personalidade e da privacidade na Era Digital.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Fontes de Direito, Leis, Normas e Regulamentos

AFRICA DO SUL. **Constituição da República da África do Sul, de 11 de outubro de 1996**. Cidade do Cabo: Parlamento da África do Sul, 1996. Disponível em: < https://www.concourt.org.za/images/phocadownload/the_text/english-2013.pdf>. Acesso em: 29 mar. 2019.

ARGENTINA. **Constitución de la Nacion Argentina, de 1853, actualizada por la Reforma Constitucional de 22 de agosto de 1994**. Santa Fe: Convencion Nacional Constituyente – Boletin Oficial, 1994. Disponível em: <http://www.constitution.org/cons/argentin.htm?PHPSESSID=095185bf7651b6839b7c935f65b5d89e>. Acesso em: 25 fev. 2019.

ARGENTINA. **Ley 25.326** - Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Buenos Aires: Boletin OFicial, 2000. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>. Acesso em: 29 mar. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ISO / IEC 27001: 2013.** Rio de Janeiro: ABNT, 2013. Disponível em: < https://www.abntcatalogo.com.br/norma.aspx?ID=306580>. Acesso em: 26 mar. 2019.

_____. **ISO / IEC 27002: 2013.** Rio de Janeiro: ABNT, 2013. Disponível em: < https://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 26 mar. 2019.

_____. **NBR 6022**. Rio de Janeiro: ABNT, 2003.

_____. **NBR 6023.** 2 ed. Rio de Janeiro: ABNT, 2018.

_____. **NBR 6024**. Rio de Janeiro: ABNT, 2012.

_____. **NBR 6027**. Rio de Janeiro: ABNT, 2012.

_____. **NBR 6028**. Rio de Janeiro: ABNT, 2013.

_____. **NBR 10520**. Rio de Janeiro: ABNT, 2002.

_____. **NBR 14724**. Rio de Janeiro: ABNT, 2011.

ÁUSTRIA. **Datenschultzgesetz.** Viena: Parlamento da Áustria: 2000. Disponível em: < https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597>. Acesso em: 20 mar. 2019.

BRASIL. Constituição de 1988. **Constituição da República Federativa do Brasil.** 53. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2018.

_____. **Decreto-Lei 2.848, de 07 de dezembro de 1940**. Código Penal. Rio de Janeiro - Diário Oficial da União, 31 dez. 1940. In: Vade mecum acadêmico de direito Rideel. 22 ed. São Paulo: Rideel. 2016.

_____. **Decreto nº 7.962, de 15 de março de 2013**. Brasília: DOU, 15 mar. 2013. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Acesso em: 20 fev. 2019.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Brasília: DOU, 11 maio 2016. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 20 fev. 2019.

_____. **Decreto nº 8.777, de 11 de maio de 2016**. Brasília: DOU, 12 maio 2016. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm>. Acesso em: 20 fev. 2019.

_____. **Decreto nº 9.319, de 21 de março de 2018**. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília: Diário Oficial da União - Seção 1, de 22 mar. 2018.

_____. **Emenda Constitucional nº 45/2004**. In: Vade mecum acadêmico de direito Rideel. 22 ed. São Paulo: Rideel. 2016.

_____. **Lei Complementar 105, de 10 de janeiro de 2001**. Brasília: DOU, 11 jan. 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 20 fev. 2019.

_____. **Lei Complementar nº 116, de 31 de julho de 2003**. Dispõe sobre o Imposto Sobre Serviços de Qualquer Natureza, de competência dos Municípios e do Distrito Federal, e dá outras providências. Brasília. 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp116.htm. Acesso em: 29 jun. 2019.

_____. **Lei Complementar nº 157, de 29 de dezembro de 2016**. Brasília. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp157.htm>. Acesso em: 30 jun. 2019.

_____. **Lei nº 4.680, de 18 de junho de 1965**. Dispõe sobre o exercício da profissão de Publicitário e de Agenciador de Propaganda e dá outras providências. Brasília. 1965. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L4680.htm>. Acesso em: 29 jun. 2019.

_____. **Lei nº 5.869, de 11 de janeiro de 1973**. Institui o Código de Processo Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L5869compilada.htm>. Acesso em: 20 nov. 2019.

_____. **Lei nº 7.232, em 29 de outubro de 1984**. Brasília: DOU, 30 out. 1984. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L7232.htm>. Acesso em: 10 fev. 2019.

_____. **Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: DOU, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 20 fev. 2019.

_____. **Lei nº 8.245, de 18 de outubro de 1991**. Brasília: DOU de 21 out. 1991. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8245.htm>. Acesso em: 11 fev. 2019.

_____. **Lei nº 9.099, de 26 de setembro de 1995**. Brasília: DOU, 27 set. 1995. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9099.htm>. Acesso em: 12 fev. 2019.

_____. **Lei nº 9.800, de 26 de maio de 1999**. Brasília: DOU, de 27 jun. 1999. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9800.htm>. Acesso em: 12 fev. 2019.

_____. **Lei nº 10.259, de 12 de julho de 2001**. Brasília: DOU, de 13 jul. 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10259.htm>. Acesso em: 12 fev. 2019.

_____. **Lei n° 10.358, de 27 de dezembro de 2001**. Brasília: DOU, de 28 dez. 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/leis_2001/L10358.htm>. Acesso em: 13 fev. 2019.

_____. Código Civil. **Lei nº 10.406, de 10 de janeiro de 2002**. 3 ed. São Paulo: EDIPRO, 2019.

_____. **Lei nº 11.280, de 16 de fevereiro de 2006.** Brasília: DOU, 17 fev. 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11280.htm>. Acesso em: 13 fev. 2019.

_____. **Lei nº 11.341, de 07 de agosto de 2006**. Brasília: DOU, 08 fev. 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11341.htm>. Acesso em: 20 fev. 2019.

_____. **Lei nº 11.382, de 06 de dezembro de 2006**. Brasília: DOU, 07 dez. 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11382.htm>. Acesso em: 20 fev. 2019.

_____. **Lei nº 11.419, de 19 de dezembro de 2006**. Brasília: DOU, 20 dez. 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11382.htm>. Acesso em: 19 fev. 2019.

_____. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasil. In: Vade mecum acadêmico de direito Rideel. 22 ed. São Paulo: Rideel. 2016.

_____. **Lei nº 12.737/2012, de 30 de novembro de 2012**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 fev. 2019.

_____. **Lei 12.414, de 09 de junho de 2011**. Brasília: DOU, 10 jun. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 20 fev. 2019.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Diário Oficial da União de 24 abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 fev. 2019.

_____. Código de Processo Civil. **Lei nº 13.105, de 16 de março de 2015**. In: Vade mecum acadêmico de direito Rideel. 22 ed. São Paulo: Rideel. 2016.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Diário Oficial da União, de 15 ago. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 16 ago. 2018.

_____. **Lei nº 13.853/2019, de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Diário Oficial da União – DOU, de 09 set. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>. Acesso em: 09 out. 2019.

_____. **Medida Provisória nº 2.200-1, de 27 de julho de 2001**. Brasília: DOU, 28 jul. 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-1.htm>. Acesso em: 12 fev. 2019.

_____. **Medida Provisória nº 869/2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília: Senado Federal, 28 dez. 2018. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>. Acesso em: 20 mar. 2019.

_____. Ministério do Desenvolvimento, Planejamento e Gestão. **PORTARIA Nº 107, DE 2 DE MAIO DE 2018** Aprova a versão revisada da Estratégia de Governança Digital da Administração Pública Federal para o período 2016-2019 e atribui à Secretaria de Tecnologia da Informação e Comunicação a competência que especifica. Brasília, 2018. Disponível em:<http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=03/05/2018&jornal=515&pagina=70>. Acesso em: 09 jul. 2018.

_____. Câmara dos Deputados do Brasil. **Projeto de Lei nº 5.762/2019.** Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022. Brasília: Câmara dos Deputados do Brasil, 2019. Disponível em: <

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704>. Acesso em: 07 abr 2020.

_____. Senado Federal. **Projeto de Lei nº 1.179/2020** - Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). Brasília: Senado Federal, 2020. Disponível em: < https://www2.camara.leg.br/legin/fed/lei/2019/lei-13853-8-julho-2019-788785-norma-pl.html>. Acesso em: 07 abr. 2020.

_____. **Resolução 185/2013, do CNJ**. Disponível em: <http://www.cnj.jus.br/busca-atos-adm?documento=2492>. Acesso em: 25 out. 2017.

CANADÁ. **Carta Canadense de Direitos e Liberdades de 1982**. Ottawa: Parlamento do Canadá: 1982. Disponível em: < https://laws-lois.justice.gc.ca/eng/const/page-15.html#h-38>. Acesso em: 29 mar. 2019.

CHILE. **Constitución Política de la República de Chile de 1980**. Santiago: Biblioteca del Congreso Nacional, 2018. Disponível em: < https://www.leychile.cl/Navegar?idNorma=242302>. Acesso em: 29 mar. 2019.

CHILE. **Ley 19.628**. Santiago: Diario Oficial, 1999. Disponível em: < https://www.leychile.cl/Navegar?idLey=19628>. Acesso em: 20 mar. 2019.

COLÔMBIA. **Constituição Política da Colômbia, de 06 de julho de 1991**. Bogotá: Gaceta Constitucional, n 114, de 4 jul. 1991. Disponível em: < http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf>. Acesso em: 29 mar. 2019.

_____. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. **Decreto nº 1.377/2013**. Bogotá: Diário Oficial, 2013. Disponível em: <https://www.mintic.gov.co/portal/604/w3-article-4274.html>. Acesso em: 29 mar. 2019.

_____. **Ley nº 1.273/2009**. Bogotá: Diário Oficial, 2009. Disponível em: < http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf>. Acesso em: 29 mar. 2019.

_____. **Ley nº 1.581/2012**. Bogotá: Diario Oficial: 2012. Disponível em: < https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>. Acesso em: 29 mar. 2019.

COMISSÃO INTERAMERICA DE DIREITOS HUMANOS. **Declaração Americana dos Direitos e Deveres do Homem**. Bogotá: CIDH, 1948. Disponível em: < https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htmAcesso em: 20 dez. 2018.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem de 1950**. Roma: Jornal do Conselho da Europa, 1950. Disponível em: < http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=536&lID=4>. Acesso em: 20 dez. 2018.

CONSELHO DA UNIÃO EUROPEIA – CUE. PARLAMENTO EUROPEU. **Convenção de Bruxelas de 1968 relativa à Competência Jurisdicional e à Execução de Decisões em matéria civil e comercial**. Bruxelas: Jornal Oficial das Comunidades Europeias, 1968. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:41968A0927(01)&from=PT>. Acesso em: 20 jun. 2019.

CONSELHO DA UNIÃO EUROPEIA - CUE. PARLAMENTO EUROPEU. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE - Regulamento Geral sobre a Proteção de Dados**. Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL>. Acesso em: 17 mar. 2019.

CONSELHO EUROPEU. PARLAMENTO EUROPEU. **Diretiva 95/46/CE**. Bruxelas: Jornal Oficial da União Europeia, 1995. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046 >. Acesso em: 20 fev. 2019.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. **Resolução 185, de 18/12/2013**. Brasília: CNJ, 2013. Disponível em: < http://www.cnj.jus.br/busca-atos-adm?documento=2492>. Acesso em: 20 fev. 2019.

COREIA DO SUL. **Constituição da República da Coreia, de 12 de julho de 1948**. Seul: Assembleia Nacional da Coreia do Sul, 1948. Disponível em: < https://archive.is/20120710041912/http://korea.assembly.go.kr/res/low_01_read.jsp?boardid=1000000035>. Acesso em: 29 mar. 2019.

EGITO. **Constituição da República Árabe do Egito, de 18 de janeiro de 2014.** Zurique: WIPO, 2014. Disponível em: < https://wipolex.wipo.int/en/legislation/details/15307> Acesso em: 29 mar. 2019.

EQUADOR. **Constituição da República do Equador, de 11 de agosto de 1998**. Quito: Diario Oficial, 1998. Disponível em: < https://www.oas.org/juridico/mla/sp/ecu/sp_ecu-int-text-const.pdf>. Acesso em: 29 mar. 2019.

ESPANHA**. Constitución española de 1978**. Madri: Congreso de los Diputados, 1978. Disponível em: < https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229 >. Acesso em: 12 abr. 2019.

ESTADOS UNIDOS DA AMÉRICA – EUA. **Children's Online Privacy Protection Act - COPPA**. Washington D.C.: United States Congress, 1990. Disponível em: < https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>. Acesso em: 29 mar. 2019.

ESTADOS UNIDOS DA AMÉRICA - EUA. **Fourth Amendment for the United States Constitution**. Washington D.C. The United States Congress, 1792 Disponível em: < https://www.law.cornell.edu/constitution-conan/amendment-4>. Acesso em 15 nov. 2018.

ESTADOS UNIDOS DA AMÉRICA – EUA. **Health Insurance Portability and Accountability Act – HIPPA.** Washington D.C. The United States Congress, 1996.

Disponível em: <https://www.govinfo.gov/app/details/CRPT-104hrpt736/CRPT-104hrpt736>. Acesso em: 29 mar. 2019.

ESTADOS UNIDOS DA AMÉRICA - EUA. **Privacy Act (5 USC § 552a /1974) (US)**. Washington: The United States Congress, 1974. Disponível em: <https://www.justice.gov/opcl/file/844481/download>. Acesso em: 22 mar. 2019.

EUROPEAN COMISSION. **Commission Decision of 12 December 2011 on the reuse of Commission documents – 833/2011**. Bruxelas: European Comission, 2011. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011D0833&from=en>. Acesso em: 20 abr. 2019.

EUROPEAN COMISSION. **Contribution Of The European Structural And Investment Funds To The 10 Commission Priorities Digital Single Market.** Bruxelas: European Comission, 2015. Disponível em: <https://ec.europa.eu/commission/publications/contribution-european-structural-and-investment-funds-digital-single-market_pt>. Acesso em: 23 mar. 2019.

HUNGRIA. **Act LXIII of 1992 on the protection of personal data and the publicity of data of public interest.** Budapeste: Parlamento Húngaro, 1992. Disponível em: <http://www.aip-bg.org/lichnidanni/pdf/hungary.pdf>. Acesso em: 20 mar. 2019.

INGLATERRA. **Data Protection Act, of 1988**. Londres: Parlamento Inglês, 1988. Disponível em: < https://www.legislation.gov.uk/ukpga/1998/29/contents >. Acesso em: 26 mar. 2019.

INGLATERRA. **Data Protection Act, of 2018**. Londres: Parlamento Inglês, 2018. Disponível em: <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>. Acesso em: 26 mar. 2019.

JAPÃO. **Constituição do Japão de 3 de novembro de 1946**. Tóquio: Arquivos Nacionais Japoneses, 1949. Disponível em: < http://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html>. Acesso em: 29 mar. 2019.

MÉXICO. **Ley Federal De Protección De Datos Personales En Posesión De Los Particulares– LFPDPPP.** Cidade do México – D.F.: Câmara dos Deputados, 2010. Disponível em: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>. Acesso em: 29 mar. 2019.

NIGÉRIA. **Constituição da República Federal da Nigéria, de 29 de maio de 1999**. Abuja: Assembleia Nacional, 1999. Disponível em: < https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Nigeria_Constitution_1999_en.pdf>. Acesso em: 29 mar. 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. **Declaração Universal dos Direitos do Homem, de 1948**. Nova Iorque: ONU, 1948. Disponível em: <https://nacoesunidas.org/direitoshumanos/declaracao/>. Acesso em: 15 dez. 2018.

PARAGUAI. **Constituição da República do Paraguai, de 20 de junho de 1992**. Assunção: Convenção Nacional Constituinte, 1992. Disponível em: < http://jme.gov.py/transito/leyes/1992.html> Acesso em: 29 mar. 2019.

PERU. **Constituição Política da República do Peru: 31 de outubro de 1993.** 11 ed. Lima: Ministerio de Justicia y Derechos Humanos, 2016. Disponível em: < http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/Const-peru-oficial.pdf>. Acesso em: 29 mar. 2019.

PERU. **Ley N° 29733 de Protección de Datos Personales del Perú**. Lima: Congreso de la Republica, 201. Disponível em: < http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf>. Acesso em: 29 mar. 2019.

PORTUGAL. **Constituição da República Portuguesa, de 25 de abril de 1976**. Coimbra: Almedina, 2013.

SUIÇA**. Constituição Federal da Confederação Suíça, de 18 de abril de 1999**. Berna: Assembleia Federal, 1999. Disponível em: <https://www.admin.ch/opc/fr/classified-compilation/19995395/index.html>. Acesso em: 22 mar. 2019.

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. **CC 41728/PR.** Relator: Ministro FERNANDO GONÇALVES, Data de Julgamento: 11/05/2005, S2 - SEGUNDA SEÇÃO, Data de Publicação: --> DJ 18/05/2005 p. 158. Brasília: STJ, DJ 18/05/2005. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/7228194/conflito-de-competencia-cc-41728-pr-2004-0029596-5/inteiro-teor-12975193?ref=juris-tabs>. Acesso em: 20 mar. 2019.

SUPREMO TRIBUNAL FEDERAL – STF. **ACO 1.295 AgR-segundo**. Rel. Min. Dias Toffoli. Brasília: STF, 2010. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=617537 >. Acesso em: 20 mar. 2019.

SUPREMO TRIBUNAL FEDERAL – STF. **ACO 1.342 AgRg/RJ**. Rel. Min. Marco Aurélio. Brasília: STF, 2010. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=618977>. Acesso em: 20 mar. 2019.

SUPREMO TRIBUNAL FEDERAL – STF. **Súmula nº 363**. Súmula da Jurisprudência Predominante do Supremo Tribunal Federal – Anexo ao Regimento Interno. Edição: Imprensa Nacional, 1964, p. 157. In: Vade Mecum Saraiva. 24 ed. atual e ampl. São Paulo: Saraiva, 2017.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Luxemburgo: Jornal Oficial da União Europeia, p. 326 – 391, 2000. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.POR > Acesso em: 15 mar. 2019

UNIÃO EUROPEIA. **Directive 95/46/EC of the European Parliament and of the Council**. Luxemburgo: Official Journal L 281, p. 031, 23 nov. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> Acesso em: 27 fev. 2019.

URUGUAI. **Constituição da República Oriental do Uruguay de 1997**. Barcelona: Red Ediciones, 2016.

URUGUAI. **Lei de Proteção de Dados Pessoais (Lei 18.331 / 2008)**. Montevidéu: Registro Nacional de Leyes y Decretos, 2008. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em: 29 mar. 2019.

2. Obras científicas, literárias e publicações institucionais oficiais

ANGEHRN, A.A. **Designing mature internet business strategies: the ICDT model**. European Management Journal. Oxford, Blackwell, v. 15, n.4, p.361-369, Aug. 1997.

ARAÚJO, Luiz I. de A. **Curso de direito dos conflitos interespaciais.** Rio de Janeiro: Forense, 2002.

ARAÚJO, Nádia de. **Contratos internacionais:** autonomia da vontade, mercosul e convenções internacionais. 4. Ed. Rio de Janeiro: Renovar, 2009.

ASAI, Toshio. **Japan Data Protection Law: A Practical Guide in Comparison With GDPR**. Tokio: Amazon E-book Kindle, 2018.

ASHMARINA, Svetlana. MESQUITA, Anabela. VOCHOZKA, Marek. **Digital Transformation of the Economy**: Challenges, Trends and New Opportunities. Berlim: Springer, 2019.

ASSOCIAÇÃO DOS DIREITOS CIVIS – ADC. **El Sistema de Protección de Datos Personales en América Latina** - Oportunidades y desafíos para los derechos humanos. São Paulo: ADC/Creative Commons, 2016. 40 p. Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf>. Acesso em: 01 abr. 2019.

ASSOCIAÇÃO DOS DIREITOS CIVIS – ADC. **Políticas de Protección de Datos Personales en las Empresas de Telecomunicaciones**: Estudio de casos de Argentina, Brasil, Chile e México. São Paulo: ADC/Creative Commons, 2016. Disponível em: < https://adcdigital.org.ar/wp-content/uploads/2017/02/Politicas-proteccion-datos-personales-telcos.pdf>. Acesso em: 01 abr. 2019.

BAMBERGER, Keineth A. MULLIGAN, Deirdre K. **Privacy on the Ground**: Driving Corporate Behavior in the United States and Europe. Cambridge: The MIT Press, 2015.

BANDEIRA DE MELLO, Celso Antônio. **Curso de direito administrativo**. 32. ed. São Paulo: Malheiros Editores, 2015.

BAPTISTA LUZ ADVOGADOS. **Proteção de dados a legislação vigente no Brasil**. São Paulo: Baptista Luz Advogados, 2017. Disponível em: <http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf>. Acesso em: 20 jan. 2019.

BARROSO, Luís R. **Curso de Direito Constitucional contemporâneo.** 8 ed. São Paulo: SaraivaJur, 2019.

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução: Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001, 255p.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008.

BECKER, Friedrich H. **Datenschutzgrundverordnung – DSGV O / General Data Protection Regulation - GDPR**: Synopse: Deutsch-Englisch / Synopsis: German-English. Steisslingen: Amazon E-book Kindle, 2018.

BELL, Daniel. **O Advento da Sociedade Pós-Industrial.** São Paulo: Cultrix, 1973.

BENJAMIN, Antônio H. V.; MARQUES, Claudia L.; BESSA, Leonardo R. **Manual de Direito do Consumidor.** 8 ed. São Paulo: Revista dos Tribunais, 2017. 560 p.

BIONI, Bruno, R. **Proteção de Dados Pessoais** - A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2018.

BITTAR, EDUARDO C.B. **Metodologia da pesquisa jurídica**: teoria e prática da monografia para os cursos de direito. 15ª ed. São Paulo: Saraiva, 2017.

BLANKE, Hermann Joseff. PERLINGEIRO, Ricardo. **The Right of Access to Public Information**: An International Comparative Legal Survey. Berlim: Springer Verlag, 2018.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BOBBIO, Norberto. **Da estrutura à função**: novos estudos de teoria do Direito. Barueri: Manole, 2007.

BOFF Salete O. FORTES, Vinícius B. FREITAS, Cinthia O. de A. **Proteção de Dados e Privacidade** – Do Direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lúmen Juris, 2018.

BOSTROM, Nick. **Superintelligence: Paths, Dangers, Strategies**. 1ª ed. Oxford, RU: Oxford University Press, 2014.328 p.

BOURQUE, Linda B; CLARK, Virginia A. **Processing Data**: The Survey Example (Quantitative Applications in the Social Sciences). Thousand Oaks, CA: Sage Publications Inc., 2006.

BRASIL. Ministério do Desenvolvimento, Planejamento e Gestão. **Estratégia Brasileira para a Transformação Digital (E-DIGITAL).** Brasília, 2018. 107 p. Disponível em:< https://www.governodigital.gov.br/documentos-e-arquivos/estrategiadigital.pdf/view>. Acesso em: 09 jul. 2018.

BUCCI, Maria Paula Dallari. Notas para uma metodologia jurídica de análise de políticas públicas. In **Políticas públicas**: possibilidades e limites - organizado por Cristiana Fortini, Júlio César dos Santos Esteves e Maria Teresa Fonseca Dias. Belo Horizonte: Fórum, 2008. p. 225-260 Disponível em:

<https://edisciplinas.usp.br/pluginfile.php/1706397/mod_resource/content/1/mpaula_notas%20para%20uma%20metodologia%20juridica%20de%20analise%20de%20pp.pdf>. Acesso em: 12 dez 2018.

CABRAL, Arnoldo Souza. YONEYAMA, Takashi. **Economia digital**. São Paulo: Atlas, 2001. 246 p.

CANOTILHO, José. J. Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Almedina, 2002. p. 257-266.

CAPURRO, R.; HJØRLAND, B. **O conceito de informação**. *Perspectivas em Ciência da Informação*, Belo Horizonte, v.12, n.1, p.148-207, jan./abr. 2007. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/54/47>. Acesso em: 18 out. 2017.

CARVALHO, André C. de. LORENA, Ana Carolina. **Introdução à Computação** - Hardware, Software e Dados. Rio de Janeiro: LTC Editora, 2016.

CISCO. **Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper**. San Jose, CA: Cisco, 2019. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf>. Acesso em: 21 mar. 2019.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. **Justiça em Números 2017**: ano-base 2016/Conselho Nacional de Justiça. Anual. Brasília: CNJ, 2017. 188p.

CONSELHO NACIONAL DE JUSTIÇA – CNJ. **Relatório Justiça em Números 2018**: ano-base: 2017/Conselho Nacional de Justiça – Brasília: CNJ, 2018.

DIDIER JUNIOR, Fredie; ZANETI JUNIOR, Hermes. **Curso de direito processual civil** - v. 4: processo coletivo. 11. ed. Salvador: JusPODIVM, 2017. 543 p.

DINAMARCO, Cândido Rangel. LOPES, Bruno V. C. **Instituições de direito processual civil**. 7 ed. São Paulo: Malheiros, 2016.

DINAMARCO, Cândido Rangel. **Teoria geral do novo processo civil.** São Paulo: Malheiros, 2016.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 18ª ed. São Paulo: Atlas, 2005.

DÖRR, Dieter. WEAVER, Russell W**. Perspectives on Privacy**: Increasing Regulation in the USA, Canada, Australia and European Countries. Berlim: De Gruyter, 2014.

DUGGAL, Pavan. **Cyberlaw Approaches For Africa.** Nova Deli: Saakshar Law Publications, 2018.

ECO, Umberto. **Como se faz uma tese**. São Paulo: Perspectiva, 2008, 21ª Edição.

FARIA, Renato V. MONTEIRO, Alexandre L. M. R. SILVEIRA, Ricardo M. **Tributação da Economia Digital**. Desafios no Brasil, Experiência Internacional e Novas Perspectivas. São Paulo: Saraiva, 2018.

FEILER, Lukas. **Information Security Law in the EU and the U.S**.: A Risk-Based Assessment of Regulatory Policies. Viena: Springer Verlag, 2012.

FRENCH, Carl. **Data Processing and Information Technology**. 10 ed. Londres: Thomson Learning, 1996.

GEIST, Michael. **Law, Privacy and Surveillance in Canada in the Post-Snowden Era (Law, Technology and Media).** Ottawa: University of Ottawa Press, 2015.

GLOBAL PARTNERS DIGITAL. **Travel Guide to the Digital World**: data protection for human rights defenders. Londres: Global Partners Digital & Creative Commons, 2018. 96 p. Disponível em: <https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf >. Acesso em: 16 out. 2019.

GOMES, Rodrigo D. de P. **Big Data:** Desafios à Tutela Da Pessoa Humana Na Sociedade Da Informação. Rio de Janeiro: Lúmen Juris, 2017.

GREENLEAF, Graham. **Asian Data Privacy Laws**: Trade & Human Rights Perspectives. Oxford: OUP Oxford, 2014.

GREGORIO, Carlos G. Protección de Datos Personales: Europa v Estados Unidos, todo un Dilema para América Latina. In: CONCHA CANTÚ, H.A., LÓPEZ-AYLLÓN, S. TACHER, Epelstein L. (editores) **Transparentar al Estado**: la Experiencia Mexicana de Acceso a la Información; sine Nomine et sine Loco. Cidade do México: Universidad Nacional Autónoma de Méxiko, 2004. 299 p.

HAUNTS, Stephen. **A Gentle Introduction to GDPR**: Resolving Compliance Challenges in Business. Liverpool: Amazon E-book Kindle: 2018.

HILBERT, Martin; LÓPEZ, Priscila. **The World's Technological Capacity to Store, Communicate, and Compute Information**. New York: Science, ed 332, p. 60-65, 2011. Disponível em: <https://www.researchgate.net/publication/49826525_The_World's_Technological_Capacity_to_Store_Communicate_and_Compute_Information>. Acesso em: 20 jan. 2019.

HÜBNER M. M. **Guia para elaboração de monografias e projetos de dissertação de mestrado e doutorado**. São Paulo: Pioneira, 1998.

HUDAK, Heather C. **Digital Data Security.** Nova York: Crabtree Publishing Company, 2016.

JELLINEK, Georg. **A Declaração Dos Direitos Do Homem E Do Cidadão** - Contribuição Para A História do Direito Constitucional Moderno. vol. 2. São Paulo: Atlas, 2015.

JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. São Paulo: Saraiva, 2005. p.39-45.

KAZEMI, Robert. **General Data Protection Regulation**. Hamburgo: Tredition, 2018.

KLOSEK, Jacqueline. **Data Privacy in the Information Age**. Westport: Praeger Publishers, 2000.

LAKATOS, Eva Maria, MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5ª ed. São Paulo: Atlas, 2003.

LAMY, Marcelo. **Metodologia da pesquisa jurídica**: técnicas de investigação, argumentação e redação. Rio de Janeiro: Elsevier, 2011.

LEITE, George Salomão; LEMOS, Ronaldo**. Marco civil da internet**. São Paulo: Atlas, 2014.

LIBERT, Barry. **The Big Data Revolution**. 1 ed. Nova Iorque: New Word City, 2014.

LORENZETTI, Ricardo L. Informática, *cyberlaw*, *e-commerce*. In: LUCCA, Newton de. FILHO, Adalberto S (Coords.). **Direito e internet** – aspectos jurídicos relevantes. 2 ed. São Paulo: Quartier Latin, 2005.

LYMAN, Peter; VARIAN, Hal R. **How Much Information 2003?**. Berkeley: UC Berkeley - School of Information Management and Systems, 2003. Disponível em: <>. Acesso em: 20 out. 2018.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MAGRANI, Eduardo. **Digital rights**: Latin America and the Caribbean / [Editor] Eduardo Magrani. – Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2017. 238 p.

MAKULILO, Alex B. **African Data Privacy Laws.** Viena: Springer Verlag, 2016.

MARQUES, Claudia Lima. **A nova crise do contrato: estudos sobre a nova teoria contratual**. São Paulo: Ed. RT, 2007.

MATTERN, Friedeman. **Algegenwärtige Datenverarbeitung** - Trends, Visionen, Auswirkungen. In: ROBNAGEL, Alexander, et. al. Berlim: Springer, 2008.

MCLEAN, David. **International Co-operation in civil and criminal laws.** Nova York: Oxford University Press: 2010.

MEADOWS, A. J. **A comunicação científica**. Brasília: Briquet de Lemos, 1999. p.35.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 25ª ed. São Paulo: Malheiros, 2000. p.95.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet, COELHO, Inocêncio. **Curso de direito constitucional**: São Paulo, SaraivaJur, 2018. 1.638 p.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, Inovação e Tecnologia**. vol. 1. São Paulo: Saraiva, 2015.

MENDES, Laura S. **Privacidade, Proteção de Dados e Defesa do Consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MISTRY, Jamshed; DHAVALE, Dillep. **Application of balanced scorecard in e-commerce environment.** Journal of Knowledge Globalization, v. 4, n. 2, p. 91-113, 2011.

MORAES, Alexandre de. **Direito Constitucional**. 34 ed. São Paulo: Atlas, 2018.

MORAIS, Fabíola V. Direito contratual na União Europeia e cláusulas contratuais gerais comunitárias. GOMES, Fábio Luiz (coord). *In:* **Direito Internacional:** perspectivas contemporâneas. São Paulo: Saraiva, 2010.

NADER, Paulo. **Introdução ao Estudo do Direito**. 39 ed., rev. e atual. Rio de Janeiro: Forense, 2017. 419 p.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Data Privacy, Ethics And Protection Guidance Note On Big Data For Achievement Of The 2030 Agenda**. Nova Iorque: e United Nations Development Group (UNDG), 2017.

_____. **International Data Responsibility Group Annual Report – 2017**. Nova Iorque: e United Nations Development Group (UNDG), 2017.

_____. INTERNATIONAL COMMUNICATION UNION – ITU. **Global Cybersecurity Index (GCI) 2018**. Genebra: ITU, 2017. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf>. Acesso em: 20 mar. 2019.

PERLINGEIRO, Ricardo. Justiça Administrativa No Brasil: uma jurisdição administrativa judicial, extrajudicial ou híbrida? In: **Revista CEJ**. Brasília, Ano XVIII, n. 62, p. 79-82, jan./abr., 2014. Disponível em: < http://www.jf.jus.br/ojs2/index.php/revcej/article/viewFile/1863/1815>. Acessoem: 20 mar. 2019.

PINHEIRO, Patrícia P. **Proteção de Dados Pessoais** - Comentários à Lei N. 13.709/2018 LGPD. São Paulo: Saraiva, 2018.

PINOCHET, Luis. **Tecnologia da Informação e Comunicação**. Rio de Janeiro: Elsevier, 2014.

PIRES, Adilson R. Interação econômica e soberania. GOMES, Fábio Luiz (coord). *In:* **Direito Internacional:** perspectivas contemporâneas. São Paulo: Saraiva, 2010.

PRIVACY INTERNATIONAL. **A Guide for Policy Engagement on Data Protection** – The Keys to Data Protection. Londres: Privacy International, 2018. 100 p. Disponível em: <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>. Acesso em: 16 out. 2019.

RAMALHO, David da S. **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Lisboa: Almedina, 2017.

RAMOS, Eduardo A. ANTUNES, André. VALLE, André B. do Valle. KISCHINEVKY, AndrÉ. **E-Commerce.** Rio de Janeiro: FGV Editora, 2014.

SARACEVIC, T. **Ciência da informação**: origem, evolução e relações. Perspectivas em Ciência da Informação, Belo Horizonte, v. 1, n. 1. jan./jun. 1996. p.56.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**: uma Teoria Geral dos Direitos Fundamentais na Perspectiva Constitucional. 13ed. Porto Alegre: Livraria do Advogado Editora, 2018. 520 p.

SCHOLZ, Trebor. **Digital Labor**: The Internet as Playground and Factory. Londres: Routledge, 2012. 274 p.

SMITH, David R. **Digital Transmission Systems**. Alphen aan den Rijn, Netherlands: Kluwer International Publishers, 2003.

SOUZA, Carlos Affonso; LEMOS, Ronaldo **Marco civil da internet**: construção e aplicação / Carlos Affonso Souza e Ronaldo Lemos. Juiz de Fora: Editar Editora Associada Ltda, 2016.

STAPLETON, John J. **Security without Obscurity**: A Guide to Confidentiality, Authentication, and Integrity. Auerbach Publications, 2014. Boca Raton, FL: Auerbach Publications, 2014.

STRENGER, Irineu. **Direito Internacional Privado**. 5 ed. São Paulo: RTr, 2003.

TAPSCOTT, Don. **Economia Digital.** São Paulo: Macron Books, 1997.

TEIXEIRA, Tarcísio. **Curso de Direito e Processo Eletrônico** - Doutrina, Jurisprudência e Prática. São Paulo: Saraiva Jur, 2018.

TEIXEIRA, Tarcísio. **Marco civil da internet:** comentado. São Paulo: Almeidina, 2016.

UNIVERSIDADE FEDERAL FLUMINENSE – UFF. **Apresentação de trabalhos monográficos de conclusão de curso** / Universidade Federal Fluminense. – 10. ed. rev. e atualizada por Estela dos Santos Abreu e José Carlos Abreu Teixeira. – Niterói: EdUFF, 2012.

VENOSA, Silvio de S. **Direito Civil**. Reais. 17 ed. vol 4. São Paulo: Atlas, 2016.

VIEIRA, Elianete. **O início da descoberta.** 1 ed. São Paulo: Scortecci, 2013.

VOIGT, Paul. BUSSCHE, Axel var der. **The EU General Data Protection Regulation (GDPR)**: A Practical Guide. Viena: Springer Verlag, 2018.

WALDFOGEL, Joel. PEITZ, Martin. **The Oxford Book of Digital Economy**. Nova York: William Morrow, 2012. 624 p.

WALTERS, Robert. TRAKMAN, Leon. ZELLER, Bruno. **Data Protection Law**: A Comparative Analysis of Asia-Pacific and European Approaches. Viena: Springer, 2019.

WAZLAWICK, Raul Sidnei. **História da Computação**. Rio de Janeiro: Elsevier, 2017.

WEBSTER, Frank. **Theories of the Information Society.** Cambridge: Routledge, 2002.

Este livro, fruto da Dissertação de Mestrado apresentada ao Programa de Pós-Graduação Justiça Administrativa, da Faculdade de Direito da Universidade Federal Fluminense, tem como objetivo identificar e compreender os aspectos contextuais, geracionais e normativos mais relevantes para a conformação do Regime Jurídico da Lei de Proteção de Dados Pessoais - LGPD no Brasil, à luz da implementação da Lei nº 13.709/2018. Com especial atenção voltada para os Direitos Humanos, o princípio da dignidade da pessoa humana, o direito constitucional fundamental à privacidade e os direitos à proteção de dados pessoais, à segurança digital e à autodeterminação informativa, a obra é ideal tanto para estudos nas áreas de graduação e pós-graduação,quanto para saciar as mentes curiosas, em relação às boas práticas cidadãs na titularidade de novos direitos, a serem exercidos e reconhecidos .

A contribuição pretendida também apresenta estudos interdisciplinares, contemplando temáticas que abordam, dentre outras, as taxonomias advindas da Ciência da Computação e da Informática, da Economia Digital, do Direito Constitucional em perspectiva comparada, o Direito Internacional Público e Privado e o Direito Administrativo, para verificar modalidades de exercício da jurisdição brasileira em demandas envolvendo a violação à proteção de dados pessoais, considerando possíveis conflitos de competência e o exercício jurisdicional transnacional (cross-border), quando da entrada em vigor da LGPD ou conforme as Leis de Proteção de Dados Pessoais estrangeiras, com o intuito de corresponder a uma necessidade coletiva de saber e aprender, visando à consolidação de uma infraestrutura social mais ética e capaz de fortalecer o Estado Constitucional Democrático, a dignidade da pessoa humana, a privacidade e a proteção de dados - como direitos fundamentais e inalienáveis, na Sociedade Globalizada da Informação.