UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

CLARA CORBAN BRITTO GUERRA

CLOUD COMPUTING E LGPD:
estudo sobre a aplicabilidade da Tese de Convergência de Bennett na proteção de dados pessoais

Recife
2023

CLARA CORBAN BRITTO GUERRA

CLOUD COMPUTING E LGPD:
estudo sobre a aplicabilidade da Tese de Convergência de Bennett na proteção de dados pessoais

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestra em Direito. Área de concentração: Transformações do Direito Privado. Linha de pesquisa: Direito Internacional e Globalização

Orientadora: Profa. Dra. Eugênia Cristina Nilsen Barza.

Recife
2023

Catalogação na fonte
Bibliotecária Ana Cristina Vieira, CRB-4/1736

G934c Guerra, Clara Corban Britto.
Cloud Computing e LGPD: estudo sobre a aplicabilidade da Tese de Convergência de Bennett na proteção de dados pessoais / Clara Corban Britto Guerra. -- Recife, 2023.
125 f.: il.

Orientadora: Profa. Dra. Eugênia Cristina Nilsen Ribeiro Barza.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. Centro de Ciências Jurídicas. Programa de Pós-Graduação em Direito, 2023.

Inclui referências.

1. Direito Internacional Privado. 2. Sociedade da Informação. 3. Direito à Privacidade. 4. Segurança dos dados. 5. Tecnologia da Informação. I. Barza, Eugênia Cristina Nilsen Ribeiro (Orientadora). II. Título.

340.9 CDD (22. ed.) UFPE (BSCCJ 2023-39)

CLARA CORBAN BRITTO GUERRA

CLOUD COMPUTING E LGPD:

estudo sobre a aplicabilidade da Tese de Convergência de Bennett na proteção de dados pessoais

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestra em Direito. Área de concentração: Transformações do Direito Privado. Linha de pesquisa: Direito Internacional e Globalização.

Aprovado em: 28/08/2023

BANCA EXAMINADORA

_____

Profa. Dra. Eugenia Cristina Nilsen Ribeiro Barza (Orientador)
Universidade Federal de Pernambuco - UFPE

_____

Prof. Dr. Aurélio Agostinho da Boâviagem (Examinador Interno)
Universidade Federal de Pernambuco - UFPE

_____

Profa. Dra. Wanilza Marques de Almeida Cerqueira Fortuna (Examinadora Externa)
Faculdade Frassinetti do Recife – FAFIRE

_____

Prof. Dr. Adelgício de Barros Correia Sobrinho (Examinador Externo)
Universidade Salgado de Oliveira - UNIVERSO

AGRADECIMENTOS

Aos meus pais por todo o apoio e amor que deles tive durante toda a minha jornada, não só acadêmica, mas também de vida.

Às minhas irmãs, Clarissa, Indira e Esther, por serem um exemplo de busca por conhecimento e amor para mim.

Ao meu tio, Lemuel Guerra, pelo apoio tanto acadêmico quanto emocional.

Ao meu companheiro Dales, por não ter me deixado desistir mesmo nos momentos mais difíceis e por acreditar na minha jornada acadêmica e profissional.

A minha querida orientadora Dra. Eugenia Barza. Não só pelo seu apoio, como também pelo aprendizado adquirido durante o processo de orientação, mas principalmente por acolher minhas demandas com gentileza.

Aos meus colegas de linha de pesquisa, Andréia; Débora; Luciana; Madson e Soraya pelas angústias e alegrias partilhadas durante a jornada de pós-graduação, mesmo que à distância.

Por fim, gostaria de agradecer aos funcionários da Pós-Graduação de Direito e também da UFPE. Toda a equipe de professores com os quais tive oportunidade de aprender sobre as ferramentas do Direito Internacional Privado e da Pesquisa Acadêmica, também aos servidores, aos funcionários da limpeza, coordenadores e secretários que possibilitam ao PPGD desenvolver suas atividades.

RESUMO

O tema deste trabalho será a ascensão da economia da informação e da proteção de dados pessoais segundo os parâmetros do Direito Internacional Privado. O objetivo proposto é observar como as inovações tecnológicas, a exemplo da computação em nuvem, criam demandas legislativas de proteção de dados no comércio internacional e provocam o movimento descrito por Bennett como Tese da Convergência de diretrizes em diversos ordenamentos nacionais como o brasileiro. Apresenta-se em que medida o proposto por Bennett se verifica em relação à regulamentação da proteção de dados levando em consideração a proposição da *Global Data Privacy* definida por Schwartz. Pontua-se como os serviços de computação em nuvem os quais contém transferências de dados transfronteiriços, a exemplo dos serviços de *AWS (Amazon Web Services)*, criam demandas normativas por lidarem com uma quantidade massiva de dados pessoais dos indivíduos e geram a necessidade da crescente tutela sobre o tema. Passa-se desde o papel das Organizações Internacionais — como a OCDE; UNIÃO EUROPEIA; UNCITRAL — até o papel das empresas transnacionais da tecnologia como a *Amazon* na criação das tendências legislativas sobre a proteção de dados no âmbito da *cloud computing*.

Palavras-chave: dados pessoais; computação em nuvem; convergência jurídica.

ABSTRACT

The theme of this work will be the rise of the information economy and the protection of personal data according to the parameters of Private International Law. The proposed objective is to observe how technological innovations, such as cloud computing, create legislative demands for data protection in international trade and provoke the movement described by Bennett as the Convergence Thesis of guidelines in various national legal systems such as Brazil's. It is presented to what extent Bennett's proposal is verified in relation to data protection regulation, taking into account the proposition of Global Data Privacy defined by Schwartz. It is pointed out how cloud computing services that contain cross-border data transfers, such as AWS (Amazon Web Services), create normative demands by dealing with a massive amount of personal data from individuals and generate the need for increasing protection on the subject. It goes from the role of International Organizations - such as OECD; EUROPEAN UNION; UNCITRAL - to the role of transnational technology companies such as Amazon in creating legislative trends on data protection in cloud computing.

Keywords: personal data; cloud computing; legal convergence.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
APPI	Act on the Protection of Personal Information
AWS	Amazon Web Services
AZ	Zona de Disponibilidade
BCR	Binding Corporate Rules
B2B	Business to Business
CCPA	The California Consumer Privacy Act
CDC	Código de Defesa do Consumidor
CJI	Comissão Jurídica Interamericana
CSP	Cloud Service Providers
EUA	Estados Unidos da América
ETN	Empresa Transnacional
FaaS	Function as a Service
GDPR	General Data Protection Regulation
GfK	Growth from Knowledge
IA	Inteligência Artificial
IaaS	Infrastructure as a Service
IBM	International Business Machines
IGOs	Organizações Governamentais Internacionais
IoT	Internet das Coisas
ITIL	Information Technology Infrastructure Library
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
LGPD	Lei Geral de Proteção de Dados
OCDE	Organization for Economic Cooperation and Development
OEA	Organização dos Estados Americanos
OI	Organização Internacional
OV	Organização Virtual
PaaS	Plataforma como Serviço
RTB	Race-To-The-Bottom Teory
SaaS	Software as a Service
SLA	Service Level Agreements

SLM	Service Level Managemen
SVoD	Subscription Video on Demand
UNCITRAL	United Nations Commission on International Trade Law
UE	União Europeia
UNIDROIT	Instituto Internacional para a Unificação do Direito Privado

SUMÁRIO

1 INTRODUÇÃO

O objetivo central deste trabalho é discutir a aplicabilidade da Tese de Convergência pensada por Bennett (1991) na ascensão da proteção de dados pessoais a partir da análise do paradigma computacional amplamente popularizado 'computação em nuvem', devido a natureza dotada de transferências de dados pessoais transfronteiriças.

Este estudo investigará de que maneiras a natureza transfronteiriça da proteção de dados pessoais contribui para a convergência jurídico internacional em torno do tema, considerando ordenamentos jurídicos de países distintos no atual cenário da crescente relevância da *internet* e dos meios computacionais em curso, com o objetivo de indagar se há o movimento de convergência normativa sobre o tema no ambiente jurídico internacional e também em diversos ordenamentos nacionais, como o brasileiro.

A presente dissertação de mestrado também investigará como o desenvolvimento tecnológico molda o ambiente jurídico internacional e nacional, focalizando-se na força do mercado de trocas comerciais internacionais através de instituições transnacionais, para estabelecer padrões normativos.

O método utilizado será o hipotético-dedutivo, através da técnica da análise documental, que observará o protagonismo da temática da proteção de dados pessoais na convergência jurídica internacional e na harmonização das normas internacionais sobre o tema. Com este fim serão consultados de documentos oficiais e públicos, como leis, regulamentos e diretivas para discutir como a proteção de dados pessoais incidiu globalmente nos serviços de 'computação em nuvem', devido à natureza descentralizada, focalizando-se como a presença deste serviço oferecido por *Big Tech's* a exemplo da *Amazon,* se comporta diante das legislações nacionais, a partir da análise do caso brasileiro.

O fenômeno de aproximação jurídica ocorre através da necessidade de adequação imposta por Organizações Internacionais (OI's), relevantes em termos globais, como requisito aos membros e possíveis candidatos a fazerem parte dela, o que exige dos países a participação no diálogo político e comercial dentro dos parâmetros da chamada *Global Data Privacy*.

Organizações internacionais como a OCDE, União Europeia e UNCITRAL criam a necessidade da adequação interna dos países membros como resposta à força normativa advinda principalmente das empresas transnacionais (ETNs) que oferecem serviços cibernéticos e são dominantes tanto nos países desenvolvidos quanto nos em

desenvolvimento, as denominadas *Big Tech's.*

A análise aqui proposta está estruturada em três capítulos. No primeiro capítulo apresentamos uma seção inicial de revisão da literatura sobre a consolidação da sociedade da informação, caracterizada pelo crescente compartilhamento de dados na rede mundial de computadores, tomando como base os postulados propostos por Zuboff (2019), Bioni (2020) e Doneda (2011), sendo o último um dos precursores da análise da consolidação da sociedade da informação e da construção da proteção de dados como direito fundamental ramificado da privacidade.

Ainda no referido capítulo, será abordado como o conceito de privacidade surgiu no âmbito jurídico e seu aperfeiçoamento desde a década de 1960, na qual a proteção de dados pessoais tem seus primeiros marcos regulatórios, até os anos 2000. Também será descrita a importância da União Europeia ao legislar sobre o tema, a partir da focalização da perspectiva da *Global Data Privacy,* elaborada por Schatwz (2019), que explica a relevância normativa da União Europeia, e a julga fundamental para a posterior compreensão do fenômeno da convergência, como proposta por Bennett (1991).

No segundo capítulo abordamos inicialmente o funcionamento dos serviços de computação em nuvem, entendidos como uma rede compartilhada e de recursos configuráveis com natureza complexa e inovadora. Sob a perspectiva de Lynn *et al.* (2020), serão focalizadas questões relativas à segurança e proteção à privacidade concernentes aos serviços fornecidos via *internet*, e os seus principais riscos à privacidade neles implicados.

O capítulo será finalizado com a análise normativa dos impactos da tecnologia computacional no Direito Internacional Privado contratual. Para este fim, será observado o documento publicado pela Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), o *Notes on the Main Issues of Cloud Computing Contracts*, que versa sobre a regulação dos contratos de ‘computação em nuvem’.

No terceiro e último capítulo, a partir de autores como De Oliveira (2008), argumentamos sobre a harmonização de normas no âmbito internacional. Também apresentamos Bennett (1991), principal propositor da tese da Convergência, focada na proteção de dados. Busca-se neste capítulo analisar como o ambiente jurídico internacional, através de organizações internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e União Europeia, influenciaram na construção da Lei Geral de Proteção de Dados brasileira (LGPD).

Será discutido como a *Amazon*, que oferece os serviços de *software* por servidores localizados em países distintos dos lugares nos quais estão sendo disponibilizados, respondeu

às exigências da LGPD para atuar no Brasil. O plano de fundo desta discussão final busca discutir o papel das Empresas Transnacionais (ETNs), principalmente as *Big Tech's,* e das Organizações Internacionais no processo de configuração de modos de convergência jurídica.

Por fim, tenta-se responder às seguintes indagações: há de fato uma tendência das Organizações Internacionais convergem na seara de proteção de dados por conta da natureza transfronteiriça que a caracteriza? Em que medida o movimento por parte das empresas transnacionais (ETNs) de se adequarem aos padrões nacionais responde às imposições jurídico Internacionais feitas pelas Organizações Internacionais (OI's) e às necessidades/interesses das *Big Tech's* de transitarem entre ordenamentos nacionais distintos sem a necessidade de grandes modificações internas para adequar-se às peculiaridades legais de cada Estado nacional?

2 A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS

2.1 Da ascensão da sociedade da informação na interface com o direito à privacidade

Refletir sobre o papel da tecnologia e sua influência no desenvolvimento da humanidade direciona a discussão para a habilidade da raça humana de modificar a realidade material à sua volta. Álvaro Vieira Pinto (2008), ao discorrer sobre o tema no âmbito filosófico, afirma que o aprimoramento das técnicas traduz a necessidade do indivíduo de sanar as divergências entre seu desejo, fruto das necessidades inerentes à existência, e a realidade.

Pinto (2008) entende como ineficaz a elaboração do conceito da técnica sem a devida observância aos modos de produção correspondentes ao recorte na risca temporal na qual a sociedade se encontra e diz que somente "se apenas admitirmos a transformação dos produtos sem condicioná-la a transformação daquilo que os produz estaremos no puro terreno da ficção" (PINTO, 2008, p. 49). Conclui ele que a força necessária para fazer emergir a produção de novas tecnologias é a estrutura tanto econômica quanto política atuante em determinado momento e espacialidade.

A partir do entendimento da importância das forças políticas e econômicas no desenvolvimento da técnica, a Revolução Industrial pode ser considerada o marco histórico a partir do qual os esforços dedicados ao aprimoramento tecnológico passaram a ter crescente destaque na conformação da indústria e, consequentemente, nas dinâmicas sociais a ela referidas.

Ao versar sobre a ideia do progresso tecnológico e a relação do mesmo com as forças econômicas e produtivas, Zuboff (2019) diferencia a existência de novas técnicas, a exemplo das algorítmicas predominantes contemporaneamente, da estrutura do capitalismo de vigilância. No início da sua obra, Zuboff se preocupa em dispor a definição do conceito por ela elaborado e retratado ao longo dos seus escritos. Sendo assim, o capitalismo de vigilância é definido ainda nas páginas pré-textuais como:

> 1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura

> que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX […] (ZUBOFF, 2019, s.p.).

A especificidade do capitalismo de vigilância se constitui nas diversas tecnologias digitais e algorítmicas. Porém, Zuboff (2019) enfatiza que não é suficiente defini-lo unicamente mediante o advento de uma delas. Isto porque a modalidade do capitalismo pensada pela autora as vê como ferramenta essencial para emergir, e as usa apenas como potencializadoras do seu inerente proposito fim.

Dito isto, Zuboff (2019) afirma que o capitalismo de vigilância se apoia em algoritmos, mas não é definido por algoritmos. Eles são as ferramentas criadas para atender a interesses específicos que respondem e surgem das demandas do capital, semelhante as demais inovações técnicas advindas dos tempos modernos.

A imperatividade do capital sobre o mero desejo ao progresso é exemplificada por Zuboff (2019) através do trecho de uma carta escrita por Thomas Edison — inventor responsável pelo aperfeiçoamento da lampada elétrica em 1880[1] — a Henry Ford, o precursor da chamada Linha de Montagem, desenvolvida em 1909[2]. Na referida carta, Edison expõe sua preocupação com os possíveis rumos das invenções impulsionadoras da nova civilização industrial pela qual passava a época. Explica Zuboff:

> Edison e Ford compreenderam que a vida moral da civilização industrial seria moldada pelas práticas de capitalismo que ascendiam ao poder na sua época. Acreditavam que os Estados Unidos e, por fim, o mundo, teriam de elaborar um capitalismo novo, mais racional, para evitar um futuro de sofrimento e conflito. Tudo, como sugeriu Edison, teria de ser reinventado: novas tecnologias, é verdade, mas estas teriam de refletir novas maneiras de entender e satisfazer as necessidades das pessoas; um novo modelo econômico que pudesse transformar essas novas práticas em lucro; e um novo contrato social capaz de sustentar tudo isso (ZUBOFF, 2019, p. 28).

---

[1] [...] "Uma grande parte do valor de uma inovação é determinada pelo grau em que as pessoas podem entendê-la, acessá-la e integrá-la em suas vidas. O que significa que muitas tecnologias tornam-se valiosas para uma ampla gama de potenciais usuários somente após um conjunto de recursos complementares serem desenvolvidos. [...] a primeira “luz elétrica” foi inventada em 1809 por Humphry Davy, um químico Inglês, ela não se tornou prática até o desenvolvimento de bulbos, dentro do qual o arco de luz iria ser envolto (demonstrado pela primeira vez por James Bowman Lindsay em 1835), e bombas de vácuo para criar um vácuo dentro do bulbo (a bomba de mercúrio foi inventada por Herman Sprengel em 1875). Thomas Alva Edison construiu sobre o trabalho destes inventores anteriores quando, em 1880, inventou filamentos que permitiriam a luz queimar durante 1.200 horas” (GOMES; FERREIRA, 2018, p. 22).

[2] “Em 1909, Henry Ford teve a grande idéia que mudou o pensamento da indústria contemporânea, propagando-se até os dias de hoje. […] A indústria da época foi revolucionada com a aplicação da ideia de Henry, novos conceitos surgiram na indústria, são alguns: produção em massa, pontos de montagem, estoques intermediários, etc. Em meados daquele século a GM já produzia automóveis em larga escala, e nos anos que seguiram a morte de Henry, a GM já possuía máquinas automatizadas por relés. No entanto, a programação das máquinas era extremamente complexa, com a instalação de painéis e cabines de controle com centenas destes dispositivos mecânicos, o que exigia grande interconectividade e muita energia, isso sem mencionar outros problemas estruturais como cabeamento e vida útil das relés” (LIMA; SILVEIRA, 2003, p 16).

Atualmente, a partir do século XXI, as preocupações descritas acima parecem se concretizar veementemente. A sobreposição dos interesses mercadológicos e de lucro sobre as atividades industriais revelam-se ainda mais pertinentes com o advento de tecnologias digitais, com a presença constante da inovação e de suas imprevisibilidades.

De algoritmos de inteligência artificial à supressão da capacidade do consumidor de escolher sem a presença de estatísticas algorítmicas em plano de fundo no ambiente virtual, é clara e demanda atenção social e intelectual a vulnerabilidade da privacidade do indivíduo na sociedade da informação, dentre outros direitos, tais como os de acesso e de transparência.

Pode-se entender a relação entre a criação de tecnologias e os interesses de setores e políticos específicos quando se analisa o contexto que deu origem ao computador. Durante a Segunda Guerra Mundial — entre 1939 e 1945 — foi desenvolvida a Máquina de Turing. Na época, a criação, nomeada em homenagem ao seu inventor, Alan Turing, foi financiada pelo governo inglês. O engenho possuía estrutura basilar dos computadores de propósito geral[3], utilizados até hoje, e foi imprescindível à decodificação da Máquina ENIGMA[4], usada pelos alemães para transmitir mensagens sobre operações de guerra, um dos fatores que permitiu a vitória dos Aliados.

Além de alcançar a finalidade inicial planejada — decodificar a ENIGMA — a invenção iniciou uma mudança de paradigma na maneira como a informação era armazenada, sendo essencial para o desenvolvimento da tecnologia computacional utilizada atualmente. A partir da Máquina de Turing, os computadores foram desenvolvidos seguindo um processo de crescente sofisticação.

Décadas mais tarde, a ferramenta criada por Turing em ambiente militar se popularizou graças à criação e disseminação da *internet*. Segundo Abbate (2000), em menos de trinta anos, a *internet* foi de uma rede única experimental para uma rede interconectada entre diversos computadores em localidades distintas. Oriunda do período da Guerra Fria e

---

[3] "Os analisadores diferenciais ou computadores de propósito geral, GPAC, (do inglês General-Purpose Analog Computer) utilizam uma arquitetura baseada na interligação de blocos funcionais para criar a equação diferencial desejada. Podem ser caracterizados como modelos matemáticos em que a ideia central é resolver EDOs usando combinações dos blocos de integradores e somadores [1], [3], [8], [15]. […] As operações básicas que compõem os blocos básicos do GPAC são: integrar, somar e multiplicar por constante. Além dessas operações, o dispositivo deve ser capaz de gerar constantes e as principais funções simples, como as polinomiais (FERNANDES, 2022, p. 8)".

[4] "A máquina Enigma era uma máquina de codificação desenvolvida nos anos da Segunda Guerra Mundial e é usada em operações pelas forças armadas alemãs para comunicações codificadas. Seu suposto benefício era que a máquina poderia ser configurada em 150 quintilhões (1,58 × 1020) maneiras diferentes e mesmo se você havia interceptado uma mensagem cifrada e possuía uma máquina Enigma, se você não soubesse como configurar a máquina para descriptografia, ainda levaria até o fim do universo e além antes que você pudesse experimentar todas as configurações possíveis e encontrar o certo" (de "The Story of Computing (English Edition)" por John Dermot Turing).

desenvolvida a partir do projeto ARPANET, foi amplamente desenvolvida nos Estados Unidos. O referido autor comenta que:

> Embora o *design* da Internet tenha vindo da comunidade internacional de pesquisa de computadores, a implementação real foi feita sob os auspícios dos militares dos EUA. Ramos operacionais das forças armadas começaram a usar a ARPANET durante a década de 1970 e outras agências do Departamento de Defesa além da ARPA se envolveram (com certa relutância) no gerenciamento da rede. O Departamento de Defesa desempenharia muitos papéis no surgimento da Internet: financiando pesquisa e desenvolvimento, transferindo tecnologia para forças operacionais, usando seus recursos financeiros para moldar o mercado comercial de produtos de rede e exercendo controle gerencial sobre a ARPANET e seus comunidade de usuários (ABBATE, 2000, p. 143).

Abbate (2000) aponta duas decisões fundamentais para a internet ser disponibilizada e popularizada entre os 'civis'. A primeira delas foi a separação dos servidores destinados aos dois grupos que primeiro tiveram acesso ao protótipo da rede internacional de computadores conhecida hoje: os acadêmicos e os militares. A necessidade de separação surgiu da preocupação com a prática de publicar arquivos por parte dos academicistas. Para os militares, a publicização de servidores nos quais também ficavam informações confidenciais poderia gerar vulnerabilidades à segurança nacional.

O novo arranjo resultou nos ambientes de redes distintas, a MILNET e a ARPANET. Segundo Abbate (2000), a partir desta separação, a ARPANET se tornou uma rede voltada para a pesquisa e dominada por universidades, o que facilitou a transferência para o público ordinário, enquanto a MILNET se munia da confidencialidade necessária ao meio militar. A segunda medida foi a de comercializar a tecnologia que possibilita as redes de conexão à internet, o que resultou no aumento dos investimentos para seu aprimoramento.

Os impactos advindos da configuração do ciberespaço planetário, com a popularização dos computadores — ocorrida principalmente a partir dos anos 80 segundo Abbate (2000) — podem ser ilustrados pela mudança na sua função: de ferramenta para realizar cálculos para um meio de comunicação e de operações comerciais. Com o aprimoramento da capacidade de armazenamento computacional, arquivos diversos — escritos; imagéticos; informações pessoais — que eram guardados de maneira física, ocupavam muito espaço e eram de difícil manuseio passaram a ser compactados em arquivos digitais.

Além do aumento da capacidade de armazenamento de dados em *hardwares*, com a *internet* houve também a facilitação da transferência de arquivos entre computadores. Antes disso, "uma pessoa que desejasse transferir informações geralmente precisava carregar algum meio de armazenamento físico, tais como rolos de fitas magnéticas ou uma pilha de cartões

perfurados, sendo estes transportados de uma máquina para outra"[5] (ABBATE, 2000, p. 147).

Zuboff (2019) menciona que a consequência da digitalização de informações produzidas e armazenadas antes nos espaços físicos e não computacionais, gerou a tendência de maior produção de informações digitais, levando a humanidade a dobrar seu montante de arquivos produzidos e armazenados com uma velocidade que aumenta ao passar dos anos de maneira diretamente proporcional ao refinamento das tecnologias, explica:

> Em 1986, apenas 1% da informação do mundo era digitalizada e 25% em 2000. Em 2013, o progresso de digitalização e datificação (a aplicação de software que permite a computadores e algoritmos processar e analisar dados brutos), combinado a novas e mais baratas tecnologias de armazenamento, convertia 98% da informação mundial em formato digital (ZUBOFF, 2019, p. 230).

Houve também excedência na capacidade de processar esse montante de informações e a necessidade de desenvolver técnicas capazes de manusear e traduzir os dados coletados em cada operação realizada pelos usuários no uso *online.* Isso permitiu o tratamento algorítmico dos dados, que pode ser entendido como uma espécie de 'tradução', já que é a partir dele que é possível a transformação dos muitos dados binários coletados em aplicativos *online* diversos em informação sobre os usuários e seus hábitos.

É relevante para o eficiente desenvolvimento do presente trabalho o prévio esclarecimento do termo 'usuário'. A palavra será utilizada para denominar os indivíduos que acessam o ambiente virtual, através da conexão *online,* via dispositivos eletrônicos diversos, tais como os *smartphones*, *smartwatches*, *tablets*, computadores portáteis ou não, dentre outros.

Neste contexto, o termo remete ao *status* que engloba não só a atividade que a pessoa desempenha como consumidor dos serviços e produtos fornecidos *online*, mas também ao papel ativo no qual a relação com os aplicativos virtuais a coloca. De acordo com Aldé (2011), existe um acordo tácito que define uma função coprotagonista, que o caracteriza como mais do que um só consumidor, explica:

> O próprio termo "usuário" embute alguns acordos tácitos sobre o papel ativo de quem se conecta à rede tanto quanto a mídias de massa, remete a uma perspectiva passiva da ideia de interação com a mídia. Características técnicas da Internet, como conectividade, interatividade, horizontalidade e publicabilidade, poderiam alçar o internauta a um papel cognitivo inédito nos meios de comunicação de larga escala, da qual participa não mais apenas como consumidor, mas coprotagonista (ALDÉ, 2011, p. 28).

[5] Tradução livre do original: "A person who wanted to transfer information between computers usually had to carry some physical storage medium, such as a reel of magnetic tape or a stack of punch cards, from one machine to the other".

A enorme capacidade de armazenamento de dados aliada ao desenvolvimento de técnicas cada vez mais complexas de análise e manuseio transformou os dados pessoais dos usuários *online* em informações relevantes e passíveis de monetização. A comercialização de informações tornou-se relevante para as empresas que os utilizam para publicidade direcionada; otimização de conteúdos *on demand*; e até a serviços especializados de transferência de dados para terceiros. Zuboff exemplifica:

> […] os algoritmos do Google, derivados do superávit, selecionam e ordenam resultados de busca, e os algoritmos do Facebook, derivados do superávit, selecionam e ordenam o conteúdo de seu Feed de Notícias. Em ambos os casos, pesquisadores têm revelado que essas manipulações refletem os objetivos comerciais de cada corporação (ZUBOFF, 2019, p.218).

Há por parte das empresas de tecnologia que lideram o mercado atual um forte investimento na diversificação da monetização dos dados pessoais dos usuários de serviços *online,* tanto na busca por aprimoramento dos algoritmos de tratamento de dados pessoais até estudos de mercado para encontrar meios eficazes de diversificar os dados coletados. Adiciona-se a isso uma evidente e inevitável vulnerabilidade da privacidade dos titulares, acompanhada da consequente dificuldade de uma atuação jurídica eficaz.

A constante alternância e velocidade que caracterizam os avanços tecnológicos digitais e algoritmos demanda do Direito uma adaptabilidade normativa sem precedentes. Os legisladores lidam com os desafios da mudança das percepções de fronteiras e territorialidades, fruto de um cenário no qual o trânsito do bem tutelado — os dados pessoais — acontece num ritmo de tal modo intenso que torna anacrônicas as tradicionais limitações transfronteiriças, colocando na ordem do dia dos legisladores e dos aplicadores da Lei a dificuldade existente muitas vezes de vincular as infrações ocorridas a um autor determinado.

Posto isto, para ser desenvolvido o conceito de proteção de dados pessoais no presente trabalho, faz-se imprescindível retomar sua origem, advinda do direito fundamental à privacidade. Todo o contexto de desenvolvimento tecnológico que desaguou na vulnerabilidade da privacidade do indivíduo gerou um movimento de ramificação e posteriormente, individualização da temática de proteção de dados pessoais, que a equiparou a um direito fundamental ‘parente’ da privacidade em si.

Doneda (2020) entende que devido às evoluções tecnológicas digitais ocorridas nas últimas cinco décadas, o direito à privacidade se tornou insuficiente diante das peculiaridades que a sociedade da informação trouxe consigo. O autor argumenta ainda que houve uma ‘elevação’ da importância da informação, que sempre foi um instrumento de poder na história da humanidade, devido ao aperfeiçoamento tecnológico capaz de a direcionar para fins cada

vez mais específicos.

A sociedade da Informação — consolidada a partir dos anos 90 — é marcada pelo constante uso de ferramentas *online* como Aplicativos e *Softwares,* as quais objetivam facilitar a execução de atividades cotidianas em diversas áreas da vida social. Estes serviços são majoritariamente fornecidos de maneira gratuita nos espaços digitais. Porém, ao contrário do que a maioria dos indivíduos acredita, há contraprestação, recorrentemente indecidida pelos usuários. Ela é realizada através da disponibilização de informações pessoais, que são fonte de monetização. Sobre esse ponto, vejamos o que afirma Saldanha:

> O que ocorre é que, embora seja muito útil essa utilização quase que ininterrupta da internet, seus usuários tornaram-se vulneráveis às empresas que fornecem esse tipo de serviço, pois elas passaram a deter um número massivo de seus dados. Diante de tal conjuntura, os dados pessoais passaram a ter grande valor para as empresas, já que essas passaram a poder prever o comportamento de seus usuários, de modo que podem criar propagandas extremamente direcionadas para certos tipos de público, assim como vender os dados obtidos para outras empresas e, assim, ganhar bastante dinheiro com a monetização de informações que, de fato, não lhes pertencem (SALDANHA, 2019, p. 16).

Corroborando com a importância da monetização de informações descrita acima, Bioni (2020) destaca que os dados pessoais coletados através dos dispositivos computacionais se transformaram em bens valiosos e centrais para o desenvolvimento da economia atual. O autor descreve que em cada época há um elemento primordial no qual o desenvolvimento do período se concentra. A informação, análoga aos dados pessoais assumiu este lugar. Explica:

> A informação é o (novo) elemento estruturante (re)organizador da sociedade, tal como o fizeram a plantações e criação de animais as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrária, industrial e pós-industrial (BIONI, 2020, p. 5).

As inovações tecnológicas estão diretamente relacionadas aos paradigmas que dominam o modelo econômico de determinada época. Como já descrito na presente seção, é através da força do capital e das demandas econômicas que o progresso da técnica é impulsionado. A partir da criação de uma nova técnica, os demais aspectos econômicos e sociais acabam por se moldar.

A sociedade da informação foi descrita como novo paradigma técnico-econômico, na obra publicada pelo Ministério de Ciência e Tecnologia Brasileiro em 2000 intitulada “Sociedade informacional: Livro Verde”. O título faz referência a “Tempo Morto e Outros Tempos”, obra de Gilberto Freyre e relaciona no prefácio a temática retratada com a característica incompleta e experimental descrita na obra de Freyre “nunca […] plenamente maduro, nem nas idéias, nem no estilo, mas sempre verde, incompleto, experimental”

(TAKAHASHI, 2000, p.6). Ao retratar a recente disseminação dos meios de comunicação em massa em solos brasileiros, Takahashi define a sociedade da informação da seguinte forma:

> É um fenômeno global, com elevado potencial transformador das atividades sociais e econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infraestrutura de informações disponível. É também acentuada sua dimensão político-econômica, decorrente da contribuição da infra-estrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos. Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades (TAKAHASHI, 2000, p.28).

Takahashi (2000) apontou a ascensão da sociedade da informação como consequência da interrelação entre os três seguintes fenômenos: a convergência tecnológica; a dinâmica da indústria; e a conectividade internacional. O primeiro feito é descrito a partir da capacidade da digitalização de vários tipos de informação e mídias variadas: "a computação (a informática e suas aplicações), as comunicações (transmissão e recepção de dados, voz, imagens *etc*.) e os conteúdos (livros, filmes, pinturas, fotografias, música *etc*)" (TAKAHASHI, 2000, p. 28).

O segundo fenômeno é a dinâmica da indústria, que popularizou a aquisição de computadores através da diminuição dos custos de produção — que geralmente desencadeia a diminuição do preço de mercado — e do investimento em *designs* voltados para a otimização do manuseamento dos computadores, o que os tornou menores e crescentemente mais manuseáveis.

O terceiro ponto que gerou a ascensão da sociedade da informação, de acordo com Takahashi (2000), foi a popularização da *internet* e a conectividade internacional por ela permitida: "no curto período de oito anos, a *Internet* se disseminou por praticamente todo o mundo, propiciando conectividade a países até então fora de redes, substituindo outras tecnologias (*Bitnet*, *Fidonet etc.*) mais antigas" (TAKAHASHI, 2000, p. 28).

A partir do reconhecimento da importância da criação respectiva dos computadores e da *internet* para a consolidação da sociedade da informação, é essencial para observar a ascensão da proteção de dados pessoais, reconhecer que o surgimento de novas técnicas e instrumentos já eram dotadas de impactos sobre o funcionamento da sociedade e do Direito. Sobre o tema:

> São precisamente certas transformações sociais e certas inovações técnicas que fazem surgir novas exigências, imprevisíveis e inexequíveis antes que essas transformações e inovações tivessem ocorrido. Isso nos traz uma ulterior confirmação da sociabilidade, ou da não-naturalidade, desses direitos (BOBBIO, 2004, p. 37).

O desenvolvimento tecnológico e sua incidência sobre as relações sociais e jurídicas geram exigências que muitas vezes são dotadas de uma imprevisibilidade não natural, mas fruto das demandas ulteriores que as criam. Para traduzir as possíveis consequências da utilização das inovações tecnológicas, sua imprevisibilidade e artificialidade — já que são criadas pela própria humanidade — Doneda (2020) usa a metáfora do Golem, um ser mitológico:

> O Golem, criatura da mitologia hebraica, é um humanoide de argila, feito pelo homem; sua força e poder crescem a cada dia. Ele segue as ordens do seu criador, auxilia-o, mas é um pouco tolo e inconsciente da sua força: é capaz, se não for bem comandado, de destruir seu próprio senhor (DONEDA, 2020, posição 853).

A técnica, assim como o Golem, tem um caráter transformador potencial projetado com intencionalidade, porém controlável somente até certo ponto. Ambos — o Golem e o desenvolvimento tecnológico — são criações humanas com objetivo último de lhes servir, mas que possuem uma força desconhecida até mesmo pelo seu próprio 'criador'. Fato que resulta num perigo iminente caso não sejam devidamente administrados.

Zuboff (2019) reforça a ideia de imprevisibilidade da tecnologia e argumenta que diante das inovações tecnológicas, faltam precedentes do uso e dos possíveis impactos advindos da sua utilização. A autora supracitada também afirma que essa repentinidade é acompanhada de uma orientação econômica e política que dá prévia intenção e guia os objetivos específicos da indústria, através da ciência, para alcançar os fins de demandas geralmente mercadológicas, políticas e bélicas.

Nesse ambiente novo e marcado pela velocidade e escopo das transformações observadas, o caminho da proteção de dados pessoais pode ser entendido a partir da investigação do direito à privacidade. Para isto, é importante revisitar um dos registros pioneiros sobre a importância da privacidade para o ser humano moderno, discutida em um ensaio de Louis D. Brandeis e Samuel D. Warren, em 1890, fruto do impacto da popularização de uma inovação técnica da época, a fotografia, intitulado "O direito à privacidade".

No referido ensaio, a necessidade que o indivíduo tem à vida privada é ressaltada na máxima que define a privacidade como "o direito de estar só"[6]. Os autores também apontam a importância da mutabilidade do Direito, que deve corresponder às demandas da sociedade e do tempo, sob pena, caso não o faça, de servir inadequadamente à sociedade:

---

[6] Passagem originalmente da obra do juiz Thomas Cooley, datada de 1873. "The right to one's person may be said to be a right of complete immunity: to be let alone,[…]". (COOLEY, Thomas McIntyre. The Elements of Torts. Gale: Yale Law School Library, 2010).

> A intensidade e a complexidade da vida, acompanhando o avanço da civilização, tornaram necessário um afastamento do mundo, e o homem, sob a influência fustigante da cultura, tornou-se mais sensível à publicidade, de modo que a solidão e a privacidade se tornaram mais essenciais para o indivíduo (BRANDEIS & WARREN, 1890, p. 5)[7].

Doneda (2011) aponta que o texto publicado em 1890 foi motivado pela exposição, sem autorização, de registros sobre o casamento da filha de um dos autores, em um jornal da época. Este fato motivou Samuel Warren, que se preparava para assumir o cargo de juiz da Suprema Corte Americana, a construir, com Brandeis, também juiz, a argumentação sobre a privacidade como um direito imaterial.

No ensaio supracitado, a proteção à intimidade e à vida privada foi equiparada à integridade física, definida como um bem jurídico. A divulgação não autorizada de informações sigilosas foi apontada como causa de feridas emocionais que poderiam ser equiparadas à dor e aos efeitos de uma lesão corporal, dando origem ao reconhecimento do direito à privacidade e ao controle da informação sobre si que se desenvolveria ao longo do século XX.

Além do ensaio escrito por Warren e Brandeis em 1890, extremamente necessário para o desenvolvimento da literatura jurídica sobre a privacidade, é relevante mencionar o *Caso de Semayne*[8]. Esse julgamento ocorreu na Inglaterra, no século XVII, e foi importante para a até então lenta construção do direito individual à privacidade. Schleehauf (2021) afirma a influência da decisão sentencial que contou com a famosa expressão "a casa de todo mundo é para si seu castelo e fortaleza" (SCHLEEHAUF, 2021, s.p.)[9] sobre a *Commom Law* inglesa e para a legislação dos Estados Unidos.

A privacidade é pauta nos Estados Unidos também nas emendas adicionais ao *Bill of Rights,* advinda da preocupação com a invasão à privacidade pelo governo pós-Independência. Schleehauf (2021) aponta que a importância histórica do Caso Semayne e destaca que sua influência jurídica fez parte da elaboração da Quarta Emenda à Constituição Americana, caracterizada pela limitação das investigações de autoridades na propriedade privada dos indivíduos.

---

[7] Tradução livre do original: "The intensity and complexity of life, accompanying the advance of civilization, made it necessary to withdraw from the world, and man, under the stinging influence of culture, became more sensitive to publicity, so that solitude and privacy have become more essential for the individual".

[8] De acordo com Schleehaulf (2021), o caso ocorreu na Inglaterra do século XVII, no ano de 1604. É considerada uma decisão histórica para a construção do conceito de inviolabilidade do lar e posteriormente da privacidade. Nele, houve a decisão no Tribunal do King's Bench em favor do réu, Sr. Richard Gresham, que defendeu o direito de recusar a entrada em sua propriedade, para que fosse aplicada a lei em seu desfavor. Disponível em: <https://lawfully.usq.edu.au/tag/semaynes-case/#_ednref3>.

[9] Tradução livre do original: "the house of everyone is to him as his castle and fortress".

Há destaque à privacidade nas emendas três, quatro e cinco que determinavam, *in verbis "*(3ª) a proteção do lar contra a invasão de soldados a mando do governo, (4ª) limitações a buscas arbitrárias do governo e (5ª) garantia do indivíduo de não testemunhar sobre informações que possam incriminá-lo" (SAMPAIO, 2021, p. 19).

No século XIX, os Estados Unidos se debruçaram sobre a tutela da privacidade a partir das demandas que surgiram à época, em resposta ao controle governamental principalmente com a prática da realização de censos populacionais a partir do ano de 1860 junto a preocupação com o sigilo das correspondências.

Sampaio (2020) destaca decisões baseadas principalmente na terceira emenda e também na recorrência de casos jurídicos em defesa à privacidade. Dentre eles, o autor destaca:

> Alguns *cases* vitais para a construção da privacidade naquele país de tradição jurídica da *common law:* (i) *Boyd v. United States*, 1886, em que a Corte prestigiou a liberdade e segurança pessoais e a propriedade privada em detrimento do interesse do Estado pela produção de provas documentais e (ii) *Union Pacific Railway v. Botsford,* 1891, em que se prestigiou a intimidade do corpo da demandante — o autor acrescenta, para o mesmo fim, o caso *De May v. Roberts*, 1881, em que um médico permitiu que "'um jovem solteiro' sem estudos em medicina" presenciasse um parto, ao que a Corte reconheceu que se tratava do momento mais íntimo e sagrado da demandante, o qual apenas convidados e pessoas realmente necessárias poderiam presenciar (SAMPAIO, 2021, p. 20).

Outros países também avançaram na propagação do tema da necessidade de proteger a privacidade dos indivíduos ao longo do século XX. A tendência ocorreu junto à "capacidade técnica de cada vez mais recolher, processar e utilizar a informação" (DONEDA, 2000 *apud* CANCELIER, 2017, p. 12).

O desenvolvimento dos veículos de informação e sua popularização[10], ocorridos ainda no século XIX, foi seguido da tendência dos ordenamentos jurídicos nacionais se adequarem às inovações técnicas surgidas. Neste contexto, Doneda (2011) aponta como "a proteção de dados mantém um nexo de continuidade com a disciplina normativa da privacidade, sendo sua herdeira" (DONEDA, 2011, p. 5).

No ambiente jurídico internacional, um dos primeiros registros da tutela ao direito à privacidade ocorreu em 1948, durante a IX Conferência Internacional Americana, ocorrida em Bogotá. A Declaração Americana dos Direitos e Deveres do Homem é considerada o primeiro instrumento internacional a tratar diretamente do tema da privacidade do indivíduo, tendo sido assinado na mencionada conferência, ao mesmo tempo, em que se criava a

[10] Aqui ainda não se fala do desenvolvimento das tecnologias computacionais, mas ainda do desenvolvimento de ferramentas que popularizaram a circulação de informações. Como a fotografia; o telefone e as máquinas de cópias utilizadas nos Jornais.

Organização dos Estados Americanos (OEA) (FERREIRA; PINHEIRO & MARQUES, 2022).

No mesmo ano, a privacidade também aparece sucintamente na Declaração Universal dos Direitos Humanos, documento elaborado por representantes da ONU em 1948, cujo objetivo foi compilar os direitos humanos. Nela está presente o direito à inviolabilidade da vida privada. Ferreira, Pinheiro e Marques (2022) apontam que a partir da década de 1940 houve a ocorrência de diversos marcos legislativos internacionais que seguem os supracitados, indicando o fortalecimento da proteção aos direitos individuais internacionalmente, estando entre eles os seguintes:

> Em 1950 ocorreu a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, cujo objetivo foi garantir a proteção e o desenvolvimento dos direitos e das liberdades fundamentais; em 1966, a Assembleia Geral das Nações Unidas aprovou o Pacto Internacional dos Direitos Civis e Políticos, que só entrou em vigor em 1976 ao obter o número mínimo de adesões, denotando sua amplitude mundial e reafirmando a Declaração Universal dos Direitos Humanos (FERREIRA; PINHEIRO; MARQUES, 2022, p. 158).

Os autores citam também o Pacto de San José da Costa Rica, firmado no ano de 1969 entre os países-membros da Organização dos Estados Americanos (OEA) e a importância do movimento internacional para a evolução da privacidade como um direito fundamental.

A tendência de desenvolver as legislações sobre privacidade para responder aos avanços referentes à informação e meios de comunicação, fundamenta o entendimento de que a proteção de dados pode ser vista como uma extensão ao direito à privacidade, e só justifica o movimento de consolidação do seu *status* de direito fundamental ocorrido a partir dos anos 2000.

Mendes (2014) afirma que a proteção de dados pessoais emerge no âmbito da sociedade da informação como uma possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos a serem causados pelo processamento ocorrido através dos meios digitais, sendo sua função não proteger os dados *per se*, mas à pessoa titular deles:

> As informações pessoais constituem-se em intermediários entre a pessoa e a sociedade. A personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Por se constituírem uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a liberdade e igualdade (MENDES, 2014, posição 568).

Devido às características associadas à personalidade e à individualidade da pessoa, a proteção de dados pessoais elevou sua importância e se estrutura hoje, nas primeiras décadas dos anos 2000, como um direito de caráter fundamental, amplamente discutido e aplicado. O

reconhecimento da importância da proteção de dados pessoais fica demonstrado na aderência de diversos países à tutela sobre o tema, os quais passaram a reconhecer a relevância do tema e a criar legislações específicas para o contemplar.

É exemplo disto o impacto da criação da *General Data Protection Regulation* (GDPR), regulamento da União Europeia, de 2016, no qual o Brasil se espelhou para criar sua Lei Geral de Proteção de Dados (Lei n. 12.709/2018); e também *The California Consumer Privacy Act* (CCPA), de 2020. Ao observarmos o contexto que levou ao supracitado é possível perceber a construção histórica composta por marcos legislativos relevantes à consolidação da proteção de dados pessoais, que passamos a focalizar na próxima seção.

2.2 As quatro Gerações da Proteção de Dados Pessoais e seus marcos regulatórios

A partir da análise geracional dos marcos regulatórios da proteção de dados pessoais descrita por Mendes (2014), será desenvolvida uma linha temporal, partindo da emergência pública da questão jurídica da proteção à privacidade até o momento no qual a primeira geração da proteção de dados pessoais iniciou — a década de 1970.

Doneda (2020) afirma que os casos jurídicos sobre privacidade que chegaram aos tribunais e ganharam notoriedade eram dotados de certo elitismo e traduziam uma preocupação exclusiva das classes abastadas. O autor menciona que tais casos versavam sobre a violação à privacidade de pessoas públicas e por conta disso ganhavam notoriedade. Dentre eles, está o caso de um casal membro da realeza inglesa. O autor supracitado fala sobre esse ponto:

> Podemos observar a crônica judiciária do passado referente à privacidade para deparar-nos com algo semelhante a um elenco de celebridades de cada época: na Inglaterra, o caso que é mencionado como o exórdio da matéria nos tribunais envolve os literatos Alexander Pope e Jonathan Swift e outro ainda o próprio casal real, Príncipe Albert e Rainha Vitória; na França, o primeiro caso que envolveu a vie privée foi o affaire Rachel, envolvendo a então famosa atriz francesa Elisa Rachel Félix; na Itália, dentre os primeiros julgados que envolvem (propriamente ou não) a privacidade, encontramos envolvidos nomes como o do tenor Enrico Caruso ou então do ditador Benito Mussolini e sua amante, Clara Petacci (DONEDA, 2020, p. 6).

É compreensível a presença de figuras públicas nos casos popularizados sobre a violação à privacidade. Porém, Doneda (2020) comenta que o fim da preocupação com a tutela do direito à privacidade como exclusiva de um grupo restrito de pessoas, deu lugar a consecutiva democratização do direito à privacidade, gerada pela mudança de relacionamento

Estado e Cidadão, que visava estabelecer correspondências entre o "panorama do *Welfare State*" e o aumento do fluxo informacional possibilitado pelos avanços tecnológicos.

Por muito tempo, o Estado ocupou um lugar de agente detentor das informações pessoais dos cidadãos. Isto se deu devido a sua detenção de capacidade técnica e também do poder de coação sobre os indivíduos, que nem chegavam a questionar o fato de precisarem fornecer suas informações. O Estado se apoiava na justificativa da busca estatal pela otimização das atividades públicas, mas também almejava, de maneira implícita, exercer um efetivo controle sobre a população e suas informações. Sobre esse explica:

> Os motivos são razoavelmente implícitos: basta verificar que um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população, do que decorre, por exemplo, a realização de censos e pesquisas, o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública, visando maior eficiência. Em relação ao controle, basta aceder às várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos (DONEDA, 2020, p.8).

O mesmo autor aponta os desdobramentos da tecnologia computacional na sociedade e direciona a discussão aos impactos da mesma no âmbito jurídico. Ele pontua que "a técnica, deixada livre, pode originar ou sustentar uma determinada tendência, passando a ser uma variável a ser levada em conta na dinâmica da sociedade" (DONEDA, 2020, p. 9). Ao exemplificar os desdobramentos da técnica como formadora de tendências jurídicas e administrativas, o autor descreve a prática inaugurada na década de 1960 pelo Departamento do Censo dos Estados Unidos.

Na década de 60, através da maior possibilidade de coleta, processamento e armazenamento de dados, os Estados Unidos deram início a prática de realizar pesquisas para a captação de informações pessoais dos seus cidadãos de maneira cada vez mais detalhada e invasiva. Doneda (2020, p. 9) relata que "se passou a exigir que os cidadãos que tivessem rompido seu matrimônio esclarecessem quais eram os motivos para tal".

Como consequência, delineou-se uma resistência da opinião popular, devido ao temor da utilização inédita da capacidade técnica e o receio de que o Estado exercesse de forma abusiva a detenção das informações dos cidadãos. Na época, a desconfiança da população cresceu devido ao projeto *National Data Center*[11], elaborado em 1965, que propunha a criação de um banco de dados unitário com informações diversas da população americana. O

[11] À medida que o projeto evoluiu, chegou-se à ideia de que o centro deveria conter dados de todos os cidadãos americanos em relação à data de nascimento, cidadania, registros de impostos, benefícios da previdência social, registro de espólio e, eventualmente, registros criminais. Procederam-se a inúmeras discussões nos meios de comunicação e a diversas audiências no Congresso (MENDES, 2014, p. 663).

poder público foi pressionado a fim de evitar o abuso de poder que pudesse advir desse cenário, resultando na extinção do projeto do *National Data Center.*

Em 1973, a proteção direcionada exclusivamente aos dados pessoais armazenados computacionalmente começa a ter destaque, a partir do Relatório realizado pela Secretaria de Saúde, Educação e Cuidados Básicos dos Estados Unidos (*Secretary of Health, Education, and Welfare*) sobre Sistemas Automatizados de Dados Pessoais[12]. No prefácio do Relatório é descrito o objetivo de tratar das possíveis mudanças que o uso de computadores para armazenamento de registros sobre as pessoas poderia acarretar à sociedade estadunidense.

Na Europa, ainda no século XX, a década de 1960 também foi marcada por discussões sobre o tema da proteção informacional. No ano de 1970, a importância dada à pauta também resultou em regulamentos específicos, estabelecidos em vários países do continente. Reafirmando a capacidade de criar tendências advindas do aprimoramento da técnica, as leis europeias surgiram em resposta à tentativa de abastecer as burocracias governamentais de informações pessoais sobre as populações nacionais, assim como ocorreu nos Estados Unidos em 1973.

Dentre as principais medidas criadas na Europa sobre proteção de dados, Mendes (2014) destaca as seguintes: a Lei do Estado Alemão de Hesse (1970); a Lei de Dados da Suécia (1973); e o Estatuto de Proteção de Dados da Alemanha (1977).

É possível perceber semelhanças entre as normas que caracterizam a primeira geração de proteção de dados não só pelo período no qual começaram a ser publicadas, mas também pela tendência de abarcar o possível controle Estatal advindo da detenção de técnicas de processamento e armazenamento de dados. O resultado foi a elaboração de textos legais com características estruturais que priorizavam regular os procedimentos técnicos[13] do tratamento dos dados pessoais captados pelos governos nacionais.

Havia nas normas da época o comum desejo de certificar que os titulares[14] estavam cientes do compartilhamento dos dados — para responder ao medo do descontrole da tecnologia amplamente discutido nos anos de 1960 — e a finalidade a que seriam destinados.

---

[12] EUA, HEW, "Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems" Julho, 1973 O relatório pode ser acessado na seguinte página: <http://epic.org/privacy/hew1973report>.

[13] Grande parte das leis da década de 70 tem uma perspectiva funcional e busca controlar os bancos de dados de forma *ex ante*, condicionando o seu funcionamento à licença prévia ou ao registro nos órgãos competentes. Ademais, ao priorizar o controle rígido dos procedimentos, as normas desse período deixaram para segundo plano a garantia do direito individual à privacidade, o que pode ser percebido a partir do próprio jargão técnico utilizado nas normas.

[14] Art. 5º, V, Lei n. 13.709/2018: "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018).

Observa-se uma tendência, tanto na Europa quanto nos EUA, de se instituírem bancos de dados de unitários por parte das administrações públicas e implementou-se a tendência da descentralização das informações dos cidadãos. Sobre esse ponto, explica:

> A transformação tecnológica possibilitou que unidades organizacionais pequenas do governo e da iniciativa privada utilizassem processamento de dados eletrônicos de forma descentralizada. Tal fato ocasionou a proliferação de bancos de dados existentes (MENDES, 2014, posição 676).

O desenvolvimento das tecnologias computacionais se intensificou e se popularizou, gerando a descentralização da técnica e o afastamento de um possível monopólio por parte do Estado. O temor antes direcionado principalmente ao controle estatal estendeu-se também às empresas privadas, o que resultou na aclaração das fragilidades consoantes à proteção de dados e à privacidade dos indivíduos no ambiente cibernético.

A partir da década de 1980, a proteção de dados pessoais passou novamente a ser fortemente associada ao direito à privacidade, que já possuía *status* de direito fundamental. Neste contexto, surgiu a necessidade de não apenas ter uma legislação específica e direcionada à proteção de dados pessoais, mas, de consolidá-la nos textos constitucionais, em paridade com a privacidade. Emerge então a segunda geração da proteção de dados.

Abandona-se a tentativa de regulamentar intensamente os procedimentos técnicos do fornecimento dos dados pessoais característico da geração anterior — na qual havia o objetivo de controlar os procedimentos tecnológicos de coleta dos dados (devido à inviabilidade de fazê-lo) — e passa-se a tratar especificamente da associação com o já consolidado direito à privacidade.

Como consequência desta vinculação à privacidade informacional — como passou a ser chamada — a regulamentação referida à garantia do direito à proteção de dados pessoais ganhou espaço nas constituições. Assim, a segunda geração de marcos regulatórios do direito à privacidade na internet reconheceu os riscos iminentes e visou fortalecer o direito à proteção de dados pessoais ao equipará-lo ao direito à inviolabilidade das correspondências e do lar do indivíduo, já garantidos constitucionalmente.

O movimento de consolidação da privacidade informacional como direito fundamental foi viabilizado através das normas de caráter procedimental presentes na década anterior. Doneda (2011) afirma que o conjunto de princípios contidos no *Fair Information Principles* são inspirados na Convenção de Estrasburgo e nos *Guidelines* da OCDE. Para o autor, estas regras possuem semelhança basilar e resume essa essência nos seguintes princípios:

> a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por

> meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
> b) Princípio da exatidão, pelo qual os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
> c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
> d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas desses dados;
> e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (DONEDA, 2011, p.100).

Doneda (2011) considerou os princípios acima como basilares para diversas leis; tratados; convenções e acordos entre agentes privados (OIs) e também parte fundamental à consolidação da matéria como direito fundamental em diversos ordenamentos jurídicos. São exemplos de constituições que incorporam em seus textos dispositivos específicos sobre proteção de dados pessoais inspirados nos *Fair Information Principles,* as Constituições Espanhola e Portuguesa[15].

Já no âmbito jurídico internacional privado, advindas do modelo de princípios supracitado, foram publicadas, no início da década de 1980, as "Diretrizes sobre Proteção da

---

[15] A Constituição Espanhola de 1978 contém os seguintes dispositivos:
Art. 18. — […] 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
[…] Art. 105. — […] b) La Ley regulará el acceso de los ciudadanos a los archivios y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.
A Constituição Portuguesa de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35:
"Artigo 35. (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 da 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 proteção, 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.
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 (DONEDA, 2011, p.101).

Privacidade e o Fluxo Transnacional de Informações Pessoais"[16], realizada pelo Comitê de Ministros da *Organization for Economic Cooperation and Development* (OECD), seguidas da Convenção de *Estrasburgo,* organizada "para fortalecer a proteção dos indivíduos com respeito ao processamento automático de dados pessoais", proclamada pelo Conselho Europeu, em 1981, assinada por 30 países.

De acordo com Filho (2013) às diretrizes previstas pela OCDE acabaram homogeneizando os padrões internos dos países signatários, que estabeleceram o compromisso de editarem leis nacionais sobre a privacidade de dados. O resultado foi além dos membros da OCDE e desencadeou a criação de um padrão normativo a ser seguido sobre o tema. Segundo Filho (2013), ao menos vinte países europeus que não eram membros foram influenciados pelo padrão OCDE de proteção de dados.

O *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* continha uma seção intitulada de "recomendações aos países membros", seguida do quesito intitulado "convites". Respectivamente, aos países-membros era requisitado o compromisso com a privacidade de dados a nível governamental; a observância da orientação recomendada no documento; e a disseminação das diretrizes aos setores público e privado internamente. Já aos países fora da OCDE era sugerida a colaboração — nas relações entre fronteiras — com as diretrizes seguidas pelos membros (OCDE, 1980).

A parte seis que antecede a sessão de implementação interna dos ordenamentos jurídicos discorre sobre a interoperabilidade[17] e cooperação internacional entre os países sobre privacidade. Nela é previsto que os países, além de legislar internamente sobre o tema da proteção à privacidade aos dados pessoais no ambiente informacional, devem adotar medidas para facilitar a cooperação transfronteiriça na aplicação da lei de privacidade e desenvolvam métricas comparáveis internacionalmente relacionadas à privacidade e fluxos transfronteiriços de dados pessoais (OCDE, 1980).

Além da importante atuação das OI's na temática, há ainda dois pontos de destaque na segunda geração de proteção de dados: o fortalecimento e a autonomia dada às autoridades administrativas encarregadas da proteção de dados, referida à discussão sobre a efetividade do consentimento do indivíduo na hora de fornecer suas informações pessoais:

---

[16] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", documento divulgado em 1o. de outubro de 1980 e atualizado em 2020 Disponível em: <https://www.oecd.org/digital/privacy/>.

[17] "A interoperabilidade pode ser entendida como uma característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente" (GOVERNO DIGITAL, 2020, sem página) Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade>.

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem que pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas? (VOLKSZÄHLUNG *apud* MENDES, 2O14, posição 701).

O período se encerra sem respostas para a indagação da possibilidade de coexistência do indivíduo conectado com a preservação da sua intimidade e com o mérito do início da consolidação da proteção de dados como parte do rol de direitos fundamentais, acoplada à privacidade. Também faz parte dos resultados das mudanças jurídicas do período a força exercida — através do viés principiológico — por organizações internacionais, tais como a OCDE.

A terceira geração de normas tem como marco inicial o Ato Normativo da Lei do Censo (*Volkszählungsgesetz*), promulgado em 25 de março de 1982 na Alemanha. Nele foi estabelecido o recenseamento geral da população através da coleta de dados sobre a profissão, moradia e local de trabalho, para fins estatísticos. O referido Censo tinha como objetivo:

> […] reunir, por meio de levantamentos feitos por pesquisadores credenciados, dados sobre o estágio do crescimento populacional, a distribuição espacial da população no território federal, sua composição segundo características demográficas e sociais, assim como também sobre sua atividade econômica. Tais dados sempre foram considerados indispensáveis para quaisquer decisões político-econômicas da União, Estados e municípios (MARTINS, 2016, p. 55).

O Censo anterior ao de 1983, feito em 1970, diferia do novo por conta do parágrafo nono, o qual previa "comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais" (MARTINS, 2016, p. 56). A possibilidade de comparação e transferência de dados entre diferentes repartições públicas gerou indignação nos indivíduos e fez com que a lei fosse alvo de diversas Reclamações Constitucionais.

O resultado foi a decisão do Tribunal Constitucional Alemão ocorrida em 1983, fruto da Reclamação Constitucional, declarando nulos os dispositivos da Lei do Censo que versavam sobre a comparação e trocas de dados junto às transmissões de dados para fins de execução administrativa. No mais, "essa decisão declarou como inconstitucional parte da lei do Censo da época e respaldada na Lei Fundamental de Bonn[18], reforçando a equiparação da

[18] Promulgada no dia 23 de maio de 1949, a Lei Fundamental de Bonn tem em seu texto o gérmen daquilo que vem sendo denominado de "neoconstitucionalismo", ou seja, de uma nova cultura jurídica. A Lei Fundamental constitui-se em paradigma da própria ideia do Estado constitucional de Direito: uma ordem constitucional em que se destacam características como: "(i) a importância dada aos princípios e valores como componentes elementares dos sistemas jurídicos constitucionalizados, (ii) a ponderação como método de interpretação/aplicação dos princípios e de resolução dos conflitos entre valores e bens constitucionais, (iii) a

proteção de dados às normas fundamentais" (MENDES, 2014, posição 705).

Segundo Martins (2016), a decisão foi tomada por conta do princípio da proporcionalidade e ao direito fundamental do indivíduo de decidir ele mesmo sobre a exibição e o uso de seus dados pessoais. A partir disso, ficou estabelecido que as restrições à 'autodeterminação sobre a informação' só podem ocorrer caso suponham o predominante interesse da coletividade, sendo necessário o estabelecimento por meio de bases legais e constitucionais, consoante aos requisitos existentes no Estado de Direito.

A expressão 'autodeterminação informacional' é caracterizada pela participação do indivíduo titular dos dados nas decisões sobre o seu tratamento[19], sendo disseminada nas normas da terceira geração — datada entre 1980 até meados da década de 1990 — as quais trouxeram o envolvimento completo e continuado do titular dos dados, desde a coleta ao armazenamento e transmissão das informações a seu respeito.

Mesmo com a tendência das leis da terceira geração de estabelecer processos de coleta e tratamento mais participativos dos titulares dos dados pessoais, na prática, estes ainda ocupavam um papel passivo quando ocorriam incidentes de vazamento das suas informações ou infrações. Isto ocorria não só pela falta de acessibilidade aos processos de tratamento dos dados pessoais, mas também pelas limitadas previsões punitivas contra infrações e referidas à reparação de danos.

A quarta geração das normas de proteção de dados não foca numa maneira de preencher as lacunas de responsabilidade atribuídas aos controladores[20]. Tais ausências causaram prejuízos aos titulares das informações. Com isto, reforçou-se a criação de dispositivos legais para fortalecer o papel dos indivíduos através da autodeterminação informacional e do aumento da responsabilização dos agentes de tratamento/manuseio de dados pessoais.

É exemplo de inspiração para as normas do período o "*no fault compensation",* criado na República Federativa da Alemanha, a partir da emenda à Lei Federal de Proteção de

---

compreensão da Constituição como norma que irradia efeitos por todo o ordenamento jurídico, condicionando toda a atividade jurídica e política dos poderes do Estado e até mesmo dos particulares em relações privadas, (iv) o protagonismo dos juízes em relação ao legislador na tarefa de interpretar a Constituição, e (v) a aceitação de alguma conexão entre Direito e Moral" (Embaixada da República Federal da Alemanha, 2009).

[19] Art. 4º, X, Lei n. 13.709/2018: 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).

[20] Art. 5º, VI, Lei n. 13.709/2018: "Controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018).

Isto é, o controlador é a empresa ou a pessoa que coordena e define como o dado pessoal será tratado, da coleta à eliminação. O controlador é a parte mais interessada no tratamento dos dados, e sobre quem recai a maior responsabilidade em relação ao tratamento.

Dados Alemã criada no ano de 1979. Essa normativa visava registrar "reclamações individuais a respeito da violação à proteção de dados pessoais" (MENDES, 2014, posição 727).

Houve também o reconhecimento da capacidade da circulação e uso de informações pessoais que vulnerabilizam as pessoas, a depender da sua natureza. Neste sentido, surgiram normas de proteção direcionada aos dados considerados sensíveis, proibindo de forma total ou parcial seu uso e tratamento[21].

Outra particularidade da quarta geração de marcos regulatório do tema do direito à proteção dos dados pessoas foi que, em diversos países, normas gerais sobre a proteção de dados passaram a ser complementadas via normas setoriais, criando assim uma melhor aplicabilidade das leis:

> Tal fato tem como finalidade ampliar a proteção do indivíduo nos diversos setores em que é possível o tratamento dos seus dados pessoais, de modo que a legislação possa contemplar as diversas especificidades setoriais existentes. Assim, na maioria dos países europeus, percebeu-se a existência de uma regulamentação geral sobre proteção de dados pessoais, mas com leis setoriais suplementares (MENDES, 2014, posição 737).

É marco normativo da quarta geração a Diretiva Europeia[22] de 1995 (95/46/EC) sobre proteção de dados pessoais. Adotada pela União Europeia, ela desenvolveu nos países-membros a participação dos titulares no processo de tratamento de dados, a responsabilidade dos agentes que derem causa ao dano sofrido pelo titular, garantindo reparação pelos prejuízos[23].

A partir da Diretiva n. 46, também foi dada atenção para os dados sensíveis[24],

---

[21] Considera-se "tratamento de dados" qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[22] "Formalmente aprovada em 24 de outubro de 1995, para entrar em vigor 03 anos depois, a Diretiva é um amplo texto legal em matéria de proteção de dados pessoais. Ela exige que cada país membro da União Europeia tenha uma agência ou comissário de proteção de dados, este último um agente estatal que supervisiona a aplicação dos princípios e leis de proteção à privacidade individual. Ela também exige que cada um deles edite leis sobre o processamento de dados pessoais. A Diretiva estabeleceu um prazo de 03 anos após a data de sua vigência, para que os países membros da União Européia adotou as medidas legislativas e regulamentares necessárias para incorporar suas regras no direito interno deles. Adiante fazemos uma análise mais detalhada do escopo e regras específicas fundamentais da Diretiva" (FILHO, 2013, sem página). Disponível em: <https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais>.

[23] Artigo 23- Responsabilidade:
1 . Os Estados-membros estabelecerão que qualquer pessoa que tenha sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido . 2 . O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável. Disponível em: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>.

[24] Considerando que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados

estabelecendo a necessidade do consenso expresso e informado do indivíduo para serem processados, *in verbis*:

> […] 33. Considerando que os dados susceptíveis, pela sua natureza, de pôr em causa as liberdades fundamentais ou o direito à vida privada só deverão ser tratados com o consentimento explícito da pessoa em causa ; que, no entanto, devem ser expressamente previstas derrogações a esta proibição no que respeita a necessidades específicas, designadamente quando o tratamento desses dados for efectuado com certas finalidades ligadas à saúde por pessoas sujeitas por lei à obrigação de segredo profissional ou para as actividades legítimas de certas associações ou fundações que tenham por objectivo permitir o exercício das liberdades fundamentais. (UNIÃO EUROPEIA,1995, p. 4).

O fato da Diretiva de 1995 recair sobre os Países-membros da União Europeia fez com que houvesse o fortalecimento das regras internas sobre o tema. Também aprimorou a responsabilidade dos agentes de tratamento para com os titulares de dados lesados. Há ainda na introdução da Diretiva o explícito interesse de aumentar o intercâmbio de dados pessoais entre empresas estabelecidas em diferentes Estados da Europa[25], clarificando o desejo do fortalecimento interno da UE diante das demais regiões do mundo, com base no uso regulado do intercâmbio de dados pessoais.

O Regulamento Geral de Proteção de Dados (GDPR), substituto da Diretiva Europeia de 1995, entrou em vigor vinte e três anos depois do seu antecessor. Pode ser considerado marco normativo introdutório da atual geração normativa de proteção de dados, a qual, sob a perspectiva histórico-evolutiva apresentada por Mendes (2014), pode ser chamada de ‘quinta geração’.

Datada a partir da segunda década dos anos 2000, a presente geração é caracterizada pela uniformização do regime de tratamento de dados em diversas regiões do globo. Nesta quinta geração a matéria de proteção de dados passou a ser “[…]requisito essencial para o bom funcionamento do Mercado Único” (LIMA, 2020, p. 314).

A partir do GDPR, que advém da criação da Estratégia para um Mercado Único

---

sensíveis em domínios como a saúde pública e a segurança social — em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença — e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia , estabelecer garantias adequadas e específicas para a protecção dos direitos fundamentais e da vida privada das pessoas;

[25] [...] (5) Considerando que a integração económica e social resultante do estabelecimento e funcionamento do mercado interno nos termos do artigo 7? A do Tratado irá necessariamente provocar um aumento sensível dos fluxos transfronteiras de dados pessoais entre todos os intervenientes, privados ou públicos, na vida económica e social dos Estados -membros; que o intercâmbio de dados pessoais entre empresas estabelecidas em diferentes Estados -membros tende a intensificar-se; que as administrações dos Estados-membros são chamadas, por força do direito comunitário, a colaborar e a trocar entre si dados pessoais a fim de poderem desempenhar as suas atribuições ou executar tarefas por conta de uma administração de outro Estado -membro, no âmbito do espaço sem fronteiras internas que o mercado interno constitui. Disponível em: <https://eur-lex.europa.eu/eli/dir/1995/46/oj>.

Digital, pela Comissão Europeia, lançada em 2015, e do contexto de crescentes e rápidas inovações tecnológicas, surge a tendência de aproximação jurídica de ordenamentos internos/nacionais diversos, de modo a otimizar o fluxo transfronteiriço dos dados pessoais digitalizados.

2.3 O Global Data Privacy e o Papel do Regulamento Geral de Proteção de Dados da União Europeia (2016/679)

A existência das diretrizes de organizações internacionais como a Convenção de *Strasbourg* e as *Guidelines* da OCDE foram fundamentais para a consolidação principiológica da proteção à privacidade informacional.

O Regulamento Geral de Proteção de Dados europeu (2016/679) foi essencial ao andamento da aproximação jurídico-normativa que acontece desde a segunda década dos anos 2000. Este fenômeno, caracterizado pela presença da União Europeia como agente de tendências normativas, foi nomeado por Schwartz (2019) de Privacidade Global de Dados (*Global Data Privacy*).

Idealizado em 2016 e com entrada em vigor no dia 25 de maio de 2018, o Regulamento Geral de Proteção de Dados da União Europeia não representava uma regra apenas para os Estados-membros da UE, mas, de acordo com Schwartz (2019), para o mundo inteiro. O dia da entrada em vigor da regulamentação foi chamado popularmente pela mídia e agentes do mercado de '*GDPR DAY'*.

O impacto foi tamanho para o comércio internacional e a consolidação da proteção de dados, que disseminou a privacidade informacional como direito fundamental em diversas regiões que ainda não o reconheciam como tal. O intitulado '*GDPR Day'* gerou impacto na maior potência econômica no mundo — Estados Unidos — como exemplifica Schwartz: "O secretário de Comércio dos EUA, Wilbur Ross, deu uma declaração dizendo que as empresas americanas já haviam investido bilhões de dólares para cumprir as novas regras da lei" (SCHWARTZ, 2019, p. 3).[26]

A partir da data de vigência muito se especulou sobre a aplicabilidade das sanções convertidas em multas e o impacto que seria causado ao diálogo comercial internacional das demais regiões com a União Europeia. Para Schwartz (2019) a União Europeia influenciou a maneira como os ordenamentos internos tratariam da privacidade de dados para além dos

[26] Tradução livre do original: "US Commerce Secretary Wilbur Ross issued a statement saying US companies have already invested billions of dollars to comply with the law's new rules".

países-membros.

Afirma Schawrtz (2019) que depois do GDPR vários países, inclusive de fora da UE, como o caso do Brasil, tomaram medidas de adequação. Para o autor, o regulamento gerou impactos no comportamento administrativo-estatal interno, transnacional e corporativo dos países membros e de terceiros interessados em manter diálogo comercial com a UE.

O Regulamento Europeu é considerado por Bioni e Mendes (2019) como o ponto de chegada do caminho jurídico legislativo da Europa sobre privacidade informacional. Para que a Diretiva de 1995 fosse sucedida pelo GDPR depois de tanto tempo vigente, houve a análise das lacunas que surgiram ao longo destas mais de duas décadas do século XXI. Dentre elas, destaca-se a "necessidade de uma abordagem mais consistente e uniforme da proteção de dados por todo o bloco econômico europeu" (BIONI; MENDES, 2019, p. 164).

Bioni e Mendes (2019) ainda afirmam que o objetivo da UE de constituir um regime jurídico cada vez mais uniforme e ter um mercado totalmente integrado divergia do proposto pela Diretiva n. 46/95, que dava maior autonomia aos países-membros. A Diretiva permitia, quando ponderado pelo país-membro como motivo de interesse público, a "autorização de estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social" (UNIÃO EUROPEIA,1995, p. 4).

Enquanto a Diretiva n. 95/46 em razão do gênero do qual faz parte[27] é caracterizada por ser um ato legislativo cuja função é de fixar um objetivo geral a ser seguido observados os critérios das legislações internas/nacionais, o Regulamento Europeu de 2016 possui natureza de ato legislativo vinculativo[28] O que o fez instantaneamente aplicável a todos os Estados-membros da União Europeia.

Com as demandas técnicas surgidas no período entre a publicação de ambas, a discussão sobre a proteção de dados se tornou crescentemente importante e foi vinculada ao objetivo geral da União Europeia de possuir um regime jurídico harmônico; uniforme e capaz

---

[27] "Uma diretiva é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. No entanto, cabe a cada país organizar as suas próprias leis para alcançar esses objetivos. Um exemplo é a diretiva da UE relativa aos plásticos de utilização única, que reduz o impacto de determinados plásticos de utilização única no ambiente, por exemplo, reduzindo ou mesmo proibindo a utilização de plásticos de utilização única, como pratos, palhinhas e copos para bebidas". Disponível em: [https://european-union.europa.eu/institutions-law-budget/law/types-legislation_p].

[28] "Para alcançar os objetivos estabelecidos nos Tratados, a UE adota diferentes tipos de atos legislativos. Alguns desses atos são vinculativos, outros não. Alguns são aplicáveis a todos os países da UE, outros apenas a alguns. […] Um regulamento é um ato legislativo vinculativo. Tem de ser integralmente aplicado em toda a UE. Por exemplo, quando o regulamento da UE relativo à supressão das tarifas de itinerância quando viaja na UE expirou em 2022, o Parlamento e o Conselho adotaram um novo regulamento para melhorar a clareza do regulamento anterior e garantir a aplicação por mais dez anos de uma abordagem comum às tarifas de itinerância" Disponível em: <https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt>.

de possibilitar um mercado digital uno consistente.

Ao descreverem o poder da União Europeia de influenciar legislações externas a sua, Goldsmith e Wu (2006) denominam o papel da UE como soberano efetivo[29]. Schwartz (2019) usa da expressão dos autores para complementar a afirmação da existência do que ele chama de 'privacidade global unilateral', resultado da combinação incomum do poder de mercado da Europa com a sua preocupação pioneira com a privacidade de seus cidadãos:

> Como a UE é um mercado altamente importante para empresas internacionais, muitas empresas não têm a opção de "sair totalmente do mercado europeu". Mesmo que pudessem, não desejam criar serviços separados para eles. Finalmente, porque a UE se preocupa muito com a privacidade e há muito tempo está envolvida na legislação de regras nesta área, seus regulamentos têm alcance extraterritorial: suas leis seguem as regras pessoais dados de residentes da UE sempre e onde quer que as informações sejam transferidas para fora da UE. O resultado, de acordo com Goldsmith e Wu, é que as empresas americanas optaram por se curvar ao "significativo poder de mercado" (SCHWARTZ, 2019, p. 7).[30]

Schwartz (2019) comenta a capacidade da UE de impor suas regras globalmente, não somente em relação à privacidade, mas também em áreas diversas como o ocorrido com as diretrizes a respeito das áreas de antitrustes, proteção ao consumidor e proteção ambiental. A tendência imposta pelo bloco econômico e político supracitado é nomeada de Efeito Bruxelas e descrita como 'globalização regulatória unilateral'. Vejamos:

> Como escreve Bradford, "enquanto a UE regula apenas seu mercado interno, as corporações multinacionais muitas vezes têm um incentivo para padronizar sua produção globalmente e aderir a uma única regra". Às vezes, por meio de um processo de duas etapas, a lei também pode desempenhar um papel formal. De acordo com Bradford, depois que as empresas voltadas para a exportação ajustaram suas práticas de negócios para seguir os padrões da UE, às vezes elas pressionam seus próprios governos para promulgar os mesmos padrões a fim de obter uma vantagem competitiva (BRADFORD *apud* SCHWARTZ, 2019, p. 8)[31].

---

[29] Ao analisar o papel imperativo da União Europeia, retoma-se os argumentos tradicionais contra a centralização global e qualquer coisa que se pareça com um Estado mundial dentre elas destaca-se que "um Leviatã global ameaçaria a liberdade e a multiplicidade de unidades menores garante uma representação e um controle sobre o abuso do poder mais eficazes; e finalmente, a construção de tal autoridade talvez viesse a ser foco de amargos conflitos que desviaram a atenção da resolução de temas práticos urgentes" Porém, o que ocorre no contexto da proteção de dados pessoais se alinha mais com o que o autor aponta como salientado por boa parte da literatura "dever-se-ia pensar mais em termos de governança global, e nos múltiplos níveis, arenas e atores envolvidos nisso, ao invés de raciocinar em termos de centralização e governo globais, No nível mais geral, a governança diz respeito à criação e o funcionamento de instituições sociais (no sentido de regras do jogo) que servem para definir práticas sociais, designar papéis e orientar as interações entre os que os desempenham capazes de solucionar conflitos, facilitando a cooperação, ou, mais genericamente, aliviando problemas de ação coletiva em um mundo constituído por atores interdependentes" (HURRELL, 1999, p. 56).

[30] "As the EU is a highly important market for international companies, many companies do not have the option of "exiting the European market entirely". Even if they could, they don't want to create separate services for them. Finally, because the EU is very concerned about privacy and has long been involved in the legislation of rules in this area, its regulations have extraterritorial reach: its laws follow the rules and personal data of EU residents whenever and wherever information is transferred out of the EU. The result, according to Goldsmith and Wu, is that US companies have chosen to bow to the "significant market power".

[31] "[…]borders through market mechanisms, resulting in the globalization of standards. Global EU rule is generally not based on (de jure) law because states outside the EU remain formally bound only by their domestic laws. However, private parties in these countries increasingly follow EU law. As Bradford writes, "While the EU

Para o eficiente andamento do presente trabalho, é importante conceituar as Organizações Multinacionais acima citadas e também diferenciá-las das Empresas Transnacionais (ETNs). Para Carvalho Filho (2011) "as Empresas Transnacionais surgem como uma reconstrução dos conceitos lapidados, no decorrer do tempo, por organizações internacionais e autores do que antes era tido como Empresas Multinacionais" (FILHO, 2011, p. 90). Dito isto, será adotada a terminologia Empresa Transnacional (ETNs) devido ao caráter mais atual do termo.

O ponto de partida da análise do impacto do GDPR de 2016 em países fora da UE são os parâmetros de adequação exigidos pela Diretiva n. 95/46, não mais em vigor, e no Regulamento Europeu de 2016, que vigora atualmente na União Europeia. Schwartz (2019) aponta que ambos possuem uma imposição de um padrão mínimo de privacidade de dados aos países de fora da União Europeia para ser permitida as transferências de dados com países-membros. Na Diretiva de 1995 o artigo 25 prevê, *in verbis*:

> […] 1 . Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objecto de tratamento, ou que se destinem a ser objecto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente directiva, o país terceiro em questão assegurar um nível de protecção adequado.
> […] 4. Sempre que a Comissão verificar, nos termos do procedimento previsto no nV 2 do artigo 3 IV, que um país terceiro não assegura um nível de protecção adequado na acepção do nV 2 do presente artigo, os Estados -membros tomarão as medidas necessárias para impedir qualquer transferência de dados de natureza idêntica para o país terceiro em causa (UNIÃO EUROPEIA, 1995).

Ao observar os pontos 1 e 4 supracitados, é clara a necessidade de assegurar que o país terceiro, destinatário da transferência de dados, detivesse dispositivos equiparados aos parâmetros exigidos dos países-membros. Em seguida, o ponto 4 ilustra que, caso não existisse adequação por parte do ordenamento jurídico terceiro, seria possível, a partir da negativa da Comissão Europeia, a exigência aos Estados-membros de tomar atitude legislativa interna (com liberdade de como fazê-la) para impedir a transferência.

A Diretiva n. 95/46 auxiliou a adoção dos países-membros de legislações internas consoantes aos padrões exigidos pela União Europeia. É possível observar que durante sua vigência havia flexibilidade das normas internas (dos países-membros) para agir diante de

---

only regulates its internal market, multinational corporations often have an incentive to standardize their production globally and adhere to a single rule" Sometimes, through a two-step process, the law can also play a formal role. According to Bradford, after export-oriented companies have adjusted their business practices to follow EU standards, they sometimes pressure their own governments to enact the same standards in order to gain a competitive advantage".

transferências com países terceiros. Para Schawrtz (2019), a Diretiva n. 95/46/EC foi eficaz na criação de um mercado único de dados pessoais na UE. Porém, nas transferências com países terceiros ela "[...]não olhou para a equivalência, mas usou um referencial diferente, o da "adequação" da proteção" (SCHARWTZ, 2019, p. 11).[32]

Mesmo deixando os Estados-membros livres para legislar acerca da limitação às transferências com países terceiros fora dos parâmetros de proteção de dados da União Europeia, a Comissão Europeia, também assumia o papel de negociar com os países não-membros a fim de deliberar sobre a falta de adequação aos seus padrões. Na 'lista dos adequados', que deveria ser constantemente atualizada pela Comissão conforme a Diretiva n. 46, eram registrados os países que correspondiam às exigências da UE, sobre isto, Comenta Schwartz:

> Existem agora onze países nesta lista, o que significa que as entidades da UE podem transferir dados para essas nações sem quaisquer requisitos adicionais. Uma transmissão para uma nação na lista branca é o equivalente funcional de uma transferência dentro da UE. (SCHWARTZ, 2019, p. 12)[33].

Já o Regulamento Europeu de 2016, garantiu maior exigibilidade na adequação dos países terceiros, do que o fez a Diretiva n. 46. Com força vinculativa aos países-membros, o GDPR trouxe a indispensabilidade de um teste de adequação ao país terceiros, aplicado pela própria Comissão Europeia, que segundo o artigo 45 deve cumprir os seguintes requisitos, *in verbis*:

> […] 2. Ao avaliar a adequação do nível de proteção, a Comissão deve, em particular, ter em conta os seguintes elementos:
> (a) o estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, legislação relevante, tanto geral como setorial, incluindo em matéria de segurança pública, defesa, segurança nacional e direito penal e o acesso das autoridades públicas aos dados pessoais, bem como a implementação de tal legislação, regras de proteção de dados, regras profissionais e medidas de segurança, incluindo regras para a transferência posterior de dados pessoais para outro país terceiro ou organização internacional que sejam cumpridas nesse país ou organização internacional, jurisprudência, bem como dados efetivos e executáveis direitos dos titulares e recursos administrativos e judiciais efetivos para os titulares dos dados cujos dados pessoais estão sendo transferidos;
> (b) a existência e o funcionamento efetivo de uma ou mais autoridades de controlo independentes no país terceiro ou a que esteja sujeita uma organização internacional, com responsabilidade de assegurar e fazer cumprir as regras de proteção de dados, incluindo poderes de execução adequados, para assistir e aconselhar os titulares dos dados no exercício dos seus direitos e para a cooperação com as autoridades de supervisão dos Estados-Membros; e
> (c) os compromissos internacionais assumidos pelo país terceiro ou a organização internacional em causa, ou outras obrigações decorrentes de convenções ou

[32] tradução livre do original: "[…] not look to equivalency, but used a different benchmark, that of "adequacy" of protection".

[33] Tradução livre do original: "There are now eleven countries on this list, which means that EU entities can transfer data to these nations without any additional requirements. A transfer to a whitelisted nation is the functional equivalent of a transfer within the EU" .

> instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, nomeadamente em matéria de proteção de dados pessoais (UNIÃO EUROPEIA, 2016)[34].

Schwartz (2019) conclui, ao analisar as mudanças dos parâmetros de exigibilidade de adequação à proteção de dados da União Europeia por países diversos dos membros, que as mudanças ocorridas afirmam sua máxima de que há, por parte da união político econômica, a implementação da 'globalização unilateral de fato' progressivamente. E que a Privacidade de dados Global se consolida devido à ausência de limitações fronteiriças que dispõe seu maior objeto: os dados informatizados.

A fim de analisar a incidência da *Global Data Protection* sobre países não participantes da UE, Schwartz (2019) realizou um estudo de caso com países de ordenamentos distintos a fim de constatar o impacto do regulamento europeu sobre o tema da privacidade informacional deles. Os países observados foram os Estados Unidos e o Japão. Ao apresentar as diferentes abordagens jurídico-nacionais do Japão e Estados Unidos, Schwartz (2019) demonstra como a UE adotou respostas flexíveis diante destes dois sujeitos político e economicamente distintos.

O Japão encontra-se atualmente entre os países parte da 'lista dos adequados' em relação à sintonia com a adequação proposta pelo marco regulatório europeu. Em 2017, foram concluídas negociações com a UE e em 2019 foi divulgada pela Comissão Europeia uma decisão constatando a adequação japonesa aos parâmetros de proteção aos dados pessoais. A deliberação foi realizada à luz do artigo 45 do Regulamento Europeu de 2016.

Antes do objetivo de adequar-se às diretrizes da União Europeia de proteção de dados pessoais, o Japão, no ano de 2014 teve sua política de privacidade descrita como "conjunto de observâncias e ritos com pouca evidência de resultados tangíveis (GREENLEAF, 2014, p.

---

[34] Tradução livre do original: "When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
(a)the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
(b)the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data".

227, *apud* SCHAWRTZ, 2019, p. 13) ". Entretanto, no período de apenas quatro anos, o país foi de uma vaga efetividade de normas sobre privacidade de dados para um dos ordenamentos internos com maior padrão de adequação ao Regulamento Europeu fora da União Europeia.

As mudanças visando a adequação começaram no ano de 2015, por meio de emendas à Lei do Japão Sobre a Proteção de Informações Pessoais (APPI). Schwartz (2019) descreve as principais mudanças que aproximaram a APPI do padrão europeu: (1) a otimização da autoridade japonesa de proteção de dados; (2) uma definição mais detalhada de dados confidenciais e sensíveis; e (3) o aumento do rigor para transferências de dados pessoais internacionais. Explica a última mudança:

> […] o Japão adotou uma ideia proeminente da lei de proteção de dados da UE. A APPI considera que os dados pessoais não podem ser transferidos para um país estrangeiro, a menos que (1) o titular dos dados tenha dado consentimento prévio específico para a transferência; (2) o país no qual o destinatário está localizado tem um sistema legal considerado equivalente em suas proteções de privacidade ao sistema japonês; ou (3) o destinatário toma medidas de precaução adequadas para a proteção de dados pessoais especificados pela autoridade japonesa de proteção de dados (SCHWARTZ,2019, p. 14). [35]

As melhorias trazidas pelas emendas à APPI japonesa vieram do diálogo com a UE e do claro interesse japonês de adequar-se aos padrões europeus de proteção de dados pessoais, após as significativas mudanças no tópico de transferência internacional de dados, que levou ao dispositivo legal que garantiu a especificidade "de dados transferidos da UE relativos à vida e orientação sexual ou filiação sindical de um indivíduo" (SCHWARTZ, 2019, p. 14), houve, por parte da Comissão Japonesa de Proteção de Dados, a publicação da Lei de Regras Suplementares sobre o tema.

O interesse em adequar-se à UE era uma clara prioridade japonesa e o acordo sobre proteção de dados entre a UE e o Japão não ficou restrito apenas à privacidade informacional. Ao contrário disto, o interesse em possuir uma livre circulação do fluxo de dados informatizados antecedeu o Acordo de Parceria Econômica UE-Japão. O mesmo foi aprovado em 2017 e entrou em vigor em 1 de fevereiro do ano de 2019. A página oficial do *site* da União Europeia, descreve que:

> As empresas da UE já exportam anualmente mais de 58 mil milhões de EUR em bens e 28 mil milhões de EUR em serviços para o Japão. O Acordo de Parceria Económica UE-Japão reduz os obstáculos ao comércio que as empresas europeias enfrentam quando exportam para o Japão e ajuda-as a competir melhor neste mercado (UNIÃO EUROPEIA, 2019).

---

[35] Tradução livre do original: "In taking this step, Japan adopted a prominent idea of EU data protection law. The APPI holds that personal data may not be transferred to a foreign country unless (1) the data subject has given specific advance consent to the transfer; (2) the country in which the recipient is located has a legal system deemed equivalent in its privacy protections to the Japanese system; or (3) the recipient undertakes adequate precautionary measures for the protection of personal data specified by the Japanese data protection authority".

Além de diversas vantagens comerciais[36] que o acordo propõe, há ainda duas seções nas quais são feitas menções aos dados pessoais: a seção de 'Propriedade intelectual e indicações geográficas', que prevê regras mínimas comuns para a proteção de dados; e a segunda, que dedica um capítulo às pequenas e médias empresas europeias (PME) e a disponibilização de um *site*[37] "sobre questões comerciais específicas e uma base de dados pesquisáveis por código pautal, para obter informações sobre o acesso ao mercado japonês" (UNIÃO EUROPEIA, 2019).

Diferente dos esforços japoneses para se adequar aos padrões da UE, os EUA rejeitaram um modelo de norma generalista semelhante ao da GDPR e optaram por tutelar setores específicos, como, por exemplo, o *Privacy Act* de 1974, que tutelava os dados processados por agências federais. É válido mencionar que é neste país em que está localizado o Vale do Silício[38], na Califórnia "[…] sede das principais empresas que possuem a custódia das maiores bases de dados pessoais do mundo" (CASSINO *et al.* 2022, p. 76).

O Vale do Silício é a localidade referência na produção e desenvolvimento de *softwares* e plataformas digitais. Nele, são criadas e desenvolvidas e se localizam as principais *Big Tech's* da atualidade. Muitas delas são idealizadas a partir da coleta massiva de dados como meio de monetização e de técnicas que envolvem o uso de algoritmos e inteligência artificial, explica:

> Essas plataformas corroboram para o surgimento de grandes empresas monopolistas e estão em cinco tipos emergentes no capitalismo de plataformas: de publicidade; de nuvem; industriais; de produtos e enxutas. As plataformas de nuvem consolidaram as plataformas como um modelo de negócios poderoso e único. Elas disponibilizam às empresas uma infraestrutura virtual de computadores, servidores, sistemas de

---

[36] "Acordo comercial com o Japão:
elimina os direitos aduaneiros e outros obstáculos ao comércio e facilita às empresas de ambas as partes a importação e a exportação; assegura a abertura dos mercados de serviços, em especial dos serviços financeiros, das telecomunicações e dos transportes; garante um tratamento não discriminatório das empresas da UE que operam nos mercados de contratos públicos; melhora a proteção dos direitos de propriedade intelectual no Japão, bem como a proteção dos produtos agrícolas europeus de elevada qualidade, as chamadas indicações geográficas (IG); poupar às empresas de ambas as partes montantes substanciais de dinheiro e tempo na comercialização bilateral de bens; prevê um maior apoio às empresas de menor dimensão que são desproporcionadamente afetadas por obstáculos ao comércio". Disponível em: <https://trade.ec.europa.eu/access-to-markets/pt/content/acordo-de-parceria-economica-entre-uniao-europeia-e-o-japao>.

[37] *Site* Web japonês para apoiar as PME (Pequenas Médias Empresas) da UE que exportam para o Japão Disponível em: <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement_en>.

[38] "O Vale do Silício, situado na Califórnia (EUA), foi viabilizado graças ao intenso financiamento público de pesquisa e infraestrutura do governo estadunidense desde a Segunda Guerra Mundial, quando empregou vultosos investimentos em tecnologia. Reconhecido pelo desenvolvimento de tecnologias de ponta, esse polo industrial ostenta por combinar tanto o espírito da pesquisa científica, em particular na engenharia e ciência da computação quanto o marketing e os princípios do empreendedorismo estadunidense (CASSINO, 2022, p. 76)".

> inteligência de negócios e aprendizagem de máquina (*machine learning*). Google, Amazon, Microsoft e Alibaba já se destacam neste tipo de negócio, em que o principal objetivo é incentivar as empresas a externalizar seus sistemas, dados e negócios para infraestrutura em nuvem (CASSINO *et al,* 2022, p. 78).

Apesar da relutância dos Estados Unidos em se alinhar com as diretrizes de proteção de dados pessoais europeias integralmente, como fez o Japão e o Brasil, Lynn *et al.* (2020) apontam que ainda assim existiu diálogo entre o país e a UE. Em 2000, a Comissão Europeia adotou a Decisão 2000/520/EC, denominada de Porto Seguro (*Safe Harbor*). Nela, as empresas norte-americanas sujeitas à supervisão da Comissão Federal de Comércio poderiam certificar o seu respeito pelos Princípios *Safe Harbor* e atestar que possuíam um certo nível de adequação às normas sobre o tema, convergentes com a UE.

Mesmo antes do *Safe Harbor*, a União Europeia, independente das negociações com os EUA, já havia desenvolvido a padronização de cláusulas contratuais e as *Binding Corporate Rules* (BCRs), a fim de regular as operações com dados transmitidos através de instrumentos privados.

Schwartz (2019, p. 17), comentando as BCR, afirma que elas "são como um código de conduta para cobrir as práticas de dados de uma empresa em todo o mundo". Porém, as cláusulas contratuais e os BCRs, mesmo sendo um caminho alternativo oferecido pela UE a agentes não adequados aos seus parâmetros, são vistos como relativamente caros e inflexíveis pelas empresas norte-americanas.

Com as revelações de Snowden ocorridas em 2013, sobre a existência de programas de vigilância em massa dos EUA, houve a revogação da *Safe Harbor* pelo Tribunal Europeu de Justiça (ECJ)[39], sendo ela substituída pelo chamado "*Privacy Shield*", que foi negociado entre a Comissão Europeia e as autoridades norte-americanas em 2016, e entrou em vigor com a Decisão 2016/1250. De acordo com Lynn *et al.* (2020) o novo sistema era muito semelhante ao *Safe Harbor* em termos de funcionamento, mas foi acompanhado por uma série de outras garantias, especialmente em relação ao direito individual de reparação de danos.

Ao final da sua análise, Schwartz (2019) constata que ao exercer seu poder unilateral, a UE acaba por empregar um conjunto de estratégias que encorajaram a disseminação do Regulamento de Proteção de Dados. Ao contrário de uma imposição unilateral, o Japão optou

[39] No caso Schrems (C-362/14), decidido em 2015, o TJE considerou que a Comissão, ao certificar a adequação do esquema Safe Harbor, não levou em consideração o poder das autoridades policiais dos EUA de acessar de forma generalizada os dados da UE transferidos sob o esquema Safe Harbor (Cole e Fabbrini 2016; Padova 2016). De acordo com o ECJ, tal modelo de vigilância em massa não pode ser tolerado, pois compromete a essência do direito à privacidade protegido pela Carta de Funda da UE direitos mentais (parágrafo 94 da sentença; ver Ojanen 2017).

por se envolver em negociações bilaterais com a UE e criar um acordo recíproco que resultasse na maior zona do mundo para trocas gratuitas de dados.

Por trás disso está não apenas a avaliação do Japão sobre seus interesses econômicos, mas também um julgamento sobre os méritos dos sistemas reguladores de privacidade de dados concorrentes. O estudo de caso do Japão, feito por Schwartz (2019), também demonstra que, ao longo do tempo, a UE conseguiu aprender com as negociações anteriores e, em geral, elevar o nível necessário para cumprir seu teste de adequação aos parâmetros de privacidade de dados.

Já no caso dos Estados Unidos, a União Europeia conseguiu encontrar soluções para estender ao país suas diretrizes de adequação. O resultado não foi uma norma completamente consoante ao Regulamento Geral de Proteção de Dados europeu, sendo um fator também impeditivo a independência legislativa que os estados possuem. A UE estabeleceu soluções efetivas nas relações privadas entre empresas transnacionais (ETNs) com sedes principais em solo norte-americano que, acabam por realizar transferência de dados com Estados-membros do bloco econômico europeu.

Já ao observar a tendência jurídica de adequação à privacidade na América do Sul é possível perceber que alguns países da região buscaram legislar sobre o tema ainda na primeira década dos anos 2000, como o Chile, que em 1999 se tornou o primeiro país da América Latina a ter uma lei abrangente sobre proteção de dados, de acordo com Magrine (2021).

D'avilla *et al.* (2021) comentam que, comparado com os demais países da América Latina, o Brasil foi fortemente impactado pelos padrões de adequação europeu previstos no RGPD. Mesmo que já existissem discussões sobre a necessidade da presença jurídica no espaço digital, até 2018 as normas brasileiras não tinham nenhuma lei direcionada somente à proteção de dados. Os autores supracitados explicam que:

> O *General Data Protection Regulation,* com a exigência de padrões mínimos de privacidade para que pudesse ocorrer a transferência internacional de dados entre empresas europeias e os demais países destinatários, gerou sem sombra de dúvidas uma mudança de paradigma sobre a necessidade de normas sobre o tema. O interesse do Brasil em manter-se relevante no comércio internacional, alavancou a criação de legislação específica sobre a proteção de dados. No Brasil, especialmente, a necessidade pela edição da norma passou a ser mais crucial se comparado a outros países, uma vez que alguns Estados da América do Sul já tinham lei protetora dos dados pessoais. É o caso de Chile (Ley 25.326/2000), Uruguai (Ley 18.331/2008), Colombia (Ley Estatutária 1.581/2012) dentre outros. (D'AVILLA *et al,* 2021, p. 42)

No âmbito internacional também é possível observar a presença da Organização dos Estados

Americanos (OEA), que no ano 2000, sancionou a *Ley* 25.326, sobre a proteção de dados, e no ano de 2021 publicou uma cartilha atualizada sobre os princípios que regem a proteção de dados pessoais. A adoção dos Princípios Atualizados cumpre um mandato à Comissão Jurídica Interamericana (CJI), publicada em junho de 2018 pela Assembleia Geral da OEA[40].

O Brasil realizou debates no Congresso Nacional sobre legislações acerca do ambiente digital desde o final da primeira década dos anos 2000. As discussões tinham como pauta a insuficiência da aplicabilidade análoga das leis e códigos antecessores no ordenamento jurídico brasileiro a casos concretos ocorridos e possibilitados pela utilização do ciberespaço.

É exemplo da repercussão das primeiras discussões brasileiras sobre Direito digital e privacidade a Lei n. 12.737/12, nomeada popularmente de Lei 'Carolina Dieckmann', devido à repercussão social, nas mídias o caso da atriz brasileira de mesmo nome. Ela que teve fotos e conversas íntimas armazenadas no seu aparelho celular expostas sem sua autorização.

Em 2014 foi promulgado o Marco Civil da Internet (Lei 12.965/2014), que de maneira ambiciosa tutelou a dimensão *online* acessada pelos cidadãos brasileiros. A norma versava sobre proteção de dados em alguns artigos[41], mas foi somente depois da criação do RGPD da União Europeia que o ordenamento jurídico brasileiro atentou para a elaboração de uma lei específica sobre proteção de dados pessoais.

De acordo com D'avila *et al. (*2021), o contexto da criação da LGPD (Lei 13.709/2018) parte da pretensão brasileira de buscar uma vaga efetiva como membro da OCDE. Tal intento exige do país candidato a elaboração de uma norma protetiva de dados pessoais para pleitear uma vaga. O fato de ter a lei brasileira (Lei n. 13.709/2012) como modelo basilar o texto do GDPR, com diversos artigos similares, mostra a imperatividade da UE e também a tendência da convergência jurídica internacional sobre a matéria de proteção de dados. Descrevem Bioni e Mendes (2019):

> Apesar das diferentes técnicas legislativas, há uma convergência perceptível entre os princípios previstos no RGPD e na LGPD. Essa convergência pode ser atribuída menos a uma influência direta do processo legislativo europeu na lei brasileira do que a um longo processo de construção de um consenso transnacional acerca dos princípios básicos que regem essa matéria (BIONI; MENDES, 2019, p. 165).

---

[40] O documento é intitulado de "atualização dos princípios sobre a proteção de dados pessoais, levando em conta sua evolução" (OAS. Documentos oficiais; OEA/Ser.D/XIX.20) Disponível em: <https://www.oas.org/en/sla/iajc/docs/Publicacion_Principios_Atualizados_sobre_a_Privacidade_e_a_Protecao_de_Dados_Pessoais_2021.pdf>.

[41] Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: [...] III - proteção dos dados pessoais, na forma da lei; Art. 10º. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014).

Com ordenamentos jurídicos internos distintos, que refletem em sua maioria as realidades socioeconômicas de cada localidade, é possível notar a influência de organismos de Direito que busca homogeneizar para facilitar as transações internacionais. O que evidencia a existência de uma convergência principiológica e legislativa sobre a temática de proteção de dados advinda das diretrizes implementadas pelas Organizações Internacionais.

3 *CLOUD COMPUTING* E SUAS IMPLICAÇÕES À PRIVACIDADE

3.1 Definição de *cloud computing* e suas principais características

Ao contrário da concepção difundida pela sua recente popularização, a tecnologia de computação ‘em nuvem’ surgiu em meados da década de 1960. Segundo Satorello (2022), seu precursor foi Bob Bemer, cientista da computação da *International Business Machines* (IBM). Sua ideia se resume à implementação de um ‘recurso compartilhado’ na programação dos códigos.

Bemer propôs uma espécie de compartilhamento em tempo real *(timing share)* aos programadores da época, a fim de otimizar o processo anterior, o qual é descrito como vagaroso e carente de melhorias por Sartorello (2022): "digitavam os códigos usando cartões perfurados ou fitas e os enviavam para uma máquina a qual executava trabalhos de forma síncrona, um após o outro” (SARTORELLO, 2022, s.p.).

Para que um código computacional programado por mais de um desenvolvedor fosse elaborado, muito tempo era gasto, porque os programadores só podiam enviar suas modificações no código geral um por vez. À vista disto, o modelo criado na década de 60 conseguiu sanar o problema através da criação da ideia geral da computação ‘de nuvem’, na qual há a possibilidade, a partir da sua estrutura em rede, do acesso compartilhado entre diversos indivíduos simultaneamente. Seu funcionamento é explicado:

> […] esses sistemas precisam manter o estado de cada usuário e de cada programa e se alternar entre eles rapidamente. Embora as máquinas de hoje façam isso sem esforço, demorou algum tempo até que os computadores tivessem a velocidade e o tamanho da memória central para suportar essa nova abordagem. A *Tymshare* foi uma empresa inovadora neste aspecto. Iniciado em 1964, o serviço vendeu tempo de computador e pacotes de software para usuários. Ele tinha dois *mainframes* que podiam ser acessados por meio de conexões *dial-up* (via linha telefônica) (SATORELLO, 2022, *s.p.*).

A necessidade de otimizar o manuseio dos códigos de programação deu origem à estrutura inicial da computação ‘em nuvem’. O resultado foi uma nova forma de compartilhamento de dados e códigos menos trabalhosa para os desenvolvedores de códigos, que com o tempo, junto ao desenvolvimento dos computadores e sua capacidade de armazenamento, culminou no complexo paradigma atual.

Mesmo idealizada ainda na década de 1960, foi apenas em 1997 — de acordo com

Vellasco e Viggiani (2014) — que o termo *cloud computing* teve sua menção registrada pela primeira vez nas palavras do professor de sistemas da informação Ramnath Chellappa[42], que desenvolve o tema desde a década de 90.

Para Singh (2021) a palavra 'nuvem', que constitui o termo *cloud computing*, é usada como metáfora para a *internet* já que o serviço se refere à computação com base em rede (*internet-based*), na qual os serviços de tecnologia da informação (TI) são entregues e oferecidos em ambiente *online.* Desta forma, compreende-se a utilização do substantivo porque o seu significado científico descreve a composição extremamente volátil[43] das nuvens visíveis no céu, que estão suspensas na atmosfera terrestre.

A associação do ambiente digital em rede com as nuvens presentes na atmosfera do planeta retoma o raciocínio de Zuboff (2019) da síndrome da carruagem sem cavalos: "situações nas quais atrelamos nossa sensação de perigo inédita a fatos velhos e familiares" (ZUBOFF, 2019, p. 403). Zuboff exemplifica a tentativa por parte das pessoas de explicar, na época, o recém inventado automóvel como sendo uma carruagem sem cavalos. Exemplo este que pode sintetizar a tendência humana frequentemente associada a inovações técnicas de descrever algo nunca visto a partir das referências que já possuem.

Entendida a analogia utilizada para nomear a tecnologia que possibilita o compartilhamento de dados *online, seguimos* o entendimento da função à qual a computação em nuvem se propõe. Seu propósito pode ser definido como uma nova forma de fornecer serviços e de tratar informações, que pode ser utilizada tanto por empresas privadas e pessoas físicas, quanto pela administração pública/estatal. O guia publicado pela Agência Espanhola de Dados e disponibilizado no *site* da Organização Econômica Americana (OEA), descreve a função da computação 'em nuvem' como:

> Uma solução de computação em nuvem permite ao usuário otimizar a alocação e o custo dos recursos associados às suas necessidades de processamento de informações. O usuário não precisa fazer investimentos em infraestrutura, mas sim usar aquela disponibilizada pelo provedor de serviços, garantindo que não sejam geradas situações de falta ou excesso de recursos, bem como custo extra associado a tais situações (ESPANHA, 2013,p.5) [44].

---

[42] "Prof. Chellappa's expertise is in the fields of electronic markets, pricing, digital goods piracy and economics of information security and privacy. His research in these areas has been widely published/presented in leading journals and conferences. His work on information privacy, research on music digitization and study of software pricing have received best paper awards in premier conferences. His research methods include analytical modeling, empirical modeling and social network analysis". Disponível em: <https://goizueta.emory.edu/faculty/profiles/ramnath-k-chellappa>.

[43] Nuvem é um conjunto visível de partículas minúsculas de água líquida ou de gelo, ou de ambas ao mesmo tempo, em suspensão na atmosfera. Este conjunto pode também conter partículas de água líquida ou de gelo em maiores dimensões, e partículas procedentes, por exemplo, de vapores industriais, de fumaças ou de poeiras.

[44] Tradução livre do original: "Una solución cloud computing permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio,

As possibilidades de gerenciamento das informações que o cliente contratante possui nos serviços é destaque na computação em nuvem. Através da *Internet* são oferecidas soluções de banco de dados, hospedagem de *e-mails* e outros serviços, a depender da demanda do contratante do serviço.

O guia espanhol ainda destaca que a responsabilidade do contratado (quem está fornecendo a *cloud*) irá variar junto ao modelo disponibilizado: "desde a propriedade, a manutenção e a gestão do suporte físico de informações, processos e comunicações podem estar nas mãos de terceiros" (ESPANHA, 2013, p.6).

A utilização da tecnologia em nuvem está em ascensão nas últimas duas décadas devido ao maior acesso à conexão à *internet,* em conjunto com o aprimoramento da capacidade de armazenamento dos computadores que hospedam os *data centers*[45]. Lynn *et al.* (2020) afirmam que a tecnologia pode ser considerada o principal paradigma computacional do século XXI.

Uma das principais características que levam a este protagonismo é seu atributo comum à atualidade globalizada: a possibilidade de descentralização. Seus bancos de dados dissociados estão presentes em diversas localidades, o que possibilita aos dados o fácil trânsito em rede. Lynn *et al.* explicam que a nuvem é:

> Um modelo para permitir o acesso à rede onipresente, conveniente e sob demanda de ferramentas e recursos de computação configuráveis que podem ser rapidamente providos e liberados com esforço mínimo de gerenciamento e interação com o provedor dos serviços (LYNN *et al.,* 2020, p. 42)[46].

A ubiquidade da computação em nuvem permite que os serviços desempenhados nas redes digitais tenham recursos computacionais, principalmente de capacidade de armazenamento, oferecidos a partir das demandas que vão surgindo ao longo da utilização, o que acentua a mobilidade dos provedores de nuvem:

---

garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones".

[45] Data Center pode ser entendido basicamente como a estrutura física na qual os dados são armazenados e onde ocorre o processamento de software em nuvem. Nawaz (2019) o define de maneira mais eficiente: [...] "é uma infraestrutura de instalação de missão crítica construída envolvendo várias disciplinas de engenharia, como civil/arquitetura, elétrica, mecânica, segurança, etc., usada para hospedar a infraestrutura de tecnologia da informação da organização, como servidores, armazenamento, rede e sistemas de segurança que empresas ou outras organizações usam fornecer vários serviços facilitadores de negócios, organizando, processando, armazenando e recuperando grandes quantidades de dados" (NAWAZ, 2019, p. 7). Tradução livre do original: "is a mission critical facility infrastructure build involving the various engineering disciplines such as civil/Architecture, electrical, mechanical, safety etc. used for hosting the organization information technology infrastructure such as servers, storage, network and security systems that businesses or other organizations use to deliver various business enabling services by organizing, processing, storage and retrieval of large amounts of data".

[46]Tradução livre do original: "A model for enabling ubiquitous, convenient, on-demand network access to configurable computing tools and resources that can be rapidly provisioned and released with minimal management effort and service provider interaction".

> […] possibilitando que o provedor de serviços esteja localizado em praticamente qualquer lugar do mundo e seu objetivo final é fornecer os serviços otimizando recursos próprios, por exemplo, práticas de realocação, compartilhamento de recursos e mobilidade ou realização de subcontratos adicionais. (ESPANHA, 2013, p.6)[47].

Singh (2022) apresenta a premissa clássica e tradicional de *data centers,* na qual os recursos computacionais são adquiridos em momento prévio e personalizados pelos clientes em capacidade máxima, independente do quanto e como precisarão ser utilizados. Logo, no seu modelo tradicional, o *Data Center* sem a característica *on demand* — essenciais aos serviços em nuvem — "pode resultar num desperdício de recursos, ou até mesmo, na insuficiência destes" (SINGH, 2022, p. 40)[48].

Como os serviços de nuvem pressupõem a compra de ferramentas a qualquer momento a partir da necessidade dos clientes, é possível vislumbrar o motivo da ascensão da forma *on demand* quando comparado ao modelo tradicional. Singh (2022) descreve que utilizando da computação em nuvem as organizações (empresas provedoras) oferecem os seguintes serviços:

> […] máquinas virtuais (recurso de computação que usa software em vez de um computador físico), armazenamento virtual (formada pela combinação de vários dispositivos de armazenamento de rede) e muitos outros tipos de aplicativos de software (ou serviços) pela internet (SINGH, p. 20, 2022)[49].

A popularização dos serviços *on demand* ocorreu junto a ascensão das tecnologias digitais, intensificadas ao longo da segunda década dos anos 2000. A crescente conexão dos indivíduos, principalmente através de *smartphones*, fez com que os consumidores tivessem acesso a um número maior e mais diversificado de produtos. Isso teve como efeito o aumento na variedade de escolha, que suscitou a necessidade de ferramentas para lidar com e otimizar as relações de consumo eletronicamente mediadas.

De acordo com Suhr e Gross (2022), a ascensão da *Netflix*[50]*,* uma das maiores

---

[47] Tradução livre do original: "El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales".

[48] Tradução livre do original: "Can result in a waste of resources, or even in the management of these".

[49] Tradução livre do original: "Virtual machines (computing resources that uses software instead of a physical computer), virtual storage (formed by combining various network storage devices) and many other types of software applications (or services) over the internet".

[50] Explicam Suhr e Gross (2022) sobre o funcionamento da Netflix: "A fim de cativar o espectador, assim sendo, a empresa realiza procedimentos de personalização nas contas dos assinantes, os chamados sistemas de recomendação: é feita uma coleta de dados do usuário, como localização, histórico de conteúdo assistido, horário em que se assistiu, informações pesquisadas, interação com a plataforma, entre outros; esses, por sua vez, são analisados com uso de aprendizado de máquina e, posteriormente, direcionam obras de potencial interesse à interface específica de cada cliente. Cada assinatura também permite criar diferentes perfis para

plataformas *Subscription Video on Demand* (SVoD) do mundo, tem como base a formulação e implementação de um sistema de escolhas baseado na lógica algorítmica.

O atrativo da plataforma citada está na sugestão de novas escolhas baseadas no processamento dos dados oferecidos pelos consumidores em acessos anteriores, no âmbito de um catálogo de filmes e séries que dão ao usuário a sensação da disponibilidade de uma infinitude de opções, mas que, na verdade, são limitadas ao alcance do seu perfil comportamental, elaborado através dos dados pessoais que ele disponibiliza ao clicar e selecionar o que lhe chama a atenção.

Zuboff (2019) comenta que oferecer serviços 'por demanda', a exemplo do oferecido pela *Netflix*, é tão lucrativo quanto dependente da coleta de dados dos usuários. O exemplo da autora implica uma parceria de transferência de dados entre entes público e privado, em um projeto que provê um cenário totalmente interativo e aparentemente adaptável aos interesses dos usuários. Nele "Vagas de estacionamento públicas e privadas são combinadas em mercados *on-line* e alugadas por demanda, com o custo do estacionamento variando em tempo real, aumentando substancialmente a receita do setor" (ZUBOFF, 2019, p. 277).

O projeto da Universidade *Columbos* — Ohio Estados Unidos — em parceria com a *SideWalk*[51], marca de sapatos, ilustra a potência dos serviços *on-demand.* Aplicáveis a diversos nichos, a modalidade oferece ao cliente final o conforto da disponibilidade de serviços e produtos coerentes a suas demandas junto a otimização dos negócios dos fornecedores conforme o perfil de consumo dos usuários.

É um exemplo das vantagens da característica 'por demanda' nos serviços de *software* em nuvem o caso da franquia de *pizzarias Domino's*, que, em determinado evento anual famoso nos Estados Unidos, tem sua demanda de pedidos via aplicativos de *delivery* dobrada:

> Um exemplo que implementa o modelo de nuvem híbrida é a Domino's Pizza. Essa empresa recebe 50% mais pedidos no domingo do Super Bowl do que em uma típica sexta à noite. Em vez de comprar hardware de TI adicional para lidar com a

pessoas diferentes que acessam a conta, personalizando cada um de forma específica" (GROSS; SUHR, 2022, p. 5) Disponível em: <https://fateclog.com.br/anais/2022/324-668-1-RV.pdf>.

[51] "Quando Columbus, Ohio foi nomeada vencedora da competição do DOT, ela deu início a um projeto demonstrativo de três anos com a Sidewalk, incluindo uma centena de quiosques e livre acesso ao so ware Flow. O jornal e Guardian acabou por ter acesso a documentos e trocas de mensagens dessa colaboração segundo os quais inovações como estacionamento dinâmico, "aplicação de estacionamento otimizado" e um "mercado de mobilidade compartilhada" revelam um padrão mais problemático do que a retórica sugere. Os fluxos de dados da Sidewalk combinam ativos públicos e privados à venda em mercados virtuais dinâmicos, em tempo real, que extraem taxas máximas de cidadãos e tornam o governo municipal dependente da informação de propriedade da Sidewalk. Por exemplo, vagas de estacionamento públicas e privadas são combinadas em mercados on-line e alugadas "por demanda", com o custo do estacionamento variando em tempo real, aumentando de forma substancial a receita do setor. A aplicação de estacionamento otimizado depende de os algoritmos da Sidewalk "calcularem as rotas mais lucrativas para policiais de estacionamento", o que rendeu à cidade milhões de dólares adicionais de que ela necessita com urgência, mas que são conquistados à custa dos cidadãos" (ZUBOFF, 2019, p.277).

> demanda de chamadas incomuns no Super Bowl – capacidade que não usaria pelo resto do ano – a Domino's Pizza voltou-se para a nuvem para lidar com suas crescentes necessidades de TI naquele dia (GÓMEZ, 2013, p.8)[52].

Segundo Lynn *et al.* (2020), a estrutura técnica da arquitetura da nuvem é desafiadora à proteção de dados porque permite aos componentes tecnológicos se combinarem para construir uma rede capaz de possibilitar a operação dos recursos por meio da virtualização, executando máquinas virtuais como uma camada de abstração sobre uma camada física. Isso é possível através do processo que viabiliza a conversão de *hardware*[53] massivo e palpável em recursos de computação, disponíveis em rede na *internet*.

Satorello (2022) resume: "[…] tudo o que normalmente é necessário para montar o equivalente a uma sala de servidores, ou mesmo um *Data Center*[54] completo, estará pronto para ser utilizado, configurado e executado". São os maiores e mais famosos provedores de nuvem as empresas: *Microsoft, Google e Amazon*.

Entendido o conceito geral da *cloud computing* e os principais objetivos de sua utilização almeja, é interessante apresentar os agentes que fazem parte das possibilidades de serviços e produtos oferecidos pela tecnologia supracitada.

É uma tarefa complexa diferenciar os sujeitos presentes no serviço de computação em nuvem porque, muitas vezes, uma empresa pode ser ao mesmo tempo, usuária dos serviços e ocupar a figura de provedora diante de um cliente final. Explica o Guia Espanhol:

> Os serviços de computação em nuvem estão sendo usados quando encontramos empresas, entidades, departamentos, etc., que chamaremos de usuários ou clientes, para implementar seus processos de processamento de informações, compartilham os mesmos recursos por meio de uma rede; recursos fornecidos por uma entidade separada, chamada provedor de serviços em nuvem provedor de computação ou

---

[52] Tradução livre do original: "Un ejemplo que implementa el modelo de nube híbrida es Domino 's Pizza. Esta compañía recibe 50% más de pedidos en el domingo del Super Bowl que en una noche típica de viernes. En vez de comprar hardware adicional de TI para atender la demanda inusual de llamadas en el Super Bowl —capacidad que no usaría en el resto del año- Domino's Pizza ha utilizado la nube para manejar el incremento de sus necesidades en TI para ese día"

[53] "O termo em inglês, em si, abrange qualquer item ou ferramenta física. Com isso, "hardware" pode incluir até mesmo materiais de manutenção doméstica, como chaves de fenda ou martelos, por exemplo.
Na computação, a premissa é a mesma e o termo se refere a qualquer parte física de um produto eletrônico. Nesse sentido, entende-se como hardware desde as peças internas de um computador — como sua placa-mãe ou memória — como componentes externos, como mouses e teclados. Para simplificar mais ainda, "hardware" é qualquer item que pode ser tocado fisicamente, seja ele localizado dentro ou fora do aparelho" (BERTONZIN, *s.p.* 2021) Disponível em: <https://canaltech.com.br/hardware/o-que-e-hardware-195342/>.

[54] O Data Center ou Central de Processamento de Dados é um ambiente projetado para reunir servidores, armazenar informações, processar dados, gerenciar ativos de rede, entre outras atividades. O funcionamento dessa estrutura é crucial para administração pública e diversos setores da economia (indústria, comércio etc.). Disponível em: <https://prodest.es.gov.br/conheca-os-cinco-principais-tipos-de-data-center>.

> nuvem (ESPANHA, 2013, p.6)[55].

O sujeito que oferece o serviço de *Data Center's,* nos quais estão hospedados os computadores onde os *softwares* dos clientes são executados, é chamado de provedor de nuvem. Este agente denominado de provedor pode ter como consumidor uma empresa numa dinâmica *Business to Business*. A empresa utiliza dos serviços de *softwares* para constituir seu negócio e chegar no consumidor final. Mas, o provedor também pode ser da empresa que vende o serviço diretamente para o consumidor final.

Por exemplo, uma loja virtual pode utilizar os serviços de um provedor 'A' para disponibilizar sua página *online.* Mas o provedor de nuvem 'A' pode ao mesmo tempo oferecer seus serviços diretamente para o cliente final. Geralmente neste caso o uso tem fim de armazenamento de arquivos e disponibilização de 'espaço' computacional. O *Guía para clientes que contraten servicios de Computing* (2013) também apresenta um sujeito que merece destaque, além dos clientes e provedores acima descritos, os 'sócios':

> Além de clientes e provedores, existem outros players no mundo da computação em nuvem. Entre eles destacam-se os sócios ou parceiras dos provedores de nuvem. Eles criam, oferecem e suportam serviços na nuvem que eles vendem para o usuário final como licenças de usuário, por exemplo, criando um aplicativo de marketing executado na nuvem a partir de serviços de nuvem mais básicos. Os parceiros estão localizados entre o cliente e o provedor de nuvem, podendo formalizar seu relacionamento com este último com valores contratuais diferentes (ESPANHA, 2013, p.6)[56] .

É importante entender que os sujeitos partem das negociações presentes na utilização da nuvem por questões contratuais. Se ocorrer qualquer acidente com as informações fornecidas pelo usuário dos serviços, os agentes, a depender da responsabilidade assumida, respondem juridicamente de maneira distinta. Na seção seguinte serão abordadas as principais implicações contratuais que os serviços em nuvem podem gerar.

São três os principais modelos de computação em nuvem existentes: nuvem pública; nuvem privada; e nuvem híbrida. Lynn *et al.* (2020) os diferenciam através da classificação dos usuários aos quais atende e suas limitações de serviços. A nuvem pública armazena informações geralmente *online,* não tem restrição de usuários e atende ao provedor de *cloud*

---

[55] Tradução livre do original: "se están utilizando servicios de cloud computing cuando encontramos empresas, entidades, departamentos, etc., a los que llamaremos usuarios o clientes, que para implementar sus procesos de tratamiento de información comparten los mismos recursos a través de la red; recursos proporcionados por una entidad distinta, llamada proveedor de servicios de cloud computing o proveedor de la nube".

[56] Tradução livre do original: "Además de los clientes y proveedores, existen otros jugadores en el mundo de la computación en la nube. Entre ellos destacan los partners de proveedores de la nube. Crean, ofrecen y admiten servicios en la nube que venden al usuario final como licencias de usuario, por ejemplo, creando una aplicación de marketing que se ejecuta en la nube desde servicios en la nube más básicos. Los socios se ubican entre el cliente y el proveedor de la nube, pudiendo formalizar su relación con este último con diferentes valores contractuales".

simultaneamente ao consumidor final:

> É esse modelo que permite aos usuários acesso a recursos de computação compartilhados pela internet, usando qualquer navegador comuns não especializados (Mozilla Firefox, Internet Explorer, Safari, Google Chrome, entre outros). É baseado em um pagamento por utilização do serviço, à semelhança dos serviços públicos como eletricidade, o que permite flexibilidade para oferecer assistência adequada em momentos de alta demanda que permite aos consumidores usarem recursos a partir das suas demandas (GÓMEZ, 2013, p. 7)[57].

Gómez (2013) considera sua característica pública como negativa, por acreditar que o fato de permitir o acesso ao público em geral a deixa mais vulnerável a ataques de terceiros mal-intencionados, se comparada a outros modelos de *cloud.*

Já o modelo de nuvem privada restringe-se a redes internas personalizadas para o acesso limitado preestabelecido. Seu foco de negócio está na relação entre o provedor de nuvem e demais empresas (*B2B*). Seus serviços estão conectados a um centro de informações interno das empresas que o contratam uma estrutura de nuvem exclusiva. Afirma Gómez (2013) que esse modelo consequentemente dispõe de maior segurança, e exemplifica:

> Um exemplo disso é o utilizado pelas empresas para compartilhar arquivos em pastas comuns (que diferentes usuários podem acessar e modifique usando um login). estes vão são armazenados em servidores físicos, guardados pela empresa, que podem ser acessado a partir de uma página da web. Isso permite níveis de segurança mais elevados do que qualquer outro tipo de computação em nuvem (GÓMEZ, 2013, p. 7)[58].

O último dos principais modelos de nuvem é a híbrida. Ela funciona com duas camadas distintas divididas entre a parte aberta, executada *online*, e uma parte utilizada em redes locais.

Nela, há interação entre o provedor de nuvem e empresas consumidoras, o fornecimento dos serviços do provedor de nuvem ao consumidor final e simultaneamente, a execução dos servidores nos quais as empresas que contratam o provedor executam seus negócios destinados ao consumidor final.

Além dos tipos de *cloud* popularizados (nuvem privada, pública e híbrida) um quarto tipo de computação em nuvem — menos comum — é descrita por Oshodi (2022) como multi

---

[57] Tradução livre do original: “Es este modelo el que permite a los usuarios acceder a los recursos informáticos compartidos a través de Internet, utilizando cualquier navegador común no especializado (Mozilla Firefox, Internet Explorer, Safari, Google Chrome, entre otros). Se basa en un pago por uso del servicio, similar a los servicios públicos como la electricidad, lo que permite flexibilidad para brindar una asistencia adecuada en momentos de alta demanda que permite a los consumidores utilizar los recursos en función de sus demandas”.

[58] Tradução livre do original: “Un ejemplo de esto lo utilizan las empresas para compartir archivos en carpetas comunes (a las que diferentes usuarios pueden acceder y modificar mediante un inicio de sesión). estos se almacenan en servidores físicos, mantenidos por la empresa, a los que se puede acceder desde una página web. Esto permite mayores niveles de seguridad que cualquier otro tipo de computación en la nube”.

nuvem:

> Multi-cloud é uma abordagem de nuvem composta por mais de um serviço de nuvem e mais de um fornecedor de nuvem, público ou privado. Todas as nuvens híbridas são multinuvens, mas nem todas as multinuvens são nuvens híbridas. multinuvens tornam-se nuvens híbridas quando várias nuvens são conectadas por alguma forma de integração ou orquestração. Um ambiente multinuvem pode existir propositadamente para controlar melhor os dados confidenciais como espaço de armazenamento redundante para recuperação de desastres aprimorada ou por acidente (OSHODI, 2022, p. 11)[59] .

O ambiente de multi nuvens é criado para melhor controlar a privacidade relacionada aos dados e possibilitar mais controle diante de incidentes de perda de *Data Centers* ou de vazamento. Isto se dá devido à alocação do mesmo serviço em camadas diferentes e em provedores de nuvem distintos, com o objetivo principal da descentralização protetiva.

Já a divisão dos serviços oferecidos na computação em nuvem não é feita de maneira rigorosa. É comum que existam provedores que os fornecem de maneira mista e mesclando mais de um produto, oferecidos ao mesmo tempo. Dito isto, os modelos de serviço são:

> […] *Software* como Serviço (SaaS) A capacidade fornecida ao consumidor é usar os aplicativos do provedor executados em uma infraestrutura de nuvem e acessível por uma interface do cliente; Plataforma como Serviço (PaaS) A capacidade fornecida a um consumidor para implantar na infraestrutura de nuvem aplicativos criados ou adquiridos pelo consumidor criados usando tecnologias de desenvolvimento fornecidas pelo provedor; Infraestrutura como serviço (IaaS) A capacidade fornecida ao consumidor para fornecer processamento, armazenamento, redes e outros recursos de computação fundamentais para implantar e executar software arbitrário (LYNN *et al.*, 2020, p. 24)[60].

As funções dos serviços vão desde a simples disponibilidade de infraestrutura até o fornecimento de *software*. Como exemplos de serviços IaaS, há *Amazon Web Services* e a *Google Compute Engine*; alguns exemplos de *PaaS* são o *Heroku* e o *Red Hat OpenShift.* Como exemplos de *SaaS*, encontramos ferramentas como a *Gupy,* plataforma *online* de recrutamento e seleção, e também o *Trello,* plataforma utilizada para gerenciamento de tarefas e projetos (BESSA, 2022, s.p.).

---

[59] Tradução livre do original: “Multi-cloud is a cloud approach made up of more than one Cloud service from more than one cloud vendor, public or private. All hybrid clouds are multi-clouds, but not all multi clouds are hybrid clouds. multi-clouds become hybrid clouds when multiple clouds are connected by some form of integration or orchestration. A multi-cloud environment might exist on purpose to better control sensitive data as redundant storage space for improved disaster recovery or by accident,”.

[60] Tradução livre do original: “Software as a Service (SaaS) The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible through a customer interface; Platform as a Service (PaaS) The ability provided to a consumer to deploy to the cloud infrastructure consumer-created or purchased applications created using development technologies provided by the provider; Infrastructure as a Service (IaaS) The ability provided to the consumer to provide processing, storage, networking, and other fundamental computing resources to deploy and run arbitrary software”.

Lynn *et al.* (2020) ainda citam a *Function as a Service (FaaS)*, serviço menos popular, mas que pode ser definido como "a capacidade fornecida ao consumidor para executar funções sem estado leves e de propósito único, sob demanda, geralmente por meio de uma API" (LYNN *et al.,* 2020, p. 24)[61].

Os primeiros serviços de computação em nuvem popularizados possuem menos de duas décadas de existência, mas diversas organizações já se utilizam das suas aplicações: "pequenas *startups* até corporações globais, agências governamentais até agentes sem fins lucrativos estão abraçando a tecnologia por motivos e usos diversos" (OSHODI, 2022, p. 16).[62]

A paleta de usos da *cloud computing* abrange serviços *online* em geral: plataformas que reproduzem conteúdo audiovisual; *videogames;* no envio e armazenamento de correspondência virtual; fotos e arquivos diversos. Nas plataformas há no *back-end*[63] dos aplicativos um provedor de nuvem, possibilitando o processamento das ferramentas de *software* necessárias ao seu funcionamento. São alguns exemplos de aplicação da *cloud computing*:

> Criação de aplicativos *cloud-native:* crie, implante e dimensione rapidamente aplicativos - web, móveis e API; Aproveite as tecnologias e abordagens nativas da nuvem, como contêineres, Kubernetes, arquitetura de microsserviços, comunicação orientada por API e DevOps; Teste e criação de aplicativos- reduz o custo e o tempo de desenvolvimento de aplicativos usando infraestruturas de nuvem que podem ser facilmente ampliadas ou reduzidas; [...] Software sob demanda- Também conhecido como software como serviço (SaaS), o software sob demanda permite que você ofereça as versões e atualizações de software mais recentes aos clientes — a qualquer momento e em qualquer lugar (OSHODI, 2022, p.16) [64].

Os exemplos acima incluem as demandas relacionadas ao desenvolvimento de aplicativos, atividade dos programadores e engenheiros de *software*. Por isso, são exemplos que se afastam da demanda do consumidor final e consequentemente da preocupação direta

---

[61] Tradução livre do original: "The capacity provided to the consumer to perform lightweight, stateless, and purpose-built functions on demand, usually through an API".

[62] "tiny startups to global corporations, government agencies to no-profits are embracing the technology for all sorts of reasons".

[63] De maneira quase literal, O *Back-End* pode ser definido como a parte do código de programação que "trabalha em boa parte dos casos fazendo a ponte entre os dados que vem do navegador rumo ao banco de dados e vice-versa, sempre aplicando as devidas regras de negócio, validações e garantias num ambiente restrito ao usuário final (ou seja, onde ele não consegue acessar ou manipular algo)" Disponível em: <https://www.alura.com.br/artigos/o-que-e-front-end-e-back-end>.

[64] Tradução livre do original: "Create cloud-native applications- Quickly build, deploy, and scale applications—web, mobile, and API. Take advantage of cloud-native technologies and approaches, such as containers, Kubernetes, microservices architecture, API-driven communication, and DevOp; Test and build applications- Reduce application development cost and time by using cloud infrastructures that can easily be scaled up or down;[...]Deliver software on demand- Also known as software as a service (SaaS), on-demand software lets you offer the latest software versions and updates around to customers—anytime they need, anywhere they are".

com a privacidade dos dados. Porém, a aplicabilidade dos serviços de *cloud computing* também é ampla em serviços de *software* corriqueiros, e geram demandas relacionadas à vulnerabilidade dos usuários. São exemplos:

> (1)Armazenamento, backup e recuperação dos dados - Proteção dos seus dados de maneira mais econômica — e em grande escala — transferindo seus dados pela Internet para um sistema de armazenamento em nuvem externo que pode ser acessado de qualquer local e dispositivo; (2)Análise dos dados- Unifique seus dados entre equipes, divisões e locais na nuvem. Em seguida, use os serviços de nuvem, como aprendizado de máquina e inteligência artificial, para descobrir insights para decisões mais informadas; (3) Transmissão de áudio e vídeo- Conecte-se com seu público em qualquer lugar, a qualquer hora, em qualquer dispositivo com vídeo e áudio de alta definição com distribuição global. Ao Incorporar inteligência usa modelos inteligentes para ajudar a envolver os clientes e fornecer informações valiosas a partir dos dados capturados (OSHODI, 2022, p. 16)[65].

As aplicações supracitadas têm em comum o manuseio direto dos dados pessoais do titular. As informações armazenadas, coletadas e analisadas mediante tratamento são geralmente coletadas massivamente dos consumidores finais de serviços *online*. O que ratifica a proteção à privacidade como um desafio para empresas que utilizam da tecnologia de *cloud, mas* que também precisam estar adequadas às diretrizes jurídicas de proteção à privacidade informacional. Afirmam: "A privacidade e segurança representam desafios relevantes e potenciais barreiras por parte das organizações que consideram adotar e aquelas que já contam com serviços e provedores em nuvem" (LYNN *et al.*, 2021, p. 89)[66].

É maior a preocupação com a segurança dos dados coletados e armazenados na *cloud* — distribuída em redes *online* — se comparada à segurança das informações localizadas num banco de dados local. Dois fenômenos potencializam os riscos da computação em nuvem para a privacidade informacional, conforme os autores supracitados. São eles: a popularização da *internet* das coisas (IoT)[67]; e a facilidade com que os dados em nuvem transitam entre países.

O fato da demanda constante de conexão por parte de dispositivos diversos, como a

---

[65] Tradução livre do original: "(1) Store, back up, and recover data- Protect your data more cost-efficiently—and at massive scale—by transferring your data over the Internet to an offsite cloud storage system that's accessible from any location and any device; (2) Analyze data- Unify your data across teams, divisions, and locations in the cloud. Then use cloud services, such as machine learning and artificial intelligence, to uncover insights for more informed decisions; (3)
Stream audio and video- Connect with your audience anywhere, anytime, on any device with high-definition video and audio with global distribution. Embed intelligence Use intelligent models to help engage customers and provide valuable insights from the data captured".

[66] Tradução livre do original: "Privacy and security represent important challenges and potential barriers, both for organizations considered adopted and those currently relying on cloud services and cloud service provides".

[67] No prefácio da obra de Magrani (2018), a OiT é descrita por Doneda como "[...] um termo que acaba evocando o aumento da comunicação entre máquinas pela internet (M2M, ou machine-to-machine, que recentemente ultrapassou em volume a comunicação interpessoal pela internet), o desenvolvimento de diversos utensílios (desde os prosaicos exemplos das geladeiras ou torradeiras ligadas à internet), além de micro dispositivos, como sensores que, dispostos das mais diversas maneiras para captar dados a partir de seu ambiente, tornam-se partes integrantes da internet" (MAGRANI, 2018, p. 11).

assistente virtual *Alexa*[68] que se conecta a lâmpadas; termostatos e até geladeiras da casa do usuário, proporciona a captação intensiva de dados que revelam hábitos corriqueiros do indivíduo e sua armazenagem em *clouds*.

Neste contexto, há além do desenvolvimento de perfil detalhado do usuário através do imenso montante de dados coletados, a troca das informações constante entre os *devices* através da rede comum integrada por computação em nuvem.

Isto resulta na preocupação com o fluxo dos dados em rede *online* e também na vulnerabilidade ao qual o indivíduo é exposto através do constante acompanhamento via coleta de dados em tantos dispositivos que os cercam ao mesmo tempo. O segundo fenômeno que Lynn *et al.* (2020) consideram nocivos à privacidade informacional é a fácil passagem entre fronteiras inerentes à natureza da *cloud computing,* a qual pressupõe redes de conexão independentes da fisicalidade.

Porém, ao menos para esta segunda característica apontada por Lynn *et al.* (2020) como problemática no uso da computação em nuvem, já existem previsões jurídicas que trazem a necessidade do provedor de nuvem observar os padrões de privacidade do país ao qual estão vinculados seus servidores (computadores físicos) e também seus *Data Center's*.

Para melhor compreensão da possibilidade de localizar a nuvem, principalmente para fins de proteção à privacidade informacional, é interessante explicar as características do *Data Center*. Ao fazê-lo, Nawaz (2019) pontua sua importância no mercado e também a necessidade de geri-los conforme as diretrizes de boas práticas, previstas nas normas locais que versam sobre dados pessoais (como o caso da LGPD). Ayomaya (2020) explica que:

> O Data Center existe para atender às necessidades de TI dos negócios. As empresas realizam suas necessidades de TI executando aplicativos em servidores, salvando dados no armazenamento e compartilhando informações por meio de redes. Esses blocos de construção de TI são configurados e operados no Data Center (AYOMAYA, 2020, p. 9)[69].

O *Data Center* pressupõe uma localização exata onde ocorre o funcionamento dos dispositivos que o constituem. Nele as estruturas em rede são possibilitadas junto aos serviços de software oferecidos na nuvem. Seus componentes se dividem basicamente em três

[68] A assistente virtual dialoga com outros produtos de uso cotidiano de maneira inteligente (computacional). Explica o site da Amazon sobre o funcionamento da alexa: "Produtos habilitados para funcionar com comandos de voz como: interruptores de luz, termostatos, pequenos aparelhos e outros. Os consumidores desenvolvem no final da experiência uma conexão como um "diálogo" com a inteligência artificial Alexa em muitas partes de sua casa, escritório ou quarto de hotel. Isso seria uma simulação para obter segundo à empresa [...]uma experiência verdadeira ambientação" Disponível em: <https://aws.amazon.com/pt/iot/solutions/connected-home/iot-and-alexa/>.

[69] Tradução livre do original: "The Data Center exists to meet the IT needs of businesses. Companies perform their IT needs by running applications on servers, saving data in storage, and sharing information through networks. These IT building blocks are configured and operated in the Data Center".

principais áreas abaixo listadas:

> Infraestrutura da instalação: que inclui edifício, segurança física, energia, refrigeração, sala de servidores e outro espaço para crescimento, sistema de gerenciamento de edifícios e sistema de gerenciamento de infraestrutura de data center; Infraestrutura de TI: que inclui rede, servidores, armazenamento, backup, sistemas operacionais, virtualização, sistema de gerenciamento empresarial e segurança de TI; Serviços: que incluem Helpdesk, Network Operation Center, Security Operation Center e vários aplicativos fornecidos para empresas/clientes (NAWAZ, 2019, p. 13)[70].

A infraestrutura da instalação dos *Data Center's* pode ser entendida como seu 'corpo' funcional. É a partir dos recursos físicos contidos nela que os softwares da tecnologia de nuvem são processados. Com localização certa que abriga a matriz do provedor de nuvem. Também se subdivide em recursos físicos utilizados para implementar o serviço diretamente contratado ou aquele contratado por terceiros.

Entender sobre os componentes que possibilitam o funcionamento da *cloud computing* é relevante para desmistificar a dificuldade de localizá-la. A partir das informações sobre a infraestrutura de instalação das empresas que fornecem serviços de *software* via tecnologia em nuvem, é possível definir parâmetros relacionados a segurança, identidade e responsabilidade das partes.

3.2 Segurança na *cloud computing* e suas implicações na Privacidade Informacional

Junto à popularização das ferramentas em *cloud*, que proporcionam maior poder de processamento computacional para a coleta e processamento de informações pessoais, modelos de negócio pautados na monetização de dados pessoais têm se tornado corriqueiros. Na maioria deles, com o auxílio de *Data Center's* e *softwares,* há o uso de ferramentas de aprendizado de máquinas para processar os dados fornecidos pelos usuários dos diversos aplicativos existentes *online*.

A consequência deste atual cenário é a necessidade do aumento dos padrões de segurança da informação, o que implica em questões de caráter técnico, que garantam a existência de um sistema acessível apenas para aqueles com permissão de manuseá-lo, junto ao armazenamento otimizado dos dados capaz de assegurar o ciclo da sua existência. Lynn *et al.* (2020) pontuam as três principais diretrizes da acessibilidade adequada: "confidencialidade; integridade; e a disponibilidade das informações" (LYNN *et al.,* 2020, p.

[70] Tradução livre do original: "Installation infrastructure: which includes building, physical security, power, cooling, server room and other space for growth, building management system and data center infrastructure management system; IT infrastructure: which includes network, servers, storage, backup, operating systems, virtualization, enterprise management system and IT security; Services: which include Helpdesk, Network Operation Center, Security Operation Center and various applications provided to companies/clients".

90)[71].

Cada fase do chamado “ciclo de vida das informações pessoais” segue uma ordem correspondente ao tratamento realizado. Um exemplo de boas práticas nessa área é o da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG), que disponibilizou, em uma das publicações do seu Comitê de Privacidade, uma tabela que relaciona cada etapa com a definição de tratamento prevista na própria LGPD brasileira:

Quadro 1 – Fase Do Ciclo Do Tratamento Correspondente A Operação De Tratamento

DADOS PESSOAIS	
FASE DO CICLO DE TRATAMENTO	OPERAÇÕES DE TRATAMENTO - LGPD, ART. 5º, X
Coleta	Coleta, produção, recepção
Retenção	Arquivamento e armazenamento
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Eliminação

(BRASIL, 2022)

É possível visualizar que a segurança da informação opera desde a coleta até a eliminação dos dados pessoais. Para ser garantida, é preciso que, a contar da captação dos dados, seja certificado ao titular o consentimento consciente, respeitando o princípio da necessidade[72], a eliminação completa das informações ao seu respeito presentes no banco de dados do controlador a qualquer momento do tratamento, segundo a solicitação de vontade do titular[73]. Para que isto aconteça efetivamente é necessário que o Controlador dos Dados siga

[71] Tradução livre do original: “Here is the translation of the text you provided:Confidentiality; Integrity; and Availability of information”.

[72] A LGPD define consentimento no Art. 5º, XII, como: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018). Já o princípio da necessidade é descrito na lei no Art. 6º, III: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: […] necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (BRASIL, 2018).

[73]Segundo a LGPD, o Art. 18, VI. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: […]

VI — eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

[…] As exceções presentes na mesma lei são as seguintes: Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I — cumprimento de obrigação legal ou regulatória pelo controlador;

II — estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III — transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV — uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018)

as chamadas ‘boas práticas’, previstas no texto da LGPD.

No Capítulo VII da Norma Geral de Proteção de Dados brasileira (Lei n. 13.709/2018) estão previstas as boas práticas de tratamento de dados. A primeira seção do capítulo trata do sigilo e segurança das informações, os quais exigem dos agentes de tratamento a adoção das medidas cabíveis para manter um padrão de segurança mínimo ao guardar os dados. Também é delineado o importante papel da Autoridade Nacional de Proteção de Dados (ANPD) brasileira, já que a ela cabe estabelecer as referidas exigências de segurança. O artigo 46º da norma prevê *in verbis* que*:*

> […] 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 (BRASIL, 2018).

É perceptível a importância dos padrões técnicos para a aplicabilidade eficiente da privacidade informacional, como também o papel da ANPD para dispor destes padrões, visando padronizá-los e fiscalizá-los.

Maurer e Hinck (2020) comentam as peculiaridades da segurança da *cloud computing*, como consequência da sua natureza em rede. Seja *online* (nuvem pública) ou não (rede local), esta característica gera insegurança para a maioria dos usuários e difere do nível de gravidade dos demais riscos apresentados à segurança cibernética do indivíduo. Os autores supracitados explicam:

> Primeiro, a computação baseada em nuvem é inerentemente conectada em rede. Finalmente, se discute como conectar esses riscos a impactos potenciais. Independentemente de depender de uma conexão com a Internet para a nuvem pública ou de uma rede especializada para uma nuvem privada, qualquer coisa na nuvem, até certo ponto, depende da rede. Isso significa que qualquer infraestrutura de nuvem envolverá segurança de rede e enfrentará ameaças potenciais que podem tirar proveito disso (MAURER; HINCK, 2020, p. 23)[74].

A insegurança gerada pela utilização da computação em nuvem tem respaldo no histórico de casos de incidentes. Dentre eles, Lynn *et al.* (2020) citam o ocorrido em 2019,

[74] Tradução livre do original: “First, cloud-based computing is inherently networked. Finally, how to connect these risks to potential impacts is discussed. Regardless of whether it relies on an Internet connection for the public cloud or a specialized network for a private cloud, anything in the cloud is network dependent to some extent. This means that any cloud infrastructure will involve network security and face potential threats that can take advantage of this”.

quando uma relevante empresa de gerenciamento de dados em nuvem, a *Rubrik*, expôs um grande *cache* de informações de clientes armazenadas indevidamente em um banco de dados da *Amazon Elasticsearch*.

Bisso *et al.* (2020) ressaltam na sua pesquisa sobre vazamento de dados pessoais que as instituições alvo vão desde grandes empresas especializadas em serviços digitais até outros setores, como organizações educacionais, de saúde — detentoras de dados pessoais em grande maioria sensíveis — e também membros da administração pública. Os autores supracitados exemplificam:

> Dois grandes vazamentos de dados, ambos envolvendo empresas de assistência medica, chamaram a atenção. No primeiro caso, a empresa *Quest Diagnostics* teve dados de 12 milhões de clientes vazados [McKay 2019]. Em outro caso similar, a empresa *LabCorp* teve dados de 7,7 milhões de clientes vazados [Lam 2019]. Os dados vazados incluem nomes, endereços, data de nascimento, informações de pagamento e dados de seguro social. Além de empresas laboratoriais, hospitais também tem sido vítimas de *hackers* [Riley 2019]. Em um caso recente, dados do setor de pesquisa do Massachusetts General Hospital foram roubados, envolvendo dados de aproximadamente 10 mil pacientes (BISSO *et al.,* 2020, p. 3).

Também há casos de vazamentos de dados pessoais listados por Bisso *et al.* (2020) ocorridos no Brasil. Alguns deles envolvem vulnerabilidades por parte de órgãos públicos e também atuação criminosa de *hackers* com *IP's* rastreados e localizados em solo estrangeiro, aponta:

> Recentemente foi descoberta uma página contendo dados de mais de 200 mil brasileiros [de Souza 2019b]. Dentre os dados contidos nos registros estão nome completo, endereço residencial e documentos de identificação (e.g.. CPF e RG). Não foi possível identificar a quem pertenciam os dados, porém, foi identificado que o IP de origem apontava para um servidor da Microsoft, nos EUA. Outro caso recente é o de um atacante que está vendendo dados de aproximadamente 92 milhões de brasileiros [llascu 2019]. Segundo noticiado, os dados foram roubados de uma base de dados do Governo. Além dos dados, ele ainda está vendendo serviços de busca utilizando esta e outras bases de dados. O hacker promete conseguir informações como endereços residencial e de email, dados de documentos (e.g., CPF e Carteira de Motorista) (BISSO *et al.*, 2020, p. 4).

Os incidentes de vazamento de dados, quando divulgados por veículos de mídia, cumprem a função de alertar os usuários dos potenciais riscos associados ao processamento de dados pessoais e também, como uma forma de trazer foco à discussão. Zuboff (2019) menciona que diversos estudos — realizados com a população dos Estados Unidos — apontam para a insatisfação das pessoas quando questionadas sobre o alto nível de falta de privacidade ao qual estão expostas online:

> Um levantamento significativo, em 2015, descobriu que 91% dos entrevistados discordavam de que a coleta de informação pessoal "sem o meu conhecimento" é uma troca justa para um desconto no preço. Já 55% discordavam de que era uma troca justa para aprimoramento dos serviços. Em 2016, a *Pew Research* relatou

> apenas 9% dos entrevistados como muito tranquilos em confiar seus dados a mídias sociais e 14% como muito tranquilos em confiar dados pessoais a empresas. Mais de 60% queriam fazer algo além para proteger sua privacidade e acreditavam que deveriam haver maior regulamentação para garanti-la (ZUBOFF, 2019, p.389).

Já no Brasil, um estudo publicado pela PUC em 2015 indicou a preocupação do brasileiro com a privacidade das informações pessoais. Com a amostragem de 1104 questionários completos, aplicados entre todas as regiões do Brasil "A população-alvo utilizada para este estudo foram os usuários de internet no Brasil, os quais, segundo a Pesquisa Nacional de Amostra de Domicílios de 2011, totalizavam 77,7 milhões (IBGE, 2013 *apud* BRITO-DA-SILVA *et al.*, 2015, p. 8). A pesquisa revelou forte preocupação dos brasileiros com seus dados pessoais, principalmente:

> Os resultados indicam uma forte preocupação com relação às informações de senhas, apontadas por 822 (74%) respondentes, número de cartão de crédito 806 (73%), número de conta corrente e agência 740 (67%), saldo bancário 712 (64%) e gastos com cartão de crédito 696 (63%) (BRITO-DA-SILVA *et al.*, 2015, p. 8).

Lynn *et al.* (2020) relatam que o volume alto de incidentes ocorridos guarda um certo nexo com as tensões adicionais decorrentes dos custos de detecção, prevenção e remediação dos incidentes *versus* o lucro que pode ser captado da realização de serviços de processamento dos dados. Logo, diante do risco de incidentes iminentes com os bancos de dados, as empresas têm mais lucros ao arcar com as consequências legais dos vazamentos do que deixarem de coletar dados do que em investir em segurança.

A resposta de diversos ordenamentos internos — envolvidos ou não de maneira direta em escândalos de vazamento de dados pessoais — aos incidentes que repercutiram sobre a segurança da privacidade dos indivíduos, de acordo com Lynn *et al.* (2020) é o aprimoramento da especificidade junto ao aumento no rigor da regulamentação de proteção à privacidade.

O autor vê como insuficientes os esforços de ampliação legislativa sobre o tema da privacidade de dados devido ao rápido ritmo de mudança das inovações na computação. Isto porque o crescimento exponencial da produção dos dados dos indivíduos através da utilização de plataformas digitais junto ao constante desenvolvimento de ferramentas para aprimorar a captação de informações — majoritariamente por parte das *Big Tech's* — está superando rapidamente o ciclo de vida legislativo das normas que tutelam o tema.

Lynn *et al.* (2020) corroboram a afirmação pessimista feita por Zuboff (2019), que enxerga a velocidade inerente ao capitalismo de vigilância como estratégica e a considera

como uma das respostas à indagação de como os modelos de negócios baseados na monetização dos dados e vulnerabilidade da privacidade dos indivíduos titulares têm conseguido alcançar o sucesso de maneira tão consistente. Explica:

> […] de maneira proposital, mobilizada para paralisar a consciência e congelar a resistência, ao mesmo tempo que nos distrai com desejos que são imediatamente satisfeitos. As velocidades do capitalismo de vigilância deixam para trás a democracia da mesma forma que deixam para trás nossa capacidade de entender o que está acontecendo e considerar as consequências. Essa estratégia é tomada de empréstimo de um extensivo legado de abordagens políticas e militares para a produção de rapidez como uma forma de violência, conhecida nos últimos tempos como "choque e pavor" (ZUBOFF, 2019, p. 392).

A velocidade com a qual as novas tecnologias aperfeiçoam o processamento de dados, a memória computacional, a autonomia de inteligências artificiais, dentre outras inovações técnicas que otimizam os serviços em nuvem, é, para Zuboff (2019), inerente ao capitalismo de vigilância regido pelas *Big Tech's*. A velocidade considerada paralisante dificulta a tutela das demandas tecnológicas, ao gerar nos agentes de políticas públicas a constante incapacidade de acompanhar as atualizações técnicas.

Os principais transtornos relacionados à Segurança de Dados na utilização da *cloud* foram listados por Carvalho *et al.* (2013) como demandas de confidencialidade, de disponibilidade e de integridade, que caracterizam mecanismos de proteção de dados pessoais:

> […] (i) criptografia: trata-se de um mecanismo essencial para a proteção de dados sigilosos através de técnicas de cifragem, largamente empregado em serviços e requerido por padrões legais e de mercado; (ii) redundância: corresponde a um mecanismo básico para evitar a perda de dados e garantir a disponibilidade de serviços. Para esse fim, ao menos as informações críticas de negócio devem ser protegidas em termos de integridade e disponibilidade;
> (iii) descarte ou remoção dos dados: deve ser completo e definitivo, ao contrário da maioria das técnicas disponíveis (por exemplo, Ext3, NTFS), que apenas removem as entradas dos índices do arquivo na tabela de alocação do sistema de arquivos (Dorion, 2010). Resquícios de dados podem constituir um sério problema de segurança caso as informações sejam sigilosas (CARVALHO *et al.*, 2013, p. 33).

O trecho transcrito foi publicado em 2013, para mapear as demandas de segurança na computação em nuvem. Na seção referente à proteção de dados pessoais, foi constatada a existência de três principais quesitos problemáticos: criptografia, redundância e descarte dos dados. O trabalho do qual é citado um trecho acima deu uma importante contribuição para o mapeamento de problemas até hoje existentes.

Porém, é ulterior a algumas normas, como o texto do Regulamento Geral De Proteção de Dados da União Europeia, publicado em 2016, com entrada em vigor em 2018, que dispõe de artigos garantidores do direito do titular dos dados pessoais ao anonimato e ao

"esquecimento" [75], dentre outros dispositivos que buscaram sanar diversas demandas jurídicas de proteção de dados. Ainda em 2018, a LGPD brasileira (Lei n. 13.709/2018) foi proposta e contou com dispositivos espelhados no Regulamento da União Europeia[76].

No ano de 2020 a LGPD entrou em vigor parcialmente[77] e trouxe soluções para alguns dos problemas citados acima por Carvalho *et al.* (2013). Ao descrever as demandas de segurança da *cloud,* Carvalho *et al.* (*idem*) também apresentam o tópico 'Questões Legais'. Nele são citados três principais problemas: a localização dos dados; os privilégios do provedor *e-Discovery;* e a disparidade legal oriunda da velocidade dos avanços técnicos:

> Localização dos dados: a localização precisa dos dados na nuvem é incerta, os dados podem estar distribuídos em diversos centros computacionais (por exemplo, data centers), em diferentes países e sob diferentes jurisdições. Essa situação pode gerar conflitos ao se moverem dados de uma localização geográfica para outra; e — Discovery: como resultado de uma decisão judicial, os dispositivos de armazenamento podem ser recolhidos para análise forense em uma investigação. Contudo, todos os usuários do serviço cujos dados estão armazenados nesses dispositivos terão seus dados expostos, comprometendo a confidencialidade dos mesmos; Privilégios do provedor: o provedor do serviço tem controle parcial ou total sobre sua infraestrutura, além de acesso físico ao hardware. Usuários internos maliciosos podem conduzir atividades que comprometam gravemente a integridade e a confiabilidade do serviço como um todo; Legislação: problemas legais relacionados aos novos conceitos e paradigmas introduzidos pelas tecnologias de computação em nuvem (CARVALHO *et al.*, 2013, p. 35).

No *Guia da Agencia Espanõla de Proteccion de Datos sobre cloud computing* (2013), ao serem listados os riscos da computação em nuvem, estes são agrupados em duas principais categorias: a "falta de transparência quanto às condições em que o serviço é prestado; e a falta de controle por parte do responsável pela utilização e gestão dos dados pessoais por parte dos agentes envolvidos no serviço" (ESPANHA, 2013, p.11)[78].

---

[75] "Art. 17. Direito ao apagamento dos dados (direito a ser esquecido):
"O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.o 1, alínea a), ou do artigo 9.º, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;(União Europeia, 2016)" Disponível em: <https://gdprinfo.eu/pt-pt/pt-pt-article-17>.

[76] Segundo o Capítulo III da Lei 13.709/2018, que versa sobre os Direitos do Titular: Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei […] IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei (BRASIL, 2018).

[77] No dia 18 de setembro de 2020, com a publicação da lei 14.058/20, colocou-se o ponto final em mais um capítulo acerca do tumultuado período de *vacatio legis* da Lei Geral de Proteção de Dados (LGPD). Não custa lembrar que nem todos os dispositivos da lei estão em vigor, o que, até segunda ordem, somente ocorrerá no dia 1º de agosto de 2021. Permanecem dormentes os arts. 52, 53 e 54, que tratam das sanções administrativas que poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD). Disponível em: <https://www.migalhas.com.br/depeso/337481/a-lgpd-finalmente-entrou-em-vigor--e-agora>.

[78] "falta de transparencia sobre las condiciones en las que se presta el servicio y falta de control del responsable sobre el uso y gestión de los datos personales por parte de los agentes implicados en el servicio".

A falta de transparência é entendida como negligência do provedor do serviço de nuvem, em virtude de seu conhecimento sobre os detalhes do encargo proposto. Dentre os detalhes que os clientes e os titulares dos dados devem saber estão: o motivo da coleta de informações; quem são os agentes e o método de tratamento; e onde estão localizados os computadores que desempenham a função de *hardware*. Há falha por parte do provedor:

> Se este não fornecer informações claras, precisas e completas sobre todos os elementos inerentes à prestação, a decisão adotada pelo responsável pelo tratamento não poderá atender adequadamente a requisitos básicos como a localização dos dados, a existência de subcontratantes, a controles de acesso à informação ou medidas de segurança (ESPANHA, 2013, p.11)[79].

Portanto, inexistindo a clareza no fornecimento das informações supracitadas, fica comprometida a função do provedor de avaliar os riscos e estabelecer os controles adequados. Como resultado, há o segundo principal risco da computação em nuvem, segundo o Guia Espanhol (2013), a falta de controle:

> […] pelas dificuldades de saber no momento sempre a localização dos dados, as dificuldades em ter os dados na posse do prestador ou em os conseguir obter num formato válido e interoperável, os obstáculos à gestão eficaz do tratamento ou, em suma, a falta de controlo eficaz quando definir os elementos substantivos do tratamento em termos de salvaguardas técnicas e organizacionais (ESPANHA, 2013, p.11)[80].

Apesar das demandas de proteção de dados lidarem com transferências em rede, fato que dificulta sua tutela, diversas atualizações legislativas buscaram sanar alguns dos problemas acima descritos. Afirmam Lynn *et al.* (2020) que foi fundamental o fato de existirem servidores e *Data Center's* tangíveis alocados numa determinada jurisdição, para a emergência da regulação do tema ao nível global. O GDPR europeu contribuiu fortemente para o surgimento de uma tendência regulatória nesse sentido:

> […] A ideia de vincular a aplicabilidade da lei de proteção de dados da UE ao uso físico de um equipamento não correspondia mais à realidade tecnológica. O GDPR agora regula os controladores de dados que não estão estabelecidos na UE, mas oferecem bens ou serviços na UE ou monitoram o comportamento dos titulares de dados europeus (Artigo 3 GDPR) (LYNN *et al.,* 2021, p. 75)[81].

---

[79] Tradução livre do original: "Si este último no da una información clara, precisa y completa sobre todos los elementos inherentes a la prestación, la decisión adoptada por el responsable no podrá tener en consideración de forma adecuada requisitos básicos como la ubicación de los datos, la existencia de sub encargados, los controles de acceso a la información o las medidas de seguridad. De esta forma, se dificulta al responsable la posibilidad de evaluar los riesgos y establecer los controles adecuados".

[80] "Ante las dificultades para conocer en todo momento la ubicación de los datos, las dificultades a la hora de disponer de los datos en poder del proveedor o de poder obtenerlos en un formato válido e interoperable, los obstáculos a una gestión efectiva del tratamiento o, en definitiva, la ausencia de control efectivo a la hora de definir los elementos sustantivos del tratamiento en lo tocante a salvaguardas técnicas y organizativas".

[81] "The idea of linking the applicability of EU data protection law to the physical use of equipment no longer corresponded to technological reality (Hon et al. 2012; Esayas 2012; Christopher Kuner 2010). The GDPR now.regulates data controllers who are not established in the EU but offer goods or services in the EU or monitor the behavior of European data subjects (Article 3 GDPR)".

Até o momento da elaboração do presente trabalho, não há na União Europeia um regulamento ou diretiva exclusivo aos serviços de *cloud*. Contudo, já existem discussões na Organização Internacional que deram origem a alguns dispositivos legais sobre o tema. Vigiani e Velasco (2012) descrevem que, em 2012, o Parecer 05/2012, definiu a computação em nuvem e a incorporou no artigo 29º da Diretiva n. 95/46/CE. Em seguida, no ano de 2014, o Parlamento Europeu expôs a necessidade de uma legislação específica sobre os serviços de nuvem.

Silva; Finkelstein (2014) comentam que houve um relatório por parte do Parlamento Europeu, publicado em outubro de 2013, que listou os pontos positivos e negativos do uso da tecnologia de *cloud*. Dentre os positivos destacaram-se "a redução de custos, a possibilidade de acesso a informações em qualquer lugar, a comodidade" (SILVA; FINKELSTEIN 2014, p. 514).

Dentre os pontos negativos, o mais relevante foi a existência de ocasiões nas quais os produtos em *cloud* implicam em transferência de responsabilidade por parte dos fornecedores dos serviços.

Depois de um salto de quase uma década, em 2022 a União Europeia publicou o Regulamento de Mercado Único, juntamente com a emenda à Diretiva *Digital Services Act* (2000/31/EC). A partir disto, a UE reconheceu a importância da sociedade da informação e dos serviços que a mesma proporciona:

> […] modelos e serviços empresariais novos e inovadores, como redes sociais em linha e plataformas em linha que permitem aos consumidores celebrar contratos à distância com comerciantes, permitiram que os utilizadores empresariais e os consumidores transmitissem e acedessem a informações e efetuassem transações de formas inovadoras. A maioria dos cidadãos da União já utiliza esses serviços diariamente. No entanto, a transformação digital e o aumento do uso desses serviços também resultaram em novos riscos e desafios para os destinatários individuais do serviço relevante, empresas e sociedade como um todo (UNIÃO EUROPEIA, 2022)[82].

Apesar de não tratar exclusivamente da tutela do serviço em nuvem, o regulamento distingue os serviços em rede, para melhor enquadrá-los em situações obrigacionais correspondentes. O regulamento do Mercado Único Digital reconheceu a importância dos

[82] Tradução livre do original: "new and innovative business models and services, such as online social networks and online platforms allowing consumers to conclude distance contracts with traders, have allowed business users and consumers to impart and access information and engage in transactions in novel ways. A majority of Union citizens now uses those services on a daily basis. However, the digital transformation and increased use of those services has also resulted in new risks and challenges for individual recipients of the relevant service, companies and society as a whole".

serviços e empresas presentes *online* e também os distinguiu em categorias, com finalidade de impor obrigações específicas correspondentes.

Ainda no âmbito das Organizações Internacionais, a Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), que costuma propagar as tendências das relações contratuais operantes no comércio internacional, publicou, em 2019, o documento intitulado *Notas Sobre os Principais Problemas dos Contratos de Computação em Nuvem* (*Notes on the Main Issues of Cloud Computing Contracts*). O objetivo deste foi o de mapear as demandas de Direito contratual privado referentes à *cloud computing*, a fim de solucioná-las.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), através de publicação aprovada pelo seu Comitê de políticas de Economia Digital (*Committee on Digital Economy Policy*) no ano de 2021, também tratou do uso da tecnologia de computação em nuvem para negócios. O documento, de nomenclatura autoexplicativa (*Measuring Cloud Services Use By Businesses*), visou construir uma real perspectiva sobre o papel dos serviços em nuvem na atual economia mundial.

Já no Brasil, mesmo com uma legislação destinada a tutelar o espaço digital publicada no ano de 2012 (Marco Civil da Internet) e com a recém-entrada em vigor da LGPD, não há na legislação vigente uma definição jurídica de *cloud computing*. Em 2013, houve a elaboração de um Projeto de Lei (PL 5344/2013) que versava sobre diretrizes a respeito da computação em nuvem, porém este acabou por ser arquivado.

Segundo a Agência Câmara de Notícias (2013), entre as condutas propostas destacava-se o reconhecimento do caráter não geográfico do acesso aos dados, somado à neutralidade tecnológica e de rede, que consiste na proibição de qualquer privilégio para uma tecnologia, plataforma ou aplicativo. Também no projeto, havia ainda a sugestão da exclusão de informações a pedido do titular.

Mesmo o referido projeto arquivado no ano de 2015, a LGPD proposta contemplou algumas questões aludidas pelo PL 5344/2013, como a previsão da transferência internacional de dados pessoais junto ao direito ao esquecimento das informações do usuário, a depender de sua solicitação.[83] Isto ocorreu porque os serviços de *cloud* costumam ser utilizados majoritariamente a partir de operações realizadas com dados pessoais.

A tendência da tutela da temática de proteção de dados pessoais por meio das

[83] Previstas na lei o direito à solicitação da eliminação dos dados a qualquer momento mediante solicitação ao Controlador no Art. 18, VI, CAPÍTULO III (DOS DIREITOS DO TITULAR) e CAPÍTULO V (DA TRANSFERÊNCIA INTERNACIONAL DE DADOS) (BRASIL, 2018).

Organizações Internacionais e também de ordenamentos jurídicos internos, como foi até aqui mostrado, já é uma realidade. Porém, as implicações advindas da computação em nuvem têm se tornado uma temática pertinente nas OI's, costumando suscitar os rumos normativos da prática comercial internacional.

Na próxima seção, serão discutidas as implicações contratuais dos serviços em nuvem.

3.3 Implicações Contratuais dos serviços em nuvem

A facilidade na transferência de dados entre locais distintos, característica da *cloud computing*, acaba por criar uma demanda legislativa comum em Estados díspares. Sua estrutura em rede ocasiona "transferências contínuas de dados em uma escala global, e o interesse de uma multiplicidade de Estados, na medida que o procedimento de fragmentação utilizado pela tecnologia particiona e transfere dados automaticamente" (LYNN *et al.,* 2020, p. 73)[84].

Ao pormenorizar os desafios jurídicos que a contratação de serviços em nuvem contém, Gómez (2013) destaca diversos aspectos em áreas distintas do Direito, desde a proteção de dados até as possíveis atuações criminosas:

> […] decorrem de diferentes aspectos do direito como: proteção de dados, transferência internacional de dados, propriedade intelectual, segurança da informação armazenada na nuvem, processo penal, responsabilidade civil, direito concorrencial e tributário têm como eixo comum o problema do direito aplicável aos contratos e sob qual jurisdição os atos jurídicos foram realizados (GÓMEZ, 2013, p.10)[85].

Das demandas jurídicas que a tecnologia em nuvem traz consigo, a maioria delas é causada pela sua característica mais marcante: a ubiquidade oferecida. A estrutura em rede que a define gera dificuldades em distinguir as partes do contrato, causando implicações à responsabilidade dos agentes e a eleição do foro competente.

Apesar do Direito Internacional Privado dispor de familiaridade com negócios transfronteiriços desde os primórdios da sua criação, o ramo tem se deparado com demandas crescentemente complexas fruto do uso dos meios digitais para negócios e transações.

---

[84] Tradução livre do original: "Continuous transfers of data on a global scale, and the interest of a multiplicity of States, since the fragmentation procedure used by technology partitions and transfers data automatically".

[85] Tradução livre do original: "[…] surgen desde diferentes vertientes del derecho como: la protección de datos, la transferencia internacional de datos, la propiedad intelectual, la seguridad de la información almacenada en la nube, las actuaciones criminales, la responsabilidad civil, el derecho de la competencia y los impuestos tienen como eje común el problema de la ley aplicable a los contratos y bajo qué jurisdicción se realizaron los actos jurídicos".

Dentre as demandas existentes, tem destaque a proteção de dados pessoais através da presença normativa tanto nas Organizações Internacionais — têm ao menos uma publicação sobre o tema a OCDE; UNCITRAL; União Europeia e a OEA — e também nos ordenamentos internos de diversos países em distintas regiões do mundo (como Brasil, Japão e Estados Unidos em certa medida).

Surge daí a necessidade de investigar as peculiaridades contratuais dos serviços de nuvem a partir da proteção de dados pessoais, junto a outras demandas jurídicas que se destacam no âmbito contratual, tais como: a definição das partes; a responsabilidade; a elegibilidade do foro competente para solução de controvérsias, dentre outras questões que dizem respeito ao Direito Contratual Internacional.

De acordo com Morelli (2018), as inovações tecnológicas geraram aceleração nas transações internacionais junto a uma diluição das limitações geográficas através da virtualização das negociações e a consolidação do mercado eletrônico, que conecta partes em localidades distintas com muita facilidade. A existência de um mercado unicamente digital trouxe consigo características importantes para conceitos contratuais basilares. Dentre elas está o impacto no espaço-tempo das transações realizadas. O supracitado autor explica esse ponto nos seguintes termos:

> De fato, a integração econômica demandou mais do que um simples aumento de importações e exportações com redução de tarifas ou mesmo sua retirada completa, mas resultou em verdadeiros aumentos de investimentos trans-fronteiras de capital intangível (finanças, tecnologia, informação, ativos estrangeiros diretos nos países, aumento no fornecimento e diversidade de serviços), aumento nas transações internacionais pela internet e fornecimento de novos produtos para mercados consumidores (MORELLI, 2022, p. 40).

Luiz Olavo Baptista (1995) ao tratar do tema da inserção do elemento eletrônico nas operações comerciais, afirma não haver mudança na finalidade basilar das mesmas. Segundo ele, “o que é novo, nelas, é o uso dos meios de comunicação à distância, e que estes são eletrônicos, não a sua finalidade ou estrutura” (BAPTISTA, 1995, p. 14).

Decerto, o fornecimento dos serviços de *cloud* pressupõem estruturas contratuais há muito estabelecidas, junto ao objetivo final, o de atender as demandas dos serviços oferecidos pelo *software*. Porém, o elemento novo adicionado a transações desta natureza é a maneira como o serviço é ofertado: descentralizado e em redes.

Silva *et al.* (2018) trazem dados obtidos através do estudo realizado pela empresa alemã especializada em pesquisa de mercado, a *Growth from Knowledge* (GfK) que revelou ser essencial aos brasileiros o acesso ou o armazenamento de arquivos em nuvem. O estudo

também mostrou que o Brasil, dentre vinte e dois países analisados, está em segundo lugar dos países que mais acessam a tecnologia em *cloud* (SILVA *et al*. 2018, p. 95).

Gasser (2014) menciona que os contratos tiveram papel de protagonismo quando se trata das demandas jurídicas dos serviços de nuvem e de inovações tecnológicas, em geral. Ele destaca duas fases distintas nas quais houve evolução na matéria. Na primeira, os "provedores de nuvem e clientes abordaram questões centrais, usando acordos contratuais para identificar e alocar riscos e responsabilidades e criar mecanismos de fiscalização onde as regras existentes são inadequadas" (GASSER, 2014, p. 17)[86].

As adequações alavancadas pelas negociações no mercado de desenvolvimento tecnológico incluem regras sobre privacidade informacional e segurança dos dados, também padrões mínimos de oferecimento de serviços, dentre outras. Gasser (2014) conclui a explanação sobre a primeira fase, mencionando como os termos contratuais de serviços em nuvem continuam a progredir e trazem consigo avanços para mercados relacionados.

A segunda fase da utilização dos moldes contratuais como forma de padronização legal das inovações tecnológicas em nuvem é marcada pelo reconhecimento da importância dos contratos, junto do reconhecimento da sua "complexidade, insegurança jurídica e as assimetrias de poder entre as partes de um acordo". Para Gasser (*idem*), é a partir desta segunda fase que os diversos agentes interessados passam a elaborar modelos de boas práticas. Ele apresenta um exemplo:

> Por exemplo, Chief Information Officers Council (CIO), em colaboração com outras unidades governamentais, desenvolveu diretrizes para computação em nuvem eficaz contratos para o governo federal. Mais amplamente, a Comissão Europeia anunciou o desenvolvimento de "termos e condições de contrato seguros e justos" como parte de sua estratégia de nuvem e criou recentemente um grupo de especialistas sobre este tópico (GASSER, 2014, p. 17)[87].

O exemplo citado do *Chief Information Officers Council* (CIO) dos Estados Unidos diz respeito à publicação feita em 2012 visando listar diretrizes para a utilização de contratos de nuvem, nos quais fosse parte contratante o Governo Federal dos Estados Unidos[88]. Já a

---

[86] Tradução livre do original: "cloud providers and customers have addressed core issues using contractual agreements to identify and allocate risks and responsibilities and create enforcement mechanisms where existing rules are inadequate".

[87] Tradução livre do original: "For instance, the US CIO Council, in collaboration with other government units, developed guidelines for effective cloud computing contracts for the federal government.More broadly, the European Commission announced the development of "safe and fair contract terms and conditions" as part of its cloud strategy and recently set up an expert group on this topic".

[88] US CIO Council and Chief Acquisition Officers Council, "Creating Effective Cloud Computing Contracts for the Federal Government". (February 24, 2012). Disponível em: <https://cio.gov/wpcontent/uploads/downloads/2012/09/cloudbestpractices.pdf>.

União Europeia, como visto na seção anterior, possui breve menção legislativa à computação em nuvem nas recentes publicações sobre o Mercado Único Digital[89].

Ao realizar sua análise legal dos contratos de serviço em nuvem, Gómez (2018) apontam que o conflito inicial entre a parte contratante do serviço em *cloud* e seus provedores, intitulados de *Cloud Service Providers (CSP),* reside no fato do consumidor não saber ao certo a localização de suas informações. Uma vez bem definidas as partes, é estabelecido qual é o tipo de relação jurídica contratual e a legislação que lhe será aplicada e isso depende da localização dos contratados.

Sony *et al.* (2013) apontam a utilização de mitigação dos riscos via contrato como a estratégia mais utilizada pelos agentes que provêm os serviços de *cloud computing*. Nos casos de contratos com empresas que vão usar os serviços, os provedores usam contratos padronizados (*standart-form*), nos quais é alocada a jurisdição para o local no qual a organização do usuário está, ao invés da localidade do provedor da nuvem.

Os autores supracitados concluem haver dificuldade por parte de contratantes de médio e pequeno porte para alterar ou negociar os termos dos contratos padronizados, constatando desvantagem para os mesmos. Ao desenvolverem um trabalho mais prático, a partir do ponto de vista da área de engenharia de *software*, os autores Zalazar *et al.* (2013) descrevem os *Service Level Agreements* (SLA), um documento utilizado nos negócios realizados entre o provedor e o consumidor do serviço em *cloud*, como explicam nos seguintes termos:

> O SLA é um documento comercial entre o provedor e o consumidor do serviço, onde as condições em que um serviço será prestado e as compensações são definidas que será eficaz quando as condições detalhadas não forem atendidas. Este documento especifica os requisitos funcionais, a qualidade do serviço e as variáveis monetárias que serão regidas durante o período de vigência do contrato. Bianco *et al.* separam os SLAs de tecnologia da informação em três categorias: básico, médio e avançado (ZALAZAR *et al.*,2013, p. 306)[90].

---

[89] "Proposta pela Comissão Europeia em 2015, a estratégia para o mercado único digital lançou as bases para uma sociedade digital europeia unida e sustentável. Em 2016 e 2017, seguiram-se algumas realizações marcantes: o fim das tarifas de itinerância (*roaming*); a modernização da proteção de dados a portabilidade transfronteiras de conteúdos em linha acordo para desbloquear o comércio eletrónico que põe fim ao bloqueio geográfico injustificado". Disponível em: <https://www.consilium.europa.eu/pt/policies/digital-single-market/>

[90] Tradução livre do original: "El SLA es un documento de negocio entre el proveedor y el consumidor de servicio, donde se define las condiciones en que un servicio será provisto y las compensaciones que serán efectivas cuando no se cumplan las condiciones detalladas. Este documento especifica los requerimientos funcionales, la calidad del servicio y las variables monetarias que se regirán durante el periodo de validez del acuerdo.Bianco y colaboradores separaran los SLA de la tecnología de información en tres categorías: básica, mediana y avanzada".

No trecho acima são descritas as três categorias nas quais o SLA pode ser enquadrado. A partir da definição de Bianco; Lewis; Merson (2008), os SLA's utilizados no ambiente de tecnologia da informação podem ser:

> 1. básico – um único SLA com métricas bem estabelecidas que são medidas e/ou verificadas. A coleta dessas métricas geralmente é feita manualmente.
> 2. médio – introdução da qualidade multinível baseada no custo do serviço. O objetivo é equilibrar os níveis de qualidade e custo. A coleta automática de dados permite relatórios abrangentes para gerentes de TI e partes interessadas.
> 3. avançado - alocação dinâmica de recursos para atender à demanda à medida que as necessidades de negócios evoluem. (BIANCO; LEWIS; MERSON, 2008, p.5)[91].

Pode-se compreender o SLA como um documento de métricas, que pode variar do nível básico ao avançado, a depender, por exemplo, do volume de dados tratados ou da dimensão do serviço em nuvem contratado. Undheim *et al.* (2011) identificam que dentre os problemas de aderência da nuvem por parte de clientes, destaca-se a dificuldade de garantia (*assurance*)[92].

O SLA é visto como resposta à principal barreira de adoção dos serviços em *cloud* relativa aos questionamentos do cliente sobre a segurança a ele proporcionada ao fornecer dados para serem armazenados nas aplicações em serviços de nuvem. O uso do SLA funciona "para explicitamente declarar as obrigações do provedor, os mecanismos de segurança, sua eficácia e as implicações de uma possível má gestão fazem parte deste tipo de acordo"[93] (UNDHEIM *et al.*, 2011, p. 636).

Por fim, Zalazar *et al.* (2013), ao relacionarem o uso do SLA aos serviços de nuvem, aconselham os contratantes a avaliar de maneira detalhada o acordo apresentado pelo provedor de *cloud*, esmiuçando-o sobre questões tais como:

> […] as multas propostas, que podem não ser compatíveis com o impacto que representa uma violação dos objetivos do serviço; os pontos de segurança; os mecanismos termos de serviços; a modalidade de processamento crítico; e a guarda

---

[91] Tradução livre do original: " [...] 1. basic – a single SLA with well-established metrics that are measured and/or verified. The collection of these metrics is typically done manually. 2. medium – the introduction of multi-level quality based on the cost of the service. The objective is to balance the levels of quality and cost. Automatic data collection enables comprehensive reporting to IT managers and stakeholders. 3. advanced – dynamic allocation of resources to meet demand as business needs evolve".

[92] A palavra 'assurance' está relacionada, no âmbito empresarial e contratual, muitas vezes a chamada Quality assurance, que nada mais é do que "o conjunto de atividades que tentam garantir que o produto ou serviço oferecido esteja de acordo com o nível de qualidade exigido. Seu propósito é atingir os objetivos do projeto avaliando o desempenho com base em padrões de qualidade relevantes e também nos requisitos do cliente". Ou seja, este termo se refere e pode ser traduzido como 'garantia'. Disponível em: <https://gaea.com.br/afinal-o-que-e-quality-assurance/#:~:text=O%20Quality%20Assurance%20é%20o,também%20nos%20requisitos%20do%20cliente.>.

[93] Tradução livre do original: "used to explicitly state the obligations of the provider, the implemented security mechanisms, their effectiveness and the implications of possible mismanagement should be a part of this agreement".

> das informações oferecidas pelo prestador de serviços (ZALAZAR *et al.*, 2013, p.307)[94].

Os autores do trecho supracitado apresentam o SLA como essencial à espécie contratual tratada na presente dissertação. A partir das práticas disponibilizadas pela *Information Technology Infrastructure Library* (ITIL), é descrito ainda por Zalazar *et al.* (*idem*) que a utilização do SLA juntamente aos contratos de *cloud* faz parte do chamado processo de gestão de nível de serviço (SLM), que pode ser caracterizado pelas ações que determinam, documentam e acatam os requisitos para execução dos serviços contratados.

Por fim, Zalazar *et al.* (*idem*) descrevem a importância das partes envolvidas no serviço conhecerem e entenderem os conceitos principais e também as relações-chave para a contratação de serviços de computação em nuvem. Eles recomendam como indispensável a realização do acordo de serviço junto à definição das responsabilidades das partes envolvidas. Com o fim de melhor entender a responsabilização que lhes pode ser atribuída, são apresentados os sujeitos que toma parte do serviço:

> Consumidor: entidade que mantém uma relação comercial para utilizar um serviço; Provedor: entidade que fornece um determinado serviço para um consumidor; Transportador: intermediário responsável por oferecer conectividade e transporte de serviços e dados dos ambientes do provedor para os do consumidor do serviço; Broker: intermediário que se encarrega de negociar a relação entre fornecedores e consumidores. Auditor: entidade encarregada de relatar o *status* das operações, o desempenho e segurança das implementações em nuvem. (ZALAZAR *et al.*, 2013, p.309)[95].

São descritas cinco figuras-participantes dos contratos de serviços em *cloud computing:* os consumidores; os provedores; o transportador; o *broker* e o auditor. É possível entender a partir do trecho acima que o consumidor descrito é uma organização de cunho empresarial e não pessoa física dotada de hipossuficiência pressuposta na relação com o consumidor final. A análise dos autores é feita a partir da negociação entre duas empresas prestadoras de serviços.

Logo, a figura do provedor equivale à do fornecedor do ambiente em nuvem e o consumidor à empresa utilizadora dos serviços de *software* como meio de estrutura para então

---

[94] Tradução livre do original: "las compensaciones propuestas, ya que pueden no ser acordes al impacto que represente una violación a los objetivos del servicio. Igualmente, el consumidor debe estudiar los puntos de seguridad, los mecanismos de modificación de los términos de servicios, la modalidad de procesamiento crítico y reguardo de la información que ofrezca el proveedor del servicio".

[95] Tradução livre do original: "Consumidor: entidad que mantiene una relación de negocio para poder utilizar un servicio.Proveedor: entidad que brinda un determinado servicio para algún consumidor Transportador: intermediario que se encarga de ofrecer conectividad y transporte de los servicios y los datos desde los entornos del proveedor a los del consumidor del servicio Bróker: intermediario que se encarga de negociar la relación entre los proveedores y consumidores. Auditor: entidad encargada de informar el estado de las operaciones, el rendimiento y la seguridad de las implementaciones cloud".

prestar serviços ou oferecer produtos ao consumidor final, o qual, conforme a LGPD, é o titular dos dados pessoais.

Para a atribuição de responsabilidade, tem destaque o transportador. Ele tem o papel de garantir que as informações do titular coletadas previamente e armazenadas em bancos de dados do provedor ou na própria empresa consumidora, transitem com segurança. Para isto, ele possui a obrigação contratual (dispostas no SLA) de garantir padrões técnicos de segurança. Geralmente, o transportador será submetido hierarquicamente, do ponto de vista jurídico, ao provedor.

O *broker* tem a função de assimilar as vontades das partes da transação, e de integrar os interesses de ambos da melhor forma possível, para o adequado andamento da negociação de fornecimento da computação em nuvem, trabalhando junto ao auditor, que possui a função técnica de supervisionar e registrar questões relativas à funcionalidade, eficiência e segurança. Caso ocorra algum acidente relacionado à operação do *Data Center,* servidores físicos ou não, caberá ao auditor apontar as falhas técnicas e, eventualmente, reportá-las.

Entendidas as partes presentes nos servidores de nuvem e na relação contratual, serão apresentadas as possibilidades de responsabilidade destes, conforme a LGPD. Os contratos eletrônicos, em específico o contrato entre o provedor de nuvem e o consumidor, para Silva *et al.* (2018) são definidos como “os contratos pactuados entre os respectivos provedores e os usuários, nada mais sendo do que contratos de adesão”, nos quais, ao ser finalizado, pressupõe a adesão às condições gerais trazidas por uma das partes. Terminam por dizer que fica a critério do contratante (outra parte) aceitar ou não.

Ao trazer como exemplo o estudo comparado realizado por eles entre termos de responsabilidade de dois grandes provedores de *cloud computing*, Silva *et al.* (2018) concluíram existir por parte da *Google* e *Microsoft* o objetivo de se eximirem da responsabilidade no tocante à recuperação de dados, tais como fotos e outros arquivos que sejam perdidos.

Em seguida, ao apresentarem questões relevantes sobre os contratos eletrônicos celebrados entre os provedores e os consumidores, destacam que geralmente eles são feitos através do modelo *click-through agreements.* Esses contratos se diferenciam dos demais na forma de aceite dos termos. Citando Finkelstein (2011), os autores supracitados apontam que há desvantagem nos seguintes pontos:

> a) existirem cláusulas abusivas, em razão da falta de negociação; b) serem a maioria dos contratos eletrônicos, contratos de adesão; c) estar a privacidade dos usuários ameaçada, em função da falta de segurança no ciberespaço; d) possibilitarem a

> suscitação de dúvidas quanto às assinaturas digitais e às autoridades certificadoras (FINKELSTEIN, 2011, p. 177 *apud* SILVA *et al.*, 2018) .

Esses contratos podem ser regidos pelo Código de Consumidor Brasileiro ao depender das características da empresa parte da relação de consumo do serviço em nuvem. Geralmente, constatada a falta de equidade entre a organização provedora de *cloud* e a contratante do serviço de *software,* poderá ser atribuída à relação de consumo a fim de evitar a concretização de cláusulas abusivas.

Como o trabalho de Silva *et al.* (2018) foi publicado antes da LGPD, é importante mencionar que o texto da lei trouxe mudanças para transações que envolvem tratamento e transferências de dados, dentre elas destacando-se uma melhor definição dos agentes, da proteção ao titular e uma mais detalhada atribuição de responsabilidade.

Um dos elementos do texto da LGPD referido ao que estamos discutindo é a definição do Controlador e do Operador dos Dados. Tal definição é importante para a atribuição de responsabilidade na esfera contratual, representando o objetivo, buscado pelos legisladores, de garantir a proteção do titular dos dados, a pessoa física.

O Controlador dos dados é definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018). Pode ser descrito como o agente que dá causa à coleta e tratamento dos dados que tenham o interesse de utilizar as informações pessoais dos titulares para fins monetários. Geralmente, a figura do Controlador é ocupada por uma empresa especializada em tecnologia (pessoa jurídica). Na computação em nuvem, o Controlador ocupa o papel do *Cloud Service Providers (CSP)*.

Já o operador dos dados é definido pela lei brasileira como a figura responsável pela parte técnica do tratamento dos dados pessoais. Também pode ser "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018).

É possível que esta função seja desempenhada pela empresa provedora da *cloud computing*, colocando o Operador como mero encarregado da mesma, como também pode ser desempenhada por empresa terceirizada contratada pelo controlador, na figura de provedor de nuvem. Nos sujeitos do contrato em nuvem descritos previamente nesta seção, o operador equivale ao transportador dos dados.

O encarregado, descrito no artigo oitavo da LGPD, é equivalente ao *broker* pois sua função é a de estabelecer o diálogo entre os titulares dos dados e a Autoridade Nacional de

Proteção de Dados (ANPD) (BRASIL, 2019)[96]. O encarregado deve ser pessoa indicada pelos agentes de tratamento (Controlador e Operador). Logo, as ações do encarregado estão diretamente vinculadas aos mesmos.

Sobre as atribuições do Controlador, a LGPD dispõe que serão fornecidas informações claras a respeito de como será realizado o tratamento dos dados. É previsto como requisito para o tratamento dos dados por parte do Controlador que seja "necessário para atender aos interesses legítimos do controlador ou de terceiros" (BRASIL, 2018). Este inciso retrata o princípio da necessidade, que deve estar bem estabelecido no contrato com o consumidor do serviço em nuvem.

A LGPD, em seu Capítulo Quarto, Terceira Seção, trata da responsabilidade e do ressarcimento dos danos causados por acidentes advindos do tratamento dos dados pessoais. A Lei prevê que o dano causado a outrem em razão do exercício do tratamento de dados pessoais, seja de natureza patrimonial; moral individual ou coletiva, que seja fruto de violação à Lei n. 13.709/2018, atribuiu a responsabilidade de repará-lo ao Controlador e ao Operador, de maneira una ou solidária[97].

Há a possibilidade dos agentes de tratamento responderem ao dano causado de forma solidária. São os casos nos quais o Operador viola a norma (LGPD) a partir do descumprimento das orientações, quando lícitas, que foram explicitamente ditadas pelo Controlador. Ao Controlador também é exequível a responsabilidade solidária quando o mesmo estiver imediatamente ligado ao tratamento irregular de dados que cause dano para o titular das informações.

Mediante provas, serão isentos de responsabilidade os agentes de tratamento (controlador e operador), nas ocasiões previstas no artigo 49 da LGPD, situações nas quais os agentes não realizaram o tratamento que resultou danos ao titular; uma vez tendo realizado o tratamento, não desrespeitam a norma de proteção aos dados; caso o dano seja comprovadamente culpa do titular ou de terceiros.

Também é necessário que o contrato de serviço em nuvem se atenha ao capítulo quinto da LGPD, que trata da transferência internacional dos dados. O artigo 33 da norma prevê que só será permitida a transferência internacional de dados pessoais "para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei" (BRASIL, 2018).

---

[96] Redação dada pela Lei n. 13.853, de 2019.
[97] Artigo 42º da Lei n. 13.709/2018 (LGPD).

A LGPD também exige que o Controlador comprove o cumprimento dos princípios da lei, das garantias aos direitos do titular e do regime de proteção de dados previstos no país ou organismo destinatário da transferência. São listados como forma de fazê-lo, *in verbis:*

> […] a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos (BRASIL, 2018).

Logo, é de extrema importância para a forma contratual dos serviços em nuvem a presença de cláusulas específicas sobre a transferência internacional, somada a cláusulas-padrão sobre a proteção dos dados. Além disso, a própria lei brasileira reforça o princípio da adequação como requisito para possibilitar transações entre países com ordenamentos distintos.

O princípio da adequação torna exigíveis padrões legais mínimos de proteção de dados ao país terceiro, destinatário da transferência dos dados. Também é destaque no Art. 33 a observância de normas corporativas globais, amplamente utilizadas porque simplificam a dinâmica do diálogo comercial internacional.

O princípio da necessidade e da adequação presentes na LGPD aplicam-se veementemente às transferências internacionais de dados. A legislação elegível e a jurisdição das normas é mencionada já no Art. 3º da lei, no qual é garantida a aplicabilidade da LGPD, *in verbis:*

> a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público, ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados desde que o tratamento seja feito em território nacional; e os dados pessoais objeto do tratamento tenham sido coletados em território brasileiro (BRASIL, 2018) [98].

Como a lei se isenta de tutelar o tratamento de dados pessoais "realizado por pessoa natural para fins exclusivamente particulares e não econômicos" (BRASIL, 2018) [99], a LGPD

---

[98] […] o § 1º do artigo 3º define que "Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta" .(BRASIL, 2018)

[99] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018).

pode ser estabelecida como norma elegível para solucionar demandas advindas do tratamento de dados que implicam ganho financeiro. Os serviços de nuvem realizados por determinado provedor podem possuir cláusulas que os vinculam à lei brasileira, caso cumpra os requisitos para afirmar que o tratamento será ou foi realizado no território brasileiro.

É certo, a partir do até aqui estudado, que as particularidades do serviço em nuvem fazem necessária uma norma específica para tutelar seus serviços e contratos. Porém, no tocante à proteção de dados pessoais, a norma brasileira fez-se presente na tendência normativa sobre tema desencadeada principalmente pela observância das Organizações Internacionais. Bennett (1999) intitula-se de "fenômeno de Convergência", no próximo capítulo.

Ao versar sobre o tema, a Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL) trouxe esclarecimentos relevantes a algumas das principais peculiaridades atribuídas aos contratos de serviço em nuvem. Dentre elas, em um documento de 2019 da referida Comissão, destacam-se como principais disposições pré-contratuais: a definição da localidade dos dados; a definição das partes; os tipos de serviços dispostos pela nuvem e um glossário de terminologias técnicas.

Ao definir os sujeitos e relações aos quais se direcionam as diretrizes, é especificado o endereçamento aos agentes comerciais, no papel de provedor a outra parte, o consumidor final. Assim, ficam excluídos os contratos de distribuição do provedor a outros provedores de serviços de softwares em nuvem, *in verbis*:

> As presentes Notas abordam as principais questões de contratos de computação em nuvem entre entidades comerciais em que uma parte (o provedor) fornece à outra parte (o cliente) um ou mais serviços de computação em nuvem para uso final. Contratos de revenda ou outras formas de distribuição adicional de serviços de computação em nuvem estão excluídos do escopo (UNCITRAL, 2019)[100].

Sobre a localização dos dados pessoais — que, em regra, está relacionada à localidade do *Data Center* — a UNCITRAL define que deve seguir as diretrizes da lei aplicável aos dados pessoais do foro elegido para reger o contrato:

> […] leis e regulamentos de controle de exportação que podem restringir a transferência de certas informações ou software de ou para determinados países ou uma região. Conformidade com os requisitos de localização de dados estabelecidos na lei aplicável seria de suma importância para as partes. O contrato não seria capaz de substituir esses requisitos (UNCITRAL, 2019, p. 3)[101].

---

[100] tradução livre do original: "These Notes address the main issues of cloud computing contracts between commercial entities where one party (the provider) provides the other party (the customer) with one or more cloud computing services for end use. Reseller agreements or other forms of further distribution of cloud computing services are excluded from the scope".

[101] Tradução livre do original: "Export control laws and regulations that may restrict the download of certain information or software from or to certain countries or a region. Compliance with data location requirements

Há também a sugestão de cláusula referente aos riscos referidos à segurança, à integridade, à confidencialidade e à privacidade, implicados na migração de dados pessoais para uma nuvem.

É também importante destacar o trabalho reservado às terminologias específicas do uso da tecnologia em nuvem. No ponto 41 é tratada a referida necessidade:

> Devido à natureza dos serviços de computação em nuvem, os contratos de computação em nuvem contêm necessariamente muitos termos técnicos. O glossário de termos pode ser incluído no contrato, assim como as definições dos principais termos utilizados ao longo do contrato, para evitar ambiguidades na sua interpretação. As partes podem considerar o uso de terminologia estabelecida internacionalmente visando garantir consistência e clareza jurídica (UNCITRAL, 2019, p. 12)[102].

É importante mencionar a tutela da UNCITRAL sobre o tema, devido à relevância principiológica que opera sobre os ordenamentos jurídicos internos/nacionais. Bonell (2018) explica que ainda há, mesmo que diante do "crescimento sem precedentes no volume e do desenvolvimento de mercados cada vez mais integrados — se não em um, pelo menos ao nível regional" (BONELL, 2018, p. 16)[103].

A sujeição das transações comerciais transfronteiriças, na maioria, às leis nacionais. Porém, o autor termina por afirmar que, o papel das OI acaba sendo o de influenciar as legislações internas através do viés principiológico e costumeiro.

---

maintained in applicable law would be of paramount importance to the parties. The contract would not be able to override these requirements".

[102] Tradução livre do original: Due to the nature of cloud computing services, cloud computing contracts necessarily contain many technical terms. The glossary of terms can be included in the contract, as well as the definitions of the main terms used throughout the contract, to avoid ambiguities in its interpretation. Parties may consider using internationally established terminology to ensure consistency and legal clarity.

[103] Tradução livre do original: "Unprecedented growth in volume and the development of increasingly integrated markets - if not at one, at least at the regional level".

4 A TESE DE CONVERGÊNCIA NA PROTEÇÃO DE DADOS PESSOAIS

4.1 Convergência e sua presença na proteção de dados, de acordo com Bennett

A fim de explicar o que é a convergência no âmbito das diretrizes jurídicas, Drezner (2001) aponta que mesmo potencializada pela intensificação da globalização permitida pela popularização dos meios de comunicação computacionais desde os anos de 1980, os estudos sobre a convergência jurídica e política internacional são realizados desde os primórdios do fluxo fronteiriço entre Estados-Nação.

O autor descreve a importância dos avanços tecnológicos nos meios de comunicação e de transporte ocorridos na idade moderna como fundamentais para o diálogo além das fronteiras espaciais entre Estados, e aponta que "essa literatura anterior, postulava que a convergência ocorria por meio da homogeneização das sociedades via industrialização e modernização" (DREZNER, 2001, p. 56)[104].

O tráfego entre fronteiras por meio da troca de ideias está presente na humanidade há séculos. Os avanços tecnológicos potencializaram os meios de comunicação e trouxeram consigo a intensificação da globalização cultural e econômica até o nível acentuado no qual se encontra atualmente. No início do seu trabalho, Drezner (2021) conceitua a convergência e também apresenta duas hipóteses das consequências que a sua ocorrência, com a potencialização da globalização atual, traz consigo. Explica ele:

> A convergência é a tendência das políticas de se tornarem mais parecidas, na forma de uma crescente similaridade em estruturas, processos e desempenhos. Alguns afirmam que a redução das barreiras transnacionais ao intercâmbio econômico força os Estados a revogar contratos sociais de longa data que protegem seus cidadãos da crueldade do livre mercado. A globalização leva a uma corrida para baixo, onde as preocupações com o meio ambiente, o tratamento do trabalho e a saúde dos consumidores são sacrificadas no altar do comércio. Outros argumentam que o crescimento das estruturas de governança transnacionais leva a uma convergência negociada de ampla regulamentação, mas também a uma demanda potencial (DREZNER, 2001, p. 53)[105].

---

[104] Tradução livre do original: "Previous literature postulated that convergence occurred through the homogenization of societies via industrialization and modernization".

[105] Tradução livre do original: "Convergence is the tendency of policies to become more alike, in the form of a growing similarity in structures, processes and performances. Some argue that the reduction of transnational barriers to economic exchange forces states to revoke long-standing social contracts that protect their citizens from the cruelty of the free market. Globalization leads to a race to the bottom, where concerns for the environment, labor treatment and consumer health are sacrificed on the altar of trade. Others argue that the growth of transnational governance structures leads to a negotiated convergence of broad regulation, but also to a potential demand".

A supracitada definição de convergência pressupõe o 'afunilamento' das diretrizes legais internas de Estados diversos para uma similaridade que pode ser entendida como a adequação de normas em trezentos e sessenta graus, que resulta numa homogeneidade normativa no âmbito internacional, haja vista que as semelhanças não se encontram em um só aspecto, mas em diversos: na maneira como as diretrizes jurídicas sobre determinado assunto são desenvolvidas; organizadas e aplicadas pelos ordenamentos internos e também no espaço transnacional.

As hipóteses das consequências oriundas do fenômeno de convergência trazidas por Drezner (2001) podem ser resumidas da menos para a mais negativa. A consequência menos danosa é o resultado do crescimento das estruturas transnacionais de governança, as quais trariam uma regulação mais ampla e unificada, mas que resulta num *déficit* democrático devido à maior unilateralidade dos órgãos internacionais.

Já o resultado extremamente gravoso repousa sobre uma visão negativa da globalização, cuja traz consigo uma convergência de políticas e o aumento das ferramentas transnacionais, e também um intercâmbio econômico elusivamente regulado, resultando em Estados coagidos a "[...] revogar contratos sociais de longa data que protegem seus cidadãos da suposta crueldade do livre mercado" (DREZNER, *idem,* p. 54)[106]. Neste cenário, as preocupações com o meio ambiente, com a garantia dos direitos dos trabalhadores, com a saúde dos consumidores são sacrificadas em prol da otimização dos lucros econômicos.

Há distintas abordagens das teorias que constroem o conceito de convergência. Elas se articulam em torno de duas dimensões de teorias que associam a globalização com a convergência normativa. Na primeira, leva-se em consideração a primazia das forças estruturais (força Estatal) ou o poder de agentes autônomos (agentes internacionais de direito privado), como explica abaixo:

> As teorias baseadas nas forças estruturais lidam com a convergência como a variável dependente e implicam que diferentes políticas nacionais são homogeneizadas em uma política global. As teorias baseadas em agentes autônomos preferem o termo coordenação, que é mais amplo do que convergência. A coordenação de políticas implica algum acordo sobre os limites aceitáveis de políticas regulatórias, mas não significa que todos os estados implementem regras ou regulamentos idênticos (DREZNER, 2001, p. 17)[107].

---

[106] Tradução livre do original: "[...] revoke long-standing social contracts that protect their citizens from the supposed cruelty of the free market".

[107] Tradução livre do original: "Structure-based theo- ries deal with convergence as the dependent variable and imply that different national policies are homogenized into one global policy. Agent-based theories prefer the term coordination, which is more expensive than convergence. Pol- icy coordination implies some agreement on the acceptable bounds of regula- tory policies, but it does not mean that all states implement identical rules or regulations".

A segunda dimensão que aglutina correntes relativas à convergência normativa diz respeito à fonte da pressão necessária para que esta ocorra. Nas linhas argumentativas existentes, há aquela que considera a pressão econômica como principal fator producente da convergência normativa. Nela, "a pressão para modificar as políticas regulatórias vem da ameaça de saída do capital móvel, fazendo com que os estados não convergentes percam sua competitividade na economia global" (DREZNER, *idem*)[108].

Outra significativa corrente analítica da convergência aponta como fator causal preponderante para a produção da convergência a pressão ideológica. Sobre essa corrente, Drezner (2001) afirma "os Estados alteram instituições e regulamentos porque um conjunto de crenças desenvolveu poder normativo suficiente para que os líderes temam parecer retardatários se não adotarem políticas semelhantes" (*Loco citato)*[109].

Ainda se destaca na teorização sobre a convergência normativa a análise denominada de *race-to-the-bottom* (RTB). Segundo ela, a pressão necessária para criar a convergência estaria na mobilidade dos fluxos de comércio e capital ao nível globalizado. Na teoria RTB, esse fluxo é superior à capacidade estatal de impedi-lo através das legislações criadas internamente, os agentes do mercado movendo-se sempre em busca do lugar com mais potencial de retorno para eles. Comenta sobre essa corrente:

> Altas taxas de tributação das empresas, leis trabalhistas estritas ou proteção ambiental rigorosa reduzem as taxas de lucro ao aumentar os custos de produção. O capital, portanto, se envolverá em arbitragem regulatória, movendo-se para (ou importando de) países com os padrões regulatórios mais baixos. Estados. temendo uma perda de sua base tributária, não têm escolha a não ser reduzir os padrões regulatórios para evitar a fuga de capitais (DREZNER, *idem,* p. 59)[110].

Os impactos jurídicos da convergência normativa também são pessimistas quando colocados sobre a perspectiva da teoria RTB, que avalia aquela como a produção de uma maior exposição estatal diante de um mercado que deságua na redução de barreiras, tendo como resultado a troca do controle normativo pelo do exercido pelo capital. Os apontamentos feitos por Karl Polanyi concluem como principal consequência uma "forte correlação

---

[108] Tradução livre do original: "The pressure to modify regulatory policies comes from the threat of mobile capital to exit, causing non converging states to lose their competitiveness in the global economy".

[109] "states change institutions and regulations because a set of beliefs has developed enough normative power that leaders fear appearing to be laggards if they do not adopt similar policies".

[110] Tradução livre do original: "High rates of corporate taxation. strict labor laws, or rigorous environmental protection lower profit rates by raising the costs of production. Capital will therefore engage in regulatory arbitrage, moving to (or importing from) countries with the lowest regulatory stan- dards. States. fearing a loss of their tax base, have no choice but to lower regulatory standards to avoid capital flight".

negativa entre o fluxo de capital que entra num país e seus padrões baixos de regulação de mercado"(POLANYI *apud* DREZNER, 2001, p. 59)[111].

Ainda outra corrente teórica que explica a convergência de diretrizes é o modelo da sociedade mundial. Esta seria pautada em uma cultura resultante da globalização, emergindo de maneira orgânica e gradual, diferente das abruptas consequências advindas do imperativo mercado global descrito na teoria RTB (DREZNER, *idem*).

Na sociedade mundial, os Estados, entendidos como retardatários do ponto de vista regulatório, emulam as práticas dos chamados líderes globais, por serem países-membros subalternos na OCDE. O resultado é um processo de convergência de diretrizes e regulamentos mais sutil e gradual. Sobre essa corrente, destaca como efeito não planejado uma tendência à hipertrofia das burocracias nacionais, os seguintes termos:

> A resposta aqui parece ser a favor de mais regulamentação. Isso permite a "estruturação expansiva" do Estado e o desenvolvimento de novas burocracias para regular tanto a sociedade quanto a economia. O processo de estruturação tem um mecanismo de feedback implícito; à medida que o estado se expande, aumenta o número de interações interestaduais transnacionais, levando a uma maior demanda de integração da sociedade mundial (DREZNER, *idem*, p. 61)[112].

Definir a convergência através das lentes da teoria da sociedade mundial torna difícil a divisão dos processos que levam à convergência em etapas claras a serem estudadas.

Em sua contribuição própria, Drezner (2001) apresenta o que para ele são os três principais caminhos que podem levar à convergência normativa. O primeiro, através do incremento da produção acadêmica ao nível global sobre o tema, que levaria à consolidação de "metanormas enunciadas discursivamente e hegemonizadas globalmente, o que tornaria muito mais fácil o desenvolvimento e o surgimento de modelos regulatórios comuns". (DREZNER, 2001, p. 63)[113].

O segundo caminho na direção da convergência se constituiria pela ação de organizações governamentais internacionais (IGOs). Estas assumiram um papel na implementação de novos modelos de políticas, principalmente nos países menos desenvolvidos, de modo a mobilizá-los para adaptar suas estruturas de governança às injunções por elas exercidas.

---

[111] Tradução livre do original: "strong negative correlation between the flow of capital entering a country and its low standards of regulation".

[112] Tradução livre do original: "The answer here appears to be in favor of more regulation. This permits the "expansive structuration" of the state and the development of new bureaucracies to regulate both society and economy. The structuration process has an implied feedback mechanism; as the state expands, the number of transnational interstate interactions increases, leading to a greater demand for world society integration"

[113] Tradução livre do original: "metanorms that govern discourse, which makes the development and emergence of common models much easier".

Drezner ainda afirma que “as IGOs criam a imagem de todos os Estados como unidades homogêneas, acelerando a disseminação de práticas comuns entre eles" (DREZNER, 2001, *idem*)[114]. Desta forma, mesmo que tal igualdade não corrobora com a realidade fática, a homogeneidade entre os membros, criada através das IGO’s seria favorável à construção de convergência jurídica entre eles.

O terceiro caminho para a convergência jurídica global seria o movimento através do qual as legislações internas dos países atuem no sentido de copiar as formas e políticas de Estados-nação julgados internacionalmente como bem-sucedidos. Ou seja, os países com menos força em organizações internacionais de direito privado, e até mesmo considerados menos avançados em termos legislativos e econômicos podem aderir, de maneira espelhada, a normas de determinadas regiões ou países considerados mais relevantes. Sobre isto:

> No contexto atual, isso implica a adaptação por parte de outros países às políticas instituídas nos Estados Unidos. Implica também que os estados da periferia (ou seja, países não pertencentes à OCDE) estarão igualmente dispostos, se não mais, a adotar políticas convergentes. Outros estados centrais também podem convergir para uma determinada política, mas como esses estados têm um melhor histórico de sucesso, é provável que resistam a políticas que violem as normas domésticas (DREZNER, 2001, p. 64)[115].

No trecho acima, o autor cita a legislação estadunidense como exemplo de padrão normativo desejável por aqueles países denominados de periféricos (não pertencentes à OCDE). Porém, principalmente na privacidade informacional, a União Europeia mostrou imperatividade e relevância jurídica capazes de gerar padrões legislativos para diversas outras organizações internacionais e legislações internas dos países, em distintas regiões do mundo (seção 2).

Um exemplo disto é o caso brasileiro, que se espelhou nos padrões normativos de proteção de dados da União Europeia para continuar relevante no contexto comercial internacional e principalmente para estar conforme os padrões mínimos de elegibilidade exigidos pela OCDE para pleitear uma vaga na organização.

Diferente da perspectiva de Drezner (2001) até aqui descrita, o trabalho de Bennett (1991) desenvolve a produção da convergência de diretrizes partindo do referencial da perspectiva temporal e não da comparação normativa de um país com outro. Junto a isso, o

---

[114] Tradução livre do original: “IGO’s creates the image of all states as homogeneous units, accelerating the spread of common practices among them”.

[115] Tradução livre do original: “In the current context, this implies adaptation by other countries to the policies instituted in the United States. It also implies that peripheral states (ie non-OECD countries) will be equally, if not more, willing to adopt convergent policies. Other core states may also converge on a given policy, but as these states have a better track record of success, they are likely to resist policies that violate domestic norms”.

autor segue a linha de que a globalização é inevitável e favorável para a convergência de diretrizes.

Bennett (1991), após conceituar a convergência nos anos 90, direcionou seu olhar à proteção de dados pessoais como estudo de caso prático da mesma. Ele também aponta no seu trabalho que as diversas teorias de convergência existentes acabam por reproduzir formulações imprecisas sobre o que está convergindo nas legislações e, consequentemente, negligenciam os processos distintos que deságuam na convergência. Vejamos como ele comenta sobre esse ponto:

> O "problema de política comum" desempenha o papel de variável independente. A análise de políticas que depende muito dessa lógica pode facilmente cair em uma apologia do determinismo econômico ou tecnológico, pode levar a uma rejeição prematura de explicações não menos importantes para a convergência e pode obscurecer algumas divergências críticas (BENNETT, 1991, p.218)[116].

Bennett (1991) aponta como a natureza dos dados pessoais digitais é favorável para convergência normativa ao nível internacional, devido à fácil circulação entre fronteiras e da demanda de resolução dos problemas relacionados à jurisdição a que dá causa. Porém, mesmo que o autor afirme existir o papel da tecnologia como fundamental a hipótese de convergência na matéria de privacidade informacional, reforça que o fato das políticas convergirem em Estados distintos, é fruto de um processo peculiar e além do mero determinismo mercadológico e tecnológico.

Logo, para a convergência ser percebida conforme a análise de Bennett (1991), ele julga indispensável a realização do recorte de períodos diversos com o recorte regional das legislações. Assim, é possível atestar a convergência analisando se houve em espaços jurídicos distintos, ao longo do mesmo período temporal, a percepção de uma tendência normativa convergente.

A convergência emerge no cenário avançado de industrialização, no qual existe a "[...] tendência das sociedades se desenvolverem de um jeito parecido, com estruturas, processos e performances similares" (BENNETT, 1991, p. 215)[117]. Este contexto resulta no surgimento de problemas semelhantes em distintas localidades e consequentemente, deságuam em soluções iguais.

Bennett (1991) visa distinguir a convergência de políticas dos estudos descritos por ele

---

[116] Tradução livre do original: "The "common policy problem" plays the role of an independent variable. Policy analysis that relies heavily on this logic can easily fall into an apology for economic or technological determinism, can lead to a premature rejection of no less important explanations for convergence, and can obscure some critical divergences".

[117] Tradução livre do original: "tendency of societies to develop in a similar way, with similar structures, processes and performances".

como meramente comparativos, feitos a partir de um recorte de localidade somado à análise do período temporal específico das legislações internas confrontadas. Sua perspectiva considera não só o contraste entre as legislações estudadas, mas também o padrão desenvolvido ao longo do tempo sobre determinado tema. O autor tem como ponto de referência comparativo não países distintos na mesma época, mas uma condição de divergência ou variabilidade de algum estágio anterior:

> A convergência significa sair de pontos de partida distintos para um único lugar comum. Saber que os países são diferentes não nos conta nada sobre a convergência. Tem que haver movimentos ao decorrer do tempo, semelhantes, que identifiquem um traço comum (BENNETT, 1991, p. 219)[118].

Ao constatar as convergências de temas específicos em legislações distintas, Bennett observa tendências legislativas que, por meio de métodos e agentes diferentes, tendem a convergir no âmago da norma. Sendo assim, o autor não rejeita as peculiaridades e divergências inerentes às regiões, países e organizações ao legislarem, mas constata que há um ponto de chegada em comum almejado. O que gera a convergência, na grande maioria dos casos, no viés principiológico que constitui as legislações.

De acordo com Bennett (1991), a convergência de diretrizes (*policy convergence*) ocorre em camadas distintas, indo do interesse dos países de resolver problemas em comum até a semelhança no processo de formatação das normas sobre determinado tema.

Dentre as camadas nas quais ocorrem a convergência são descritas por Bennett: (i) a *policy content*, que se caracteriza pela similaridade no âmbito formal de diretrizes governamentais, como estatutos, normas administrativas e resoluções; (ii) a *policy tools,* a camada que diz respeito à afinidade entre as ferramentas disponíveis para administrar as diretrizes (os mecanismos regulatórios, o sistema administrativo ou judicial) em legislações diferentes; (iii) a *policy outcomes,* situação na qual a convergência é observada na similaridade das consequências de implementação regulatória sobre o tema; e, por fim, a camada (iv) de convergência no *policy style,* que apresenta semelhanças nos resultados advindos do processo de formação de diretrizes jurídicas.

No que diz respeito aos processos que podem levar à convergência, Bennett (1991) relata a existência de quatro deles: a) a emulação; b) as redes e comunidades políticas; c) a harmonização; e, d) a penetração.

Passamos agora a expor um pouco mais de cada um dos processos.

---

[118] Tradução livre do original: “Convergence means moving from different starting points to a single common place. Knowing that countries are different tells us nothing about convergence. There must be similar movements over time that identify a common trait”.

a) Convergência por Emulação

Este tipo de convergência explica a semelhança entre objetivos de políticas públicas, de conteúdo de normas e instrumentos jurídicos, que não necessariamente precisam versar sobre a mesma matéria, contudo podem trazer pontos positivos de uma norma de determinado país para a construção de diretrizes administrativas em outro. Bennett (1991) aponta como este processo pode ser benéfico para formulação de normas sobre temas inseguros e hesitantes, como, por exemplo, o direito digital e a proteção de dados.

b) Convergência por meio de Redes e Comunidades Políticas

Resulta da existência de ideias compartilhadas entre uma rede duradoura de elites engajadas e com interação regular no nível transnacional. A convergência não é o resultado de constrangimentos impostos pelo problema, ou de insegurança coletiva, mas sim de uma elite identificável ligada pelo conhecimento e experiência de um problema político comum e uma preocupação partilhada pela sua resolução, como aponta Bennett (1991).

Diferente da emulação, há o envolvimento numa experiência de aprendizado sobre o problema. Este processo se relaciona diretamente com a matéria de proteção de dados, pois as discussões sobre o tema surgem na comunidade acadêmica e se estendem ao processo legislativo, resultando nas políticas e diretrizes existentes hoje no ordenamento brasileiro relativas à proteção de dados.

c) Convergência por Harmonização

Ao descrever este tipo de convergência Bennett (1991) aponta o papel impulsionador da interdependência para garantir a implementação completa e bem-sucedida de diretrizes e evitar inconsistências. O cenário é a transnacionalização[119] de problemas políticos como, por exemplo, a poluição ambiental, o aquecimento global e as questões pertinentes ao compartilhamento de informações. Os problemas resultantes da forte globalização, geram a necessidade de países diversos pensarem em soluções de maneira conjunta. A harmonização com as políticas internas necessita não só de atores de Direito Internacional, necessita de motivação e oportunidades regulares de interação entre Estados. Também é indispensável a

[119] "A transnacionalização não é um fenômeno distinto da globalização. Em uma perspectiva etimológica, o termo transnacional é oriundo do prefixo trans que, no latim, significa "além de". Destarte, o termo "transnacional" diz respeito àquilo que vai além da nação. Referido fenômeno tem como característica a permeabilidade. A globalização, por sua vez, possui uma perspectiva de envolvimento, de conjunto, enquanto a transnacionalidade é um novo espaço, que não se confunde com espaço internacional ou nacional(STELZER, 2011)".Disponível em: <http://revista.fumec.br/index.php/meritum/article/view/5249>.

ação imperativa por parte de organizações internacionais responsáveis.

d) Convergência por Penetração

Faz contraste com as relações aparentemente cooperativas da convergência por harmonização, pois, quando ocorre, faz com que determinados ordenamentos internos se vejam forçados a entrar em sintonia com ações normativas adotadas por outros Estados, geralmente guiadas por agentes privados, como as organizações internacionais de Direito Privado e empresas transnacionais (ETN): "[...] a maioria das evidências de convergência através da penetração reside no papel das empresas transnacionais em garantir com sucesso uma estrutura regulatória comum para seus produtos" (BENNETT, 1991, p. 225)[120].

Em *The Governance of Privacy* (2003)*,* Bennett e Raab analisam os fenômenos de convergência no campo de regulação da privacidade e de divergência na escolha de mecanismos utilizados em diferentes experiências normativas (Suécia, Estados Unidos, Alemanha e Inglaterra). Das perspectivas abordadas que causam a convergência, eles pontuam a existência do chamado determinismo tecnológico até a convergência por penetração acima descrita de regimes específicos em diferentes Estados. Nessa obra é possível observar uma percepção da convergência normativa em termos de um modelo de desenvolvimento ao longo do tempo, privilegiando seu caráter processual menos do que seu caráter de condição.

Ao mostrar existirem diversas camadas de convergência possíveis nas quais podem até ocorrer divergências normativas em algum ponto, Bennett não deixa de reconhecer o papel da União Europeia como coercitivo e essencial na convergência jurídica da proteção de dados. Bennett (2020, p.19) descreve a relevância da UE no impulso para surgirem outros marcos regulatórios nacionais referidos à privacidade informacional em vários países:

> [...] esse assunto tornou-se objeto de legislações nacionais, inicialmente, em lugares como a Alemanha, Suécia e França, criando externalidades ao longo da União Europeia e em outras partes do mundo, porque eles não podiam regular os dados que fluíam para além das fronteiras, produzindo instrumentos de harmonização internacional como a OCDE, o Conselho da Europa e, finalmente, a União Europeia, pela qual eles tinham um impacto coercitivo maior em outros países (DATA PRIVACY, 2020, p, 19)[121].

---

[120] Tradução livre do original: "Most evidence of convergence through penetration resides in the role of transnational companies in successfully ensuring a common regulatory framework for their products".

[121] Tradução livre do original: "[...] this subject became the subject of national legislation, initially, in places like Germany, Sweden and France, creating externalities throughout the European Union and in other parts of the world, because they could not regulate the data that flowed beyond borders, producing instruments of international harmonization such as the OECD, the Council of Europe and, finally, the European Union, through which they had a greater coercive impact on other countries".

Mendes (2014) recorre à denominação de convergência feita por Bennett para traduzir o movimento ocorrido nos ordenamentos internos em países e regiões distintas. Tal movimento consiste na evolução de legislações num mesmo estilo sobre o assunto ao decorrer do tempo, descrito por Bennett (1991) como Tese de Convergência. Nela, identifica-se um padrão na evolução normativa da proteção de dados em localidades diversas, numa mesma época:

> A convergência significa mais que similaridade. Denota um padrão que ultrapassa o tempo, um processo dinâmico, ao invés de uma condição estática. (…) Deste modo, a partir de uma posição em que os Estados não tinham nenhuma ou muito pouca legislação de proteção de dados e, por isso, havia diversos tipos de estratégia para o tema, um consenso emergiu durante a década de 1970, em volta de princípios. Podemos concluir portanto, que a convergência ocorreu (BENNETT, 2011 *apud* MENDES, 2014, posição 765).

A convergência também é observada no padrão seguido por diversos ordenamentos jurídicos internos/nacionais, caracterizados pela adição da proteção de dados pessoais a textos constitucionais com o arcabouço de direito fundamental, somado à lei ordinária de disposições gerais sobre o tema. O resultado é uma regulamentação da proteção de dados generalizada, com impactos na economia e nas relações sociais (através da cultura de boas práticas) conjuntamente com os órgãos da administração pública (MENDES, 2014).

Com abrangência e âmbito de aplicações variadas, a convergência dos ordenamentos jurídicos internos se expressa nas semelhanças observadas pelos países ao legislar e implementar diretrizes sobre a matéria de proteção de dados. Porém, como dito acima, o fenômeno ultrapassa a mera similaridade. Explica Bennett que a convergência é:

> […] um processo dinâmico moldado por diferentes forças, como o determinismo tecnológico, a imitação voluntária dos "pioneiros", a construção de redes entre elites (*elite networking*), a harmonização por meio de organizações internacionais (OCDE) e as pressões internacionais para que ideias jurídicas penetrem em diferentes jurisdições, como foi o caso da Convenção 108 de 1981 (DATA PRIVACY BRASIL, 2019, p. 9)[122].

É exemplo o caso brasileiro, no qual houve, na elaboração da norma geral de proteção de dados o espelhamento dos dispositivos do texto do Regulamento Geral de Proteção de Dados Pessoais, da União Europeia. Também é fruto do processo da convergência, o Brasil se vê coagido a adequar-se aos padrões legais de privacidade impostos pela União Político-Comercial (UE) para que pudesse continuar dialogando com o comércio internacional e também, para que pudesse ser elegível a uma vaga na OCDE.

Os Estudos de Bennett reforçam a existência da convergência de diretrizes como

[122] Tradução livre do original: "a dynamic process shaped by different forces, such as technological determinism, the voluntary imitation of the "pioneers", the construction of networks between elites (elite networking), harmonization through international organizations (OECD) and pressures international institutions for legal ideas to penetrate different jurisdictions, as was the case with Convention 108 of 1981".

viável por diversos fatores. Dentre eles, o autor destaca a existência do determinismo tecnológico, que traz consigo o inevitável interesse da aproximação jurídico internacional às normas internas dos países, devido às tecnologias digitais em rede que pressupõem a insignificância de fronteiras, inclusive normativas.

A harmonização internacional de normas é objeto de estudo do direito internacional desde os primórdios da matéria. Sua análise na literatura existente reafirma as dificuldades presentes na sua aplicação plena. Mesmo diante de uma realidade globalizada, na qual o diálogo entre fronteiras se tornou presente, questões referentes à esfera jurídica de diversas especialidades possuem nuances complexas quando adentrado o assunto de harmonização de normas.

A nova conjuntura em que emergem os dilemas da privacidade informacional de dados trouxe demandas jurídicas inéditas até o momento, que geraram novas possibilidades legislativas. Isto se dá devido ao objeto desta matéria, os dados digitais, que trazem consigo fluidez e intangibilidade e geram a necessidade de que as normas, assim como eles, também sejam transfronteiriças.

4.2 Da criação da LGPD à adequação da *Amazon Web Services (AWS)*

Entendido o conceito de convergência elaborado por Bennett (1991) e também a sua equiparação com a harmonização jurídica, é possível perceber a incidência da mesma na proteção de dados. Ao recapitular a maneira como o Brasil chegou ao texto da vigente da LGPD (Lei n. 13.709/2018), é possível analisar o processo de convergência ocorrido na matéria de privacidade informacional.

É interessante atentar para os impactos que uma ETN como a *Amazon* causa e também sofre neste processo. É entendido que o papel das *Big Tech's* — que também se encaixam na definição de ETN's — dão causa à necessidade de legislar sobre as demandas relativas aos usos de novas tecnologias que se popularizam, ao mesmo tempo que, precisam se adequar e estar em consonância com a atual política de proteção de dados pessoais, no caso do oferecimento dos serviços em nuvem, como requisito da sua presença nos países. Sobre esse ponto explica:

> Ao mesmo tempo em que a globalização proporcionou um acesso quase que ilimitado a diferentes mercados consumidores, ela também impôs às grandes empresas a necessidade de adaptar seus produtos às demandas desses mercados. Esse processo gerou um aumento na concorrência entre as empresas, desafiando-as a

> estar continuamente se renovando e produzindo da maneira mais eficiente possível (lPEREZ,2016, p. 18).

A autora explica que o acesso a ilimitados mercados consumidores, geraram para as empresas a necessidade de adaptar seus produtos às demandas desses mercados. Como efeito disto, é relatada a necessidade de constante adaptabilidade dos seus produtos para melhorar seu desempenho concorrencial.

A partir do raciocínio acima, é possível, utilizando de analogia, relacionar a adequação à proteção de dados a uma demanda concorrencial. Junto à adaptação tecnológica constante — característica das *Big Tech's* como a *Amazon* — há também uma corrida para a adaptabilidade às tendências normativas que regulamentam atividades que as utilizam, tornando-se necessário o movimento de convergência jurídica, de modo a regulamentar de modo eficiente a presença dos serviços e produtos tecnológicos nas diversas regiões do mundo.

É conveniente, para desenvolver a presente seção, definir, respectivamente, os conceitos de empresas transnacionais (ETN) e também de *Big Tech's.* Carvalho Filho (2011) destaca como uma das definições mais aceitas de ETN a dada pela conferência das Nações Unidas de Comércio e Desenvolvimento, que as caracteriza como:

> Uma empresa que compreende as entidades em mais de um país que operam sob um sistema de tomada de decisão que permite políticas coerentes e de uma estratégia comum. As entidades são tão ligadas, por posse ou não, que uma ou mais delas podem ser capazes de exercer uma influência significativa sobre os outros e, em particular, partilhar conhecimentos, recursos e responsabilidades com os outros. (UNCTAD, 2010 *apud* CARVALHO, 2011, p. 91).

Luiz Olavo de Baptista, ao conceituar empresa transnacional, afirma que ela "se aproxima do conceito jurídico de grupo de sociedades, mas com acréscimo de que é um grupo constituído por sociedade sediadas em países diferentes, constituintes sob leis diversas, cada qual com certa autonomia, agindo por sua conta, mas em benefício conjunto" (BAPTISTA, 1987, p.17). Esse autor utiliza de analogia para definir a regulação das transnacionais como 'quimérica', e o faz para traduzir a contra-intuitividade da tutela das mesmas nas relações internacionais[123].

Já as *Big Tech's* podem ser entendidas como "as grandes empresas associadas a plataformas de uso intensivo de dados, quase todas situadas na América do Norte, e também

[123] Símbolo de calendário do ano tripartite, adotado pelos gregos, a Quimera tinha cabeça de leão, corpo de cabra e posterior de serpente, o que a fez tornar-se sinônimo de impossibilidade lógica, de utopia. Assim também é a regulamentação da empresa transnacional no quadro das Relações Internacionais, tais como as vemos hoje (BAPTISTA, 1987, p. 16).

cada vez mais na China" (MOROZOV, p.149). Ou seja, nelas, a maior captação de receita vem das ferramentas que implicam coleta e processamento de dados.

Ao desenvolver seu trabalho intitulado *The Big Nine*, Amy Webb (2019) lista as principais *Big Tech's* da atualidade: "são as nove gigantes da tecnologia Google, Amazon, Apple, IBM, Microsoft e Facebook nos Estados Unidos e Baidu, Alibaba e Tencent na China" (WEBB, 2019, p. 12)[124]. É possível notar que a presença das nove transnacionais da tecnologia atualmente se divide entre as potências econômicas em disputa pelo 'título' de maiores economias do mundo: Estados Unidos e China.

Por se encaixarem na definição de ETN, as denominadas *Big Tech's* podem ser entendidas como empresas transnacionais especializadas em tecnologia, por possuírem receita principal baseada nos produtos e serviços digitais. Além disto, por buscarem estar sempre à frente umas das outras em inovação, elas também são as precursoras de tendências tecnológicas globais.

A partir dos conceitos acima descritos, a *Amazon pode* ser entendida como uma *Big Tech* transnacional, já que possui histórico marcante na seara de inovações de paradigmas de mercado a partir de novas tecnologias e também é um exemplo de aderência à adequação à proteção de dados pessoais.

O início das suas atividades foi no ano 1994, com o intuito inicial de vender livros via *internet*. A *Amazon Books* foi resultado da ideia do seu fundador, Jeffrey Bezos, um dos pioneiros em vendas ao consumidor via *e-commerce.* Ele foi visionário ao acreditar que a popularização dos computadores resultaria numa nova plataforma de comércio. Cano *et al.* (2002) apontam que a estratégia do CEO popularmente chamado de Jeff Bezos foi elaborada de maneira minuciosa para desbravar os negócios na modalidade *online*. Descreve o autor que:

> Inicialmente ele fez uma lista dos 20 produtos mais apropriados para serem vendidos na Internet, desde roupas até ferramentas de jardinagem, chegando a uma lista dos "cinco mais": CDs, vídeos, hardware, software e livros. Uma gama de critérios foi utilizada para chegar a este resultado, entre eles o tamanho do mercado de cada produto: o de livros movimentava US$ 82 bilhões no mundo todo (Success, julho de 1998), bem como o preço. Jeff queria vender um produto barato. Outro fator preponderante foi o poder de escolha que os clientes teriam, graças à grande variedade de títulos. (CANO *et al.,* 2002, p. 11).

Foi em julho de 1995 que a *Amazon Books* deu início às suas atividades no 'espaço' virtual. Cano *et al.* (2002) destacam que uma livraria entendida até então como tradicional

[124] Tradução livre do original: "The nine technology giants are Google, Amazon, Apple, IBM, Microsoft and Facebook in the United States and Baidu, Alibaba and Tencent in China".

não chegava a oferecer mais de cem mil títulos ao cliente, enquanto a *Amazon* oferecia "[...]mais de um milhão de títulos em oferta, e somente 500 best-sellers em estoque" (CANO *et al.,* 2002, p.11).

Devido ao fato dos produtos estarem disponíveis no catálogo *online,* com compra realizada também neste meio, a maneira como a venda, logística de entrega e a manutenção do estoque funcionavam, trouxeram à empresa grande destaque no ramo. Parte deste sucesso se deu devido à administração do negócio a partir da demanda registrada através dos dados que a ferramenta de busca do *site* proporciona até hoje para os clientes.

Porém, mesmo tendo se destacado através da virtualização das vendas e como uma das pioneiras do formato *e-commerce,* a constância da *Amazon* como uma Empresa Transnacional e *Big tech* de sucesso se dá por mérito da variedade de serviços que a mesma oferece. A empresa dispõe desde o *e-commerce,* com produtos físicos e virtuais, até serviços de *software.* Tudo isso para ambos os públicos: fornecedores e consumidores finais.

Os seus produtos são divididos no trio das seguintes categorias: o *e-commerce*; conteúdo digital e soluções digitais. Mesmo que a segmentação exista, Cano *et al.* (2002) assinalam que a fronteira entre serviços não existe de maneira muito definida, sendo muitas vezes flexíveis. Os produtos e serviços podem oferecer duas ou três funções ao mesmo tempo.

O autor cita o exemplo da *Amazon Web Services* (AWS), que "fornece análise de dados e assistência digital para negócios, sendo colocada nas áreas sobrepostas de conteúdo digital e solução digital" (CANO *et al.,*2002, p. 16). Sobre o serviço em nuvem da empresa em questão, os autores supracitados destacam que:

> A AWS oferece uma ampla oferta global de computação, armazenamento, banco de dados e outras ofertas de serviços para desenvolvedores e empresas de todos os tamanhos. Como sua receita não foi publicada até 10 anos depois, o público não sabia se a AWS estava lucrando antes disso. Em abril de 2015, quando a Amazon anunciou pela primeira vez que as vendas brutas da AWS totalizaram US$ 4,7 bilhões no ano fiscal anterior, o preço de suas ações disparou e seu valor de mercado ultrapassou rapidamente a Berkshire Hathaway de Warren Buffett e se tornou a quinta maior empresa em valor de mercado (Carter, 2017). Graças à AWS, a receita anual da Amazon em 2015 ultrapassou US$100 bilhões pela primeira vez, duas décadas após o estabelecimento da Amazon (CANO *et al.,* 2002, p.16, *apud* COLES, 2017)[125].

Como vemos acima, Cano *et al.* (2002) destacam como os produtos que utilizam da tecnologia em nuvem são extremamente lucrativos e relevantes para a *Amazon*. É importante

[125] Tradução livre do original: "AWS, has served its own computing needs and those of other companies since 2004 and it has become the largest cloud-computing service provider with a 47% market share (Coles, 2017). The more Amazon invests in AWS, the more appealing it becomes for companies and programmers".

ressaltar a relevância econômica dos serviços que implicam no manuseio dos dados, com o fim de apontar o quanto a garantia da privacidade informacional impactou e foi, de certa forma, moldada pelas relevantes empresas transnacionais como a *Amazon* e outras *Big-Tech's*.

Do ponto de vista da convergência apontada por Bennett (1991), o processo pelo qual o Brasil passou para se adequar aos padrões normativos externos ao país, no que se refere à legislação sobre proteção dados, tanto quanto a necessidade de que a *Amazon* se adequasse às normas de proteção de dados pessoais para atuar em territórios como o da União Europeia e posteriormente o brasileiro, ilustram um tipo de convergência descrita pelo autor como Convergência por Penetração.

Ambas as legislações — a GDPR europeia e a LGPD brasileira — exigem dos agentes com atividade comercial relacionada aos dados pessoais a adequação às legislações específicas sobre o tema. O texto da LGPD e a maneira como seus artigos foram delineados a partir do GDPR europeu, evidenciam traços da convergência por penetração.

Bennett (1991) entende que os chamados regimes internacionais facilitam a cooperação transnacional entre países e dispõem de incentivo para diminuir as diferenças. Porém, o autor acredita que a definição presente na literatura específica em relação a "regime internacional" é restrita à tradição de relações internacionais, que não se compõe do estudo de políticas domésticas, nem do trabalho mais teórico sobre seus processos de formulação.

A análise dos processos de convergência consegue revelar o impacto que as diretrizes transnacionais podem causar em legislações internas. Bennett aponta o estudo de Brickman (1984) sobre a regulação química, no qual foi constatado que:

> Organizações internacionais como a CE (Comunidade Européia) e a OCDE (Organização para Cooperação e Desenvolvimento Econômico) forneceram estruturas institucionais indispensáveis para a construção de uma resposta comum. A adesão à CE não apenas compromete os países europeus a evitar ações regulatórias que distorcem o comércio, mas também fornece vários mecanismos para atrair os estados membros para negociações com o objetivo de desenvolver políticas congruentes (BRICKMAN, 1984, *apud* BENNETT, 1991, 219)[126].

[126] Tradução livre do original: "International organizations such as the EC (European Community) and the OECD (Organization for Economic Cooperation and Development) have provided indispensable institutional structures for building a common response. Adherence to the EC not only commits European countries to avoiding regulatory actions that distort trade, but also provides various mechanisms for attracting member states to negotiations aimed at developing congruent policies".

É possível observar, através do estudo supracitado, que, ao legislar sobre determinado tema, uma organização internacional não só obriga seus membros a se adequarem, mas também amplia os mecanismos que levam seus integrantes a diretrizes jurídicas congruentes. A depender da imperatividade da organização que realiza a regulamentação, pode haver uma tendência harmonizadora também para Estados além dos signatários.

É um exemplo disto a União Europeia e a OCDE. Ao exigirem adequação sobre uma matéria, elas geram uma cadeia de consequências adequadas para os seus países-membros e também para terceiros. Isto se dá devido à força normativa e comercial que essas organizações exercem em âmbito comercial internacional.

O Brasil, ao decidir entrar em sintonia com as diretrizes de privacidade informacional, almejava continuar presente e relevante no comércio internacional e também estar em paridade com os padrões de privacidade de dados da OCDE, redigindo o texto da sua norma Geral de Proteção de Dados a partir do GDPR europeu.

O processo de aproximação harmonizadora, através das lentes da tese de convergência diferente da definição quase utópica da harmonização jurídica internacional integral e progressiva, avoca o reconhecimento de que tal decurso tem sido "progressivo, irregular e desigual" (BENNETT,1991, p. 92)[127].

A natureza *sui generis* da proteção de dados fez com que o tema fosse regulamentado de maneira semelhante em ordenamentos internos distintos. Esse fenômeno se deu pelas necessidades de circulação de produtos que possibilitam a monetização dos dados pessoais[128] , relacionados à demanda de privacidade informacional, que tem como característica a fluidez entre as fronteiras físicas dos países, por estarem, em sua grande maioria, disponibilizados para consumo nas redes virtuais.

São exemplos os serviços de *software* da computação em nuvem, que possuem bancos de dados em lugar físico diverso do qual a operação está sendo oferecida ao cliente final. Sendo assim, cria-se um fluxo de dados que perpassa fronteiras e jurisdições diversas.

---

[127] Tradução livre do original: "International organizations such as the EC (European Community) and the OECD (Organisation for Economic Co-operation and Development) provided indispensable institutional frameworks for building a common response. EC membership not only commits European countries to avoiding trade-distorting regulatory actions, but also provides various mechanisms to draw member states into negotiations with the aim of developing congruent policies".

[128] "Existem duas abordagens para a monetização de dados, uma interna e uma externa, sendo interna aquela que visa a transformar os dados em inteligência capaz de alavancar resultados, e a externa aquela que transforma os dados pessoais em um produto com relevância e valor de mercado, de modo a se apresentar como uma nova fonte de receita para o negócio" (MODESTO, 2020, p. 6).

A *Amazon Web Services* (AWS) conta com uma infraestrutura global. Ela pode ser definida como o oferecimento da computação em nuvem num modelo de regiões e zonas de disponibilidade de serviços, nelas existem servidores físicos em pontos alocados nessas regiões para atender, de maneira otimizada e em rede, as demandas dos clientes. No seu *site*, as regiões que abrigam a infraestrutura global da nuvem AWS são descritas como:

> A AWS tem o conceito de uma região, que é um local físico em todo o mundo onde agrupamos datacenters. Chamamos cada grupo de datacenters lógicos de zona de disponibilidade. Cada região da AWS consiste no mínimo em três AZs isoladas e separadas fisicamente em uma área geográfica. [...] Cada AZ tem energia, refrigeração e segurança física independentes e está conectada por meio de redes redundantes de latência ultrabaixa. Os clientes da AWS, focados em alta disponibilidade, podem projetar seus aplicativos para serem executados em várias AZs, a fim de obter tolerância a falhas ainda maiores. As regiões de infraestrutura da AWS atendem aos mais altos níveis de segurança, conformidade e proteção de dados (AMAZON, 2023)[129].

Conforme os dados disponíveis no site da AWS, existem 99 zonas de disponibilidade em 31 regiões geográficas no mundo e mais de 15 zonas de disponibilidade e outras 5 regiões da AWS no Canadá, Israel, Malásia, Nova Zelândia e Tailândia. É possível visualizar os locais do globo nos quais a AWS está presente:

Figura 1 – Mapa Da Infraestrutura Global Da Aws

(AMAZON, 2023)

[129]Disponível em: <https://aws.amazon.com/pt/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2>.

As AZ's podem ser traduzidas como 'zonas de disponibilidade', as quais abrigam os *Data Centers* diversos, com conectividade e energia naquela região territorial. A *Amazon* descreve que este sistema de organização "proporciona aos clientes a capacidade de operar aplicativos e bancos de dados de produção com alta disponibilidade, tolerância a falhas e escalabilidade em níveis superiores aos que um único *datacenter* pode oferecer" (AMAZON, 2023)[130].

O sistema de regiões de disponibilidade permite solucionar demandas de cunho jurídico nos âmbitos locais, uma vez que o serviço oferecido está alocado em uma região territorial específica, passando os clientes a ficar resguardados pela norma específica do país ao qual são vinculados. Esta formatação dá respaldo às movimentações de capital capazes de coagir legisladores internos a convergir com os padrões legislativos de países mais desenvolvidos, que tutelam o produto ou serviço oferecido *Big Tech's* transnacionais.

No processo de convergência por penetração, Bennett (1991) descreve existir por parte das Empresas Transnacionais o papel de "garantir com sucesso uma estrutura regulatória comum para seus produtos". Neste sentido há, de maneira velada, muitas vezes, uma pressão munida da força de capital por parte dos agentes, que resulta na padronização de normas internas.

As empresas transnacionais que fazem parte do atual grupo chamado de *Big Tech's* ocupam o papel do que Cano *et al.* (2002) denominam de Organização Virtual (OV). Esta é definida como uma matriz organizacional polidimensional na qual as "funções administrativas e de serviços são desempenhadas por humanos e por agentes não humanos, como outras organizações, bancos de dados, sistemas, programas, transdutores, etc., usando recursos informacionais diversos" (CANO *et al.,* 1991, p. 96).

As OVs possuem serviços de *software*, mas transitam entre uma logística virtual e física que atende demandas de consumo de diversas maneiras, utilizando como meio a virtualização. Estas organizações não deixam de se encaixar na denominação de ETN, pois geralmente operam para além das fronteiras internacionais.

Com entrada em vigor da LGPD prevista para agosto de 2020, a *Amazon Web Services (AWS)* publicou no mesmo ano, em sua página oficial um documento com informações sobre os serviços e recursos oferecidos e a necessidade de conformidade com a norma. A partir de uma visão geral da Lei Brasileira e seus impactos, é mencionada como a mesma está alinhada ao *General Data Protection Regulation* da Europa e a importância no papel das organizações:

---

[130] Disponível em: <https://aws.amazon.com/pt/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2>.

> As organizações precisam ter a capacidade de demonstrar continuamente a segurança dos dados que estão processando e a aderência à LGPD, implementando e revisando frequentemente medidas técnicas e organizacionais robustas. Isso exige a definição e a aplicação de políticas compatíveis aplicáveis ao processamento de dados pessoais (AMAZON, 2020, p. 1).

Em seguida, são definidas as funções da *AWS* no processamento dos dados, conforme a LGPD, que pode atuar tanto como um controlador quanto como um processador de dados. Ela assume o papel de controle quando "coleta e armazena informações de seus clientes diretos para registro de contas, administração, acesso a serviços, atributos de serviço ou informações de contato para a conta da AWS" (AMAZON, 2020, p. 2); de processamento de dados, "quando clientes e provedores de soluções da AWS usam os serviços da AWS para processar dados no conteúdo de seus respectivos clientes" (AMAZON, *idem*).

A necessidade de adequação da LGPD em termos dos seus parâmetros para a coleta, uso, processamento e armazenamento de dados, o documento ainda alerta sobre as penalizações dispostas que podem recair sobre usuários dos serviços da *Amazon*. Entre elas estão os "Avisos, suspensão ou bloqueio das atividades de processamento que violem a lei, além de multas de até 2% da receita bruta do infrator no Brasil no ano anterior, com o valor máximo de 50 milhões de reais" (AMAZON, *idem*).

Há uma seção sobre a responsabilidade da segurança de dados, que deverá ser compartilhada pela *AWS* e o cliente usuário da *cloud:*

> Quando o cliente transfere seus dados e sistemas de computação para a nuvem, as responsabilidades de privacidade e segurança são compartilhadas entre o cliente e o provedor de serviços de nuvem. Quando os clientes migram para a Nuvem AWS, a AWS é responsável pela proteção da infraestrutura subjacente que oferece suporte à nuvem, e os clientes são responsáveis por tudo aquilo que colocam na nuvem ou conectam à nuvem. Normalmente essa diferenciação da responsabilidade é mencionada como segurança da nuvem vs. segurança na nuvem (AMAZON, 2020, p.3).

Como o cliente dos serviços de nuvem pode, dependendo da modalidade contratada, não ser o cliente final, a empresa apresenta a modalidade de responsabilidade por incidentes compartilhados, para não se responsabilizar pela má utilização do seu serviço por terceiro. Dentre as nuances técnicas que o documento analisado nesta seção apresenta, faz-se válido destacar a preocupação da Amazon em esclarecer os padrões técnicos mínimos fornecidos pela mesma e exigidos pela LGPD[131].

[131] 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

A partir do entendimento de como a *Amazon* se propõe a garantir a segurança informacional nos serviços de nuvem da *AWS*, é possível fazer um paralelo da sua adequação como empresa transnacional às normas de organizações internacionais e internas sobre o tema. Mas, também observar como a sua atividade, como a de diversas outras empresas transnacionais, contribuíram para a ocorrência do processo de convergência por penetração na construção de legislações como a LGPD brasileira.

Ao definir a convergência por penetração, Bennett (1991) diz que "certos esforços de harmonização podem ter um efeito coercitivo sobre os Estados que demoraram a agir em uma determinada área". Desta forma, o autor argumenta que o movimento comum das empresas transnacionais da telecomunicação, criadas em maioria nos Estados Unidos, era de pressão pela desregulamentação.

Na década de 90, os registros de bancos de dados estavam predominantemente nos Estados Unidos, o que possibilitou a ocorrência de um ataque às legislações protecionistas sobre o tema. Bennett descreve que:

> O negócio multinacional exigiu o direito de passagem livre para tais informações em todo o mundo. Isso significou um ataque às políticas governamentais protecionistas, que tiveram um impacto convergente na Grã-Bretanha, Canadá, Austrália e vários outros países (BENNETT, 1991, p. 228)[132].

Porém, com o aumento do uso das ferramentas *online* como fonte de monetização, juntamente à economia de dados pessoais, o movimento passou do ataque às legislações protecionistas para a exigência de adequação à proteção informacional. Isso ocorreu a partir do momento que as *Big Tech's* perceberam a adequação como inevitável, uma vez que a temática passou a ganhar cada vez mais destaque como um direito fundamental e também concorrencial.

Há por parte das *Big Tech's* transnacionais o poder e a capacidade de determinar os rumos econômicos e políticos através das tecnologias por elas popularizadas. Sobre tais funções, explica:

> A maximização de lucros e o poder que essas grandes firmas passaram a exercer em toda a comunidade internacional tornaram-se pautas de destaque nas agendas de Governos e Organizações Internacionais o que lhes conferem características de sujeitos internacionais (CARVALHO FILHO, 2011, p. 92).

---

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 (BRASIL, 2018).

[132] Tradução livre do original: "The multinational business demanded the right of free passage for such information around the world. This meant an attack on protectionist government policies, which had a convergent impact in Great Britain, Canada, Australia and several other countries".

O papel das transnacionais de tecnologia é peculiar na convergência por penetração porque, ao mesmo tempo que são agentes penetrantes, criaram este tipo de negócio que usa de técnicas como o *Big Data, machine learning,* resultantes no fluxo de dados entre fronteiras e na economia de dados. Por outro lado, elas também precisam se adequar às diretrizes das regiões e dos países.

Sendo assim, o exemplo da incidência da proteção de dados sobre a *Amazon* ilustra a convergência por penetração, na medida que, ao adequar-se às diretrizes de proteção de dados da União Europeia e da OCDE, a empresa reconhece a importância de estar presente no mercado dos países membros de ambas. Por conseguinte, sua adequação passa a exigir de países como o Brasil padrões semelhantes. Explica:

> A crescente complexidade e amplitude dos 'fluxos de dados transfronteiriços' levou o Conselho da Europa e a OCDE a desenvolver acordos internacionais sobre o tratamento e proteção de várias categorias de dados. Os estados que ficaram para trás (por exemplo, a Grã-Bretanha) foram forçados a adequar sua legislação doméstica ou correr o risco de serem excluídos do 'clube' e dos benefícios da harmonização. Outras questões relacionadas ao comércio acarretam penalidades semelhantes para os estados que demoram a agir (BENNETT, 1991, p. 226)[133].

É possível entender os métodos de monetização de dados utilizados pelas empresas transnacionais de tecnologia como causadores da demanda de legislar sobre a proteção da privacidade informacional. A regularização jurídica se dá através dos agentes penetrantes entendidos como as Organizações Internacionais, mas também mediante o papel das empresas transnacionais especializadas em serviços de tecnologia.

As OIs e as *Big Techs* possuem meios de induzir o processo de convergência através da pressão exercida sobre os Estados que ainda não estão adequados. No caso das OIs, há a ameaça velada de serem excluídos do grupo de vantagens aos quais os países congruentes com as diretrizes de privacidade fazem parte.

Já as *Big Techs* necessitam de territórios adequados às diretrizes de proteção de dados para continuar atuando nos países nos quais estão presentes ou querem passar a operar. Isto ocorre pelo fato dos serviços como o de computação em nuvem implicarem manuseamento de dados constante em operações como coleta, armazenamento, tratamento e transferências.

---

[133] Tradução livre do original: “The increasing complexity and scale of 'cross-border data flows' has led the Council of Europe and the OECD to develop international agreements on the processing and protection of various categories of data. States that lagged behind (eg Great Britain) were forced to adjust their domestic legislation or risk being excluded from the 'club' and the benefits of harmonisation. Other trade-related issues carry similar penalties for states that are slow to act”.

4.3 Harmonização na proteção de dados: iniciativas de Organizações Internacionais até a LGPD brasileira

Conceituar o termo harmonização como gênero, compreendendo-o como a minimização de diferenças entre dispositivos normativos internos distintos, é favorável para que se compreenda a tese da convergência pensada por Bennett (1991) como um de seus sinônimos.

À luz da proposta de Bennett é possível descrever as peculiaridades da conformidade da matéria de privacidade de dados no âmbito internacional, sendo possível, através dela, analisar casos particulares e mostrar que a semelhança da normatização da proteção de dados em diversos ordenamentos internos do globo terrestre, ultrapassa a mera similaridade, o que revela a convergência como parte da harmonização jurídica internacional que vem ocorrendo sobre o tema.

A evolução da matéria de proteção de dados pessoais e de seus principais dispositivos jurídicos, aconteceu na maioria do cenário do Direito Internacional. Como visto na análise histórico-evolutiva comentada na seção 1.2., organizações como a OCDE e a União Europeia foram fundamentais para desenvolver a padronização de normas e diretrizes sobre o tema no âmbito jurídico internacional.

Primordialmente, é elementar assentir a multiplicidade de sistemas jurídicos que coexistem na esfera jurídica internacional. De Oliveira (2008) destaca a importância da utilização de ferramentas de comparação para reconhecer as semelhanças, mesmo em meio às diferenças culturais e jurídicas dos países, para permitir a categorização de elementos condizentes entre eles.

O reconhecimento e a persecução de semelhanças entre ordenamentos internos pode ser chamado de movimento de harmonização. Antes mesmo do século XXI ocorreu a tentativa de harmonizar respectivamente a esfera nacional, a regional e a global:

> No âmbito nacional, com o objetivo de minimizar a variedade local, como no caso da Inglaterra, onde ocorreu a unificação pela *common law* na Idade Média. No âmbito regional, com a tendência dos países europeus de alinhar os respectivos ordenamentos jurídicos, sendo lecionado, inclusive, nas universidades o "direito transnacional", de caráter essencialmente acadêmico. No âmbito global, os primeiros esforços visavam a unificação de áreas inteiras do direito (De OLIVEIRA, 2008, p. 29).

Dentro do ambiente acadêmico emerge do desejo da harmonização do Direito transnacional que, de acordo com Koh (2006) é exprimido como:

> Talvez a melhor definição operacional de direito transnacional seja possível usando imagens da era do computador: (1) lei que é "baixada" do âmbito internacional para o direito doméstico: por exemplo, um conceito de Direito internacional que é domesticado ou internalizado na lei municipal, como a norma internacional de direitos humanos contra o desaparecimento, agora reconhecida como lei doméstica na maioria dos sistemas municipais; (2) lei que é "carregada, então baixado": por exemplo, uma regra que se origina em um sistema, como a garantia de um teste gratuito sob o conceito de devido processo legal nos sistemas jurídicos ocidentais, que então se torna parte direito internacional, como na Declaração Universal dos Direitos Humanos e o Pacto Internacional sobre Direitos Civis e Políticos, e a partir daí torna-se internalizado em quase todos os sistemas jurídicos do mundo; e (3) lei que é emprestada ou "transplantada horizontalmente" de um país sistema para outro: por exemplo, a doutrina das "mãos impuras", que migrou da lei britânica de equidade para muitos outros sistemas jurídicos (KOH, 2006, p. 746)[134].

A partir da definição acima, o Direito transnacional pode ser entendido como uma forma híbrida das normas jurídicas internas e externas, devido à força que a segunda acaba exercendo sobre a primeira. Muitas vezes não no parâmetro formal, mas indiretamente, por meio de impactos concorrenciais e mercadológicos.

Ao decorrer da jornada da harmonização, caracterizada pela implementação de procedimentos que buscam modificar legislações internas com o propósito de criar o máximo de afinidade possível entre elas, houve a tentativa de unificação de áreas completas do Direito, visando torná-lo global.

É destaque a escolha do ramo comercial, devido às relações entre fronteiras, que incidem sobre os negócios. Em 1851 foi elaborada a minuta do "*National and International Code of Commerce Among All Civilised Nations*", seguido, em 1878, do "*Congress International du Commerce et de L'Industrie",* que objetivava a criação de um Código Internacional de Comércio, para tutelar todas as relações jurídicas sobre o tema (DE OLIVEIRA,2008). No entanto, este propósito não alcançou o resultado almejado.

No final do século XIX e início do XX, diante do reconhecimento do insucesso da unificação de ramos jurídicos inteiros, partiu-se para outra abordagem mais realista e menos descomedida de unificação de áreas específicas, explica De Oliveira (2008). Neste contexto, foram assinadas as seguintes Convenções:

---

[134] Tradução livre do original: "Perhaps the best operational definition of transnational law is possible using images from the computer age: (1) law that is "downloaded" from the international realm into domestic law: for example, a concept of international law that is domesticated or internalized in municipal law , such as the international human rights norm against disappearance, now recognized as domestic law in most municipal systems; (2) law that is "uploaded, then downloaded": for example, a rule that originates in a system, such as the guarantee of a free trial under the concept of due process in Western legal systems, which then becomes part of the law international, as in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and from there becomes internalized in almost all legal systems in the world; and (3) law that is borrowed or "horizontally transplanted" from one country system to another: for example, the "unclean hands" doctrine, which has migrated from British equity law to many other legal systems".

> Convenção de Paris sobre Propriedade Intelectual, de 20 de março de 1883, a Convenção para Unificação de Certas Regras Relativas ao Transporte Aéreo Internacional, de 12 de outubro de 1929 (“Convenção de Varsóvia"), as Convenções de Genebra sobre Cheques, em março de 1931, e algumas convenções da Conferência de Haia sobre direito de família, como a convenção para regular os conflitos de lei em matéria de casamento, a Convenção para regular a tutela de menores e a Convenção para regular os conflitos de leis e jurisdições em matéria de divórcio e separação de corpos , todas de junho de 1902 (DE OLIVEIRA, 2008, p. 30).

No período pós Segunda Guerra Mundial o movimento universalista e de aproximação normativa desenhou-se de maneira mais consistente. Intentou-se a construção de um ambiente normativo internacional, no qual é possível dialogar com os ordenamentos internos dos Estados-Nação.

Tudo ocorreu devido ao fenômeno da globalização, caracterizado pelo “estabelecimento de padrões globais estéticos, comportamentais, tecnológicos e também no campo normativo pela necessidade de facilitar a movimentação de fatores produtivos” (DE OLIVEIRA, 2008, p. 31).

Ao contextualizar o surgimento da globalização, é possível enxergá-la como possibilitada pela emergência da ascensão das tecnologias computacionais, que viabilizaram um crescente e mais veloz compartilhamento de informação ao longo do globo, aliada a outros fatores, como, por exemplo, o desenvolvimento de meios de transporte.

É também neste contexto de desenvolvimentos técnicos do século XX, que, na década de 1970, surge a primeira geração de Leis de proteção de dados pessoais, como descrito na seção 2 da presente dissertação, que se apoia no então recente temor em relação à garantia dos direitos de privacidade em sua relação com a marcha das inovações.

A partir do século XIX iniciou-se uma perspectiva nacional do Direito, vinculado sempre a um determinado Estado e dominante dentro de suas fronteiras. De Oliveira (2008) aponta que naquele momento houve a divisão jurídica entre o *Jus civile* e *Jus gentium:* o primeiro tratando da tutela dos conflitos internos, e o segundo das questões internacionais.

Porém, o avanço dos diálogos transfronteiriços entre os Estados, no contexto de sociedade da informação[135]torna quase inevitável o desejo de retorno a uma universalidade normativa sobre assuntos que ultrapassam as fronteiras espaciais com maior facilidade, como os dados pessoais digitalizados, eles quando analisados seus principais dispositivos legais,

[135] A sociedade da informação é reconhecida não somente pelo aumento de informação disponível, mas também pela nova forma do fluxo de informações. Para o teórico Manuel Castells, a característica central desta era que faz jus à caracterização de uma nova sociedade, a sociedade-rede, protagonizada de forma descentralizada pelos indivíduos, não é a informação em si, mas sim a comunicação. As redes de informação já existiam em outros meios, a diferença qualitativa das redes de informação atuais seria, portanto, a dupla via do fluxo de comunicação, na interação entre indivíduos (MAGRONI, 2014).

apresentam traços de harmonização.

Ao explicar o significado do termo harmonização, De Oliveira (2008) questiona o uso das palavras ‘unificação’ e ‘uniformização’ como sinônimos. Ele indaga se há de fato uma diferença nos conceitos dos três vocábulos e define que o termo harmonização jurídica pode ser considerado um conceito distinto, e as demais palavras entendidas como sinônimos implicam em fenômenos ímpares:

> Se de um lado, uma corrente defende a diferenciação apenas teórica entre esses conceitos, uma vez que na prática são utilizados aleatoriamente, de outro, existe uma escola que entende que, embora as expressões sejam utilizadas indistintamente, elas indicam fenômenos jurídicos diferentes (DE OLIVEIRA, 2008, p. 40).

A harmonização pode ser descrita a partir de medidas cujo objetivo é “diminuir divergências entre normas de direito material, processual ou conflitual de ordenamentos jurídicos diferentes. Seu resultado é a coexistência afinada de sistemas autônomos e independentes” (DE OLIVEIRA, 2008, p. 40).

Viegas (2004) entende a harmonização jurídica como gênero, abarcador de espécies distintas, que vão desde um mínimo de aproximação jurídica até um máximo, podendo existir na mesma classe jurídica um grau mínimo ou máximo de harmonização.

O grau mínimo de harmonização ocorre quando apenas alguns pontos ínfimos específicos são comuns em distintos ordenamentos internos de países, como, por exemplo, uma afinidade em legislar sobre algum tema específico. Já o máximo ocorre quando há uma maior semelhança entre determinadas leis de países distintos, o que para a autora já é considerado ‘unificação legislativa’.

A uniformização é definida por Viegas (2004) como mero sinônimo do termo harmonização, com a mesma característica de desejar a aproximação e presumir a existência do mínimo ao máximo grau de efetivação real, segundo o empenho dos Estados envolvidos. No mesmo sentido, De Oliveira (2008, p.42) define a uniformização como “o conjunto de disposições legislativas adotadas pelos Estados com a vontade comum de submeter certas relações jurídicas à mesma regulamentação”.

Porém, aponta a uniformização como causa da criação de um ambiente normativo internacional, capaz de impor em certo grau, uma padronização mais eficaz. São exemplos: convenções internacionais de direito uniforme e aquelas que têm em anexo uma lei modelo.

A unificação é reconhecida por De Oliveira (2008) como um processo mais intensivo que a harmonização e a uniformização, tendo como característica a utilização de legislação exata ou comum. É também considerada o último estágio da harmonização como gênero:

> Unificação legislativa é justamente o grau máximo de aproximação jurídica que porém não é simples de ser alcançado, já que além de um idêntico corpo de regras, para que estejamos diante de um Direito uniforme propriamente dito, esse Direito deve ser interpretado e aplicado também de modo uniforme (VIEGAS, 2004, p. 629).

Por fim, a diferenciação entre harmonização, uniformização e unificação jurídica, aponta as particularidades dos instrumentos e intensidades, numa linha de progresso iniciada na harmonização indo até a unificação: "pode-se dizer que o direito unificado é também uniforme e harmonizado, e que o caminho contrário seja necessariamente verdadeiro" (DE OLIVEIRA, 2008, p. 44). O mérito teórico está na possibilidade de diferenciar o gênero e suas espécies: o gênero é a aproximação jurídica, denominada frequentemente de harmonização; e as espécies a uniformização e a unificação legal.

Desde os anos 2000 é perceptível o reconhecimento no nível global do direito à proteção de dados pessoais. Mesmo com níveis distintos nas regiões do globo e nas jurisdições internas dos países, que possuem níveis distintos em termos de aplicabilidade e grau de prioridade nos seus ordenamentos, há a tendência de convergência sobre o tema. Lynn *et al.* (2020) apontam como exemplo do reconhecimento da proteção de dados pessoais o caso da Europa e dos Estados Unidos:

> Ambos os sistemas jurídicos reconhecem a importância de proteger os dados pessoais e os potenciais riscos decorrentes da utilização abusiva desses dados. No entanto, nos dois lados do Atlântico, dois modelos surgiram no campo da privacidade de dados (LYNN *et al.,* 2020, p. 69)[136].

Apesar de reconhecer que as potências econômicas trataram de maneira distinta a privacidade[137], Lynn *et al.* (2020) apontam o modo quase simultâneo do surgimento da preocupação normativa sobre o tema nos Estados Unidos e na Europa, que constituíram modelos regulatórios no campo da proteção de dados. A UE adotou um regulamento geral, enquanto os EUA rejeitaram um modelo semelhante, optando por tutelar setores específicos, sendo disso exemplo o *Privacy Act,* de 1974, que tutelava os dados processados por Agências Federais.

Ao refletir sobre a decisão estadunidense por não possuir regulamento geral de proteção de dados, faz-se válido relembrar que o país é onde está localizado o Vale do Silício,

[136] Tradução livre do original: "Both legal systems recognize the importance of protecting personal data and the potential risks arising from the misuse of such data. However, on both sides of the Atlantic, two models have emerged in the field of data privacy".

[137] Na Europa, o direito à privacidade e a proteção de dados pessoais foi reconhecida como um direito fundamental. Já nos Estados Unidos, a privacidade de modo geral estava diretamente relacionada com o direito à propriedade e, consequentemente, a vida privada (CASSINO, 2022).

no estado da Califórnia "[…]sede das principais empresas que possuem a custódia das maiores bases de dados pessoais do mundo" (CASSINO *et al.,* 2022, p. 76). Este é o cenário propício para serem desenvolvidos *softwares* para plataformas digitais com fim monetário da coleta massiva de dados:

> Essas plataformas corroboram para o surgimento de grandes empresas monopolistas e estão em cinco tipos emergentes no capitalismo de plataformas: de publicidade; de nuvem; industriais; de produtos e enxutas. As plataformas de nuvem consolidaram as plataformas como um modelo de negócios poderoso e único. Elas disponibilizam às empresas uma infraestrutura virtual de computadores, servidores, sistemas de inteligência de negócios e aprendizagem de máquina (*machine learning*). Google, Amazon, Microsoft e Alibaba já se destacam neste tipo de negócio, em que o principal objetivo é incentivar as empresas a externalizar seus sistemas, dados e negócios para infraestrutura em nuvem (CASSINO *et al,* 2022, p. 78).

Ao contrário dos Estados Unidos, na Europa, o Regulamento Europeu, passou a tutelar as transferências internacionais de dados pessoais[138]. O regulamento permitiu a livre circulação das informações entre os membros da UE, mas restringiu a transferência para países terceiros, até que um nível adequado de proteção na legislação interna tenha sido atingido[139], e ela tenha sido autorizada por meio de decisão passível de atestar se o Estado destinatário corresponde ou não aos padrões exigidos pela UE.

Como previamente comentado, o impacto do Regulamento Geral de Proteção de Dados da União Europeia (2016/679) foi essencial para a consolidação da proteção de dados pessoais internacionalmente.

A organização acabou por gerar a convergência de normas sobre o tema em diversas localidades, a exemplo de "países como Israel, Argentina, Uruguai e recentemente o Japão, têm sido certificados como provedores correspondentes ao nível de adequação exigido pela União Europeia para transferência de dados consoante a Comissão Europeia" (LYNN *et al.*, 2020, p. 71)[140].

---

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

[139] "Art. 45: Transferências poderão ser feitas com base na avaliação do nível de adequação atingido para um dado país; pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica" (UNIÃO EUROPEIA, 2016).

[140] Tradução livre do original: "Countries such as Israel, Argentina, Uruguay and recently Japan, have been certified as providers corresponding to the level of adequacy required by the European Union for transferring data according to the European Commission".

Apesar da relutância dos EUA em se comprometer com as diretrizes europeias Lynn *et al.* (2020) afirmam que existia um certo grau de acordo entre o país e a Comissão Europeia sobre a temática de proteção de dados. Ainda em 2000 a União Europeia adotou a Decisão 2000/520/EC denominada de 'porto seguro', que estabeleceu aos Estados Unidos adequação de suas regras de proteção de dados. A partir dela, as empresas dos Estados Unidos sujeitas à supervisão da Comissão Federal de Comércio deveriam certificar a sua adesão aos Princípios do *Safe Harbor*.

Porém, com as revelações de Snowden sobre a existência de programas de vigilância em massa dos EUA, houve a invalidação da decisão pelo Tribunal Europeu de Justiça (ECJ)[141]. Isto gerou a substituição do *Safe Harbor* pelo chamado *Privacy Shield*, que foi negociado entre a Comissão Europeia e as autoridades norte-americanas em 2016 e entrou em vigor com a Decisão 2016/1250. De acordo com Lynn *et al.* (2020), o novo sistema é muito semelhante ao *Safe Harbor* em termos de funcionamento, mas foi acompanhado por uma série de outras garantias, especialmente em relação ao direito individual de reparação.

Porém, em 2020 o *Privacy Sheild* existente entre a União Europeia e os Estados Unidos foi anulado pelo Tribunal de Justiça da União Europeia (TJUE). Segundo Davies (2021), o Tribunal concluiu que haviam programas de vigilância dos EUA que não cumpriam o princípio da necessidade na coleta de dados dentre outras infrações. O que resultou na anulação do acordo e, num vácuo jurídico para o futuro do fluxo de dados entre as partes. Davies afirma que o papel antes desempenhado pelo *Privacy Sheild* nas transações comerciais recaiu nas cláusulas contratuais específicas sobre a proteção de dados.

Já no Brasil haviam discussões acerca da necessidade de tutelar as demandas da utilização de novas tecnologias digitais desde o começo do século XXI, intensificadas pela popularização da *internet* na década de 90, como aponta Lima (2022). O advento do Regulamento Europeu, em 2016, voltou a atenção dos legisladores brasileiros para a necessidade da implementação de uma lei específica para a proteção de dados. Explica:

> A intenção era ter três leis estruturais e inter relacionadas, que deveriam ser compreendidas e aplicadas sistematicamente: 1) A Reforma da atual Lei dos Direitos Autorais, em vigor desde a década de 1990; 2) A Criação do Marco Civil Brasileiro da Internet, para regular direitos e deveres dos usuários e provedores de serviços de internet; 3) A Criação de uma Lei Geral de Proteção de Dados Pessoais, inspirada no RGPD europeu (LIMA,2020, p. 285).

[141] No caso Schrems (C-362/14), decidido em 2015, o TJE considerou que a Comissão, ao certificar a adequação do esquema Safe Harbor, não levou em consideração o poder das autoridades policiais dos EUA de acessar de forma generalizada os dados da UE transferidos sob o esquema Safe Harbor (COLE & FABBRINI, 2016; PADOVA, 2016). De acordo com o ECJ, tal modelo de vigilância em massa não pode ser tolerado, pois compromete a essência do direito à privacidade, protegido pela Carta de Fundação da UE de direitos fundamentais (parágrafo 94 da sentença; ver OJANEN, 2017).

Dentre as normas da jornada legislativa da privacidade de dados pessoais no Brasil que levaram à LGPD, estão as delimitações quanto ao manuseio dos dados e segurança nas operações de consumo, previstas no Código de Proteção e Defesa do Consumidor[142], que garantiu o acesso individual às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre o consumidor, bem como sobre as suas respectivas fontes.

Em seguida, no ano de 2011, foi promulgada a Lei n. 12.414/2011. Ela foi relevante para a matéria da utilização de dados pessoais para fins específicos. Popularizada como Lei do 'Cadastro Positivo', teve como objetivo formar um banco nacional de dados referentes às informações de operações financeiras e de adimplemento para fins de concessão de crédito.

Como resultado, "essa nova peça legislativa setorial acabou por trazer, de uma forma original e mais sistematizada, a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los" (BIONI, 2020, p. 122).

Em seguida, num período no qual os legisladores brasileiros já haviam reconhecido que não era mais possível adiar a regulamentação das interações jurídicas advindas das inovações tecnológicas computacionais, buscou-se ampliar a atuação referente à proteção da privacidade informacional de dados.

Neste contexto, foi elaborado o Marco Civil da Internet (MCI), em 2014, com o ambicioso propósito de tutelar o uso do ciberespaço no Brasil, através do estabelecimento de princípios, garantias, direitos e deveres aos provedores e também aos usuários da *internet*.

O MCI, nos seus primeiros artigos[143], dispõe de diretrizes e princípios referentes à liberdade de expressão e também à privacidade dos indivíduos. O texto traz consigo a garantia da inviolabilidade do sigilo do fluxo das comunicações *online* do usuário, podendo

---

[142] 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.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas (BRASIL, 1990).

[143] Art. 7º O acesso à *internet* é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
[...] Art.10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014).

ser quebrada apenas por ordem judicial.

Há também no MCI, assim como na subsequente LGPD, informações claras e completas sobre a coleta; uso; armazenamento; tratamento e proteção dos dados pessoais, junto à exigência de justificativa e do atendimento a finalidades que não sejam vedadas pela legislação. Também foi prevista na norma anterior à LGPD o princípio do efetivo consentimento, no qual há a garantia do indivíduo ter informações claras e completas constantes dos contratos de prestação de serviços[144].

Porém, mesmo com os avanços na privacidade de dados trazidos pelo MCI, o debate acerca de uma legislação específica se tornou cada vez mais relevante. Principalmente diante das pressões externas ao Brasil, no sentido de coibir o tratamento abusivo de dados pessoais, em um contexto no qual a relevância da economia de dados ganhava espaço em Organizações Internacionais e em países desenvolvidos, aos olhos do comércio internacional.

A criação do texto da Lei Geral de Proteção de Dados Brasileira ocorreu em 2018 e possuiu inspiração direta no Regulamento Europeu. A norma brasileira dispõe de artigos semelhantes nos quesitos de responsabilidade dos agentes de tratamento, direitos dos titulares dos dados e também, sobre os requisitos para ocorrer transferência de dados internacionais.

A inspiração europeia na construção da Lei n. 13.709/2018 é exemplo não só do interesse brasileiro de dialogar comercialmente com a União Europeia, mas, principalmente do protagonismo e do poder unilateral de legislar desta.

O movimento convergente das normas pode ser observado na medida que a matéria de proteção de dados acabou por impactar o diálogo com as empresas transnacionais de tecnologia e gerou a necessidade de existir uma padronização mínima como requisito da interação comercial no território brasileiro.

O protagonismo da União Europeia e também da OCDE em legislar sobre diretrizes referentes à proteção de dados pessoais não é apenas dessa organização. Há também uma tendência emergente em outras organizações de Direito Internacional Privado no estabelecimento de padrões normativos sobre o tema.

Em 2015, o Instituto Internacional para a Unificação do Direito Privado (UNIDROIT), a partir de uma sugestão de proposta do Ministro da Justiça da Hungria para a

---

[144]Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
[...] 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 (BRASIL, 2014).

criação de um modelo de normas destinado a tutelar os Negócios informatizados (*Business informatics*).

Em 2019, a secretaria da UNCITRAL publicou *Notas sobre os principais problemas de Contratos de computação em nuvem*. Em 2020 houve, por parte da UNCITRAL, uma proposta de que as duas organizações explorassem a temática jurídica referente às demandas comerciais surgidas do ambiente digital. Em seguida, a Organização dos Estados Americanos (OEA), em 2021, publicou uma cartilha atualizada sobre os princípios da proteção de dados pessoais.

Ainda em 2021, a OCDE publicou A medição do uso de serviços em nuvem pelas empresas (*Measuring the use of cloud Services by Business)*. Este documento se baseou em uma extensa coleta de dados sobre a utilização da tecnologia em nuvem no ambiente dos negócios. Através dele é reconhecida a importância crescente dos serviços *online* possibilitados por computação em nuvem para empresas, organizações diversas e também indivíduos:

> As infraestruturas de nuvem sustentam uma gama cada vez maior de serviços e ferramentas online usados por empresas (e indivíduos). Nos países da OCDE, mais de um terço das empresas comprou alguma forma de serviços em nuvem em 2018, acima dos 20% em 2015 (OCDE, 2021)[145].

O documento acima revela que diversos países-membros da OCDE já utilizam de *cloud* e que no intervalo de três anos — entre 2015 e 2018 — esse número aumentou para um terço das empresas nos países-membros que adquiriram algum tipo de serviço em nuvem.

Já dentre os que mais consomem produtos disponibilizados através da *cloud,* se destacam três membros da OCDE: em primeiro lugar, os Estados Unidos, com mais de 450 bilhões de dólares gastos; em seguida, o segundo maior mercado de *cloud,* a Alemanha, que dispõe cerca de 160 bilhões de dólares; em terceiro é o Reino Unido, com 80 bilhões de dólares[146].

A alta demanda do paradigma de computação em *cloud* e sua relevante presença comercial é realidade no que podem ser considerados os países da 'elite' econômica do mundo. Através da atenção dada ao tema da economia digital, que leva à tutela da questão da proteção de dados pessoais, é possível perceber a emergência de uma tendência legislativa.

---

[145] Tradução livre do original: "Cloud infrastructures underpin an ever-increasing range of online services and tools used by businesses (and individuals). In OECD countries, over one third of businesses purchased some form of cloud services in 2018 (OECD, 2019[1]), up from 20% in 2015" (OECD, 2017).

[146] Tradução livre do original: "The consumption of broad cloud-containing product categories is far greater in the United States, at over USD 450 billion, than in other countries – the second-largest market, Germany, totals around USD 160 billion, while the United Kingdom follows with around USD 80 billion" (OCDE, 2021, p. 21).

Há nas principais organizações internacionais de direito privado a observância à tutela da privacidade informacional e também das demandas criadas pelas tecnologias computacionais ao comércio.

Este amparo legal apresenta traços da convergência de diretrizes, como definidos por Bennett (1991), e revela existir um certo sucesso no caminho de harmonização jurídica internacional na matéria, mediante um processo com fortes bases principiológicas. Importante ressaltar que as *Big Techs*, como, por exemplo, a *Amazon*, assumem papel protagonista e dúbio neste processo.

Elas criam novos paradigmas tecnológicos acompanhados de impactos econômicos — como a computação em nuvem — extremamente relevantes para o comércio interno e internacional. Junto a isto, aumenta a vulnerabilidade da privacidade do indivíduo, característica dos avanços tecnológicos da economia da informação.

Porém, ao mesmo tempo que criam demandas legislativas fruto das suas atividades comerciais, as *Big Techs* também são impactadas pela normatividade que operam sobre as Organizações Internacionais e fazem da adequação uma oportunidade competitiva para exercerem sua presença em cada vez mais localidades.

Apesar do visível esforço normativo interno e internacional — e independente das motivações que os movem — visualizado através das diversas publicações das Organizações Internacionais a fim de tutelar os impactos dos novos paradigmas tecnológicos na economia e nos direitos dos indivíduos, ainda há uma disparidade temporal na velocidade com a qual o Direito consegue agir diante das inovações tecnológicas apresentadas pelas *Big Techs.*

Ao discutir o tema dos impactos possíveis que podem surgir da utilização de inteligência artificial e os possíveis caminhos para amenizar impactos negativos, Amy Webb (2019) afirma ter conversado com legisladores que afirmam que limitar através de leis o desenvolvimento de algo considerado tão delicado e com alto risco de imprevisibilidade como a inteligência artificial é a única solução. Ela explica que também costuma dialogar com os acadêmicos envolvidos nas pesquisas com IA, e comenta sobre eles:

> Esmagadoramente, eles trabalham em nove gigantes da tecnologia - Google, Amazon, Apple, IBM, Microsoft e Facebook, nos Estados Unidos e Baidu, Alibaba e Tencent na China - que estão construindo IA para inaugurar um futuro melhor e mais brilhante para todos nós. Acredito firmemente que os líderes dessas nove empresas são movidas por um profundo senso de altruísmo e um desejo de servir ao bem maior: eles vêem claramente o potencial da IA para melhorar a saúde cuidado e longevidade, para resolver nossos problemas climáticos iminentes e para retirar milhões de pessoas da pobreza. Já estamos vendo os benefícios positivos tangíveis de seu trabalho em todas as indústrias e na vida cotidiana (WEBB, 2019, p. 14)[147].

[147] Tradução livre do original: “Overwhelmingly, they work at nine tech giants—Google, Amazon, Apple, IBM, Microsoft, and Facebook in the United States and Baidu, Alibaba, and Tencent in China—that are building AI in

A autora afirma que o problema está nas forças externas que acabam por operar sobre o desenvolvimento dessas tecnologias: “nos EUA, as demandas implacáveis do mercado e as expectativas irrealistas de novos produtos e serviços tornaram impossível o planejamento de longo prazo” (WEBB, 2019, p. 14). E finaliza por dizer que o governo dos Estados Unidos “culpam os gigantes da tecnologia dos EUA, quando poderiam convidar essas empresas a participar dos níveis mais altos de planejamento estratégico (tal como existe) dentro do governo” (WEBB, 2019, *idem*).

Como Webb (*idem*), já no século XIX, Edson e Ford já expressavam preocupações sobre o imperativo poder do capital sobre as inovações tecnológicas e a possível deturpação do seu fim de progresso para a humanidade. A partir do recorte do Direito Internacional Privado, é possível dizer que as OI têm impactado na discussão das demandas normativas advindas das novas e constantes mudanças tecnológicas, através da publicação de documentos e relatórios sobre o tema, ferramentas da convergência por penetração, descrita por Bennett (1991).

---

order to usher in a better, brighter future for us all. I firmly believe that the leaders of these nine companies are driven by a profound sense of altruism and a desire to serve the greater good: they clearly see the potential of AI to improve health care and longevity, to solve our impending climate issues, and to lift millions of people out of poverty. We are already seeing the positive and tangible benefits of their work across all industries and everyday life”.

5 CONCLUSÕES

A presente dissertação analisa a ascensão da proteção de dados pessoais ocorrida junto ao protagonismo da economia da informação segundo os parâmetros do Direito Internacional Privado. Junto a isto são apresentadas as tendências legislativas que emergem atreladas a popularização dos meios computacionais e da *internet,* respectivamente sobre a privacidade e sobre a proteção de dados informacionais.

Identificaram-se os marcos jurídicos da proteção de dados pessoais a partir da perspetiva geracional das normas em diversos ordenamentos internos e também advindos de Organizações Internacionais como a OCDE e a União Europeia. A partir disto, conclui-se o destaque da União Europeia e da publicação do Regulamento de Proteção de Dados Pessoais da organização como atuante no movimento de convergência, inclusive sobre o Brasil.

Em seguida foi constatado como paradigma computacional predominante atualmente a computação em nuvem, que devido aos seus aspectos mais marcantes de ubiquidade e a facilidade de transferência de dados pessoais foi objeto de estudo do presente trabalho.

Constatou-se que o uso da computação em nuvem gerou impactos em diversos marcos regulatórios da adequação à proteção de dados devido à dificuldade na localização certa dos dados pessoais; a falta de transparência no tratamento, caracterizado pela falta de informações explícitas e precisas, de fácil interpretação para o usuário e inerentes à prestação; a existência de subcontratantes; a dificuldade do controle do acesso à informação ou medidas de segurança; e, por fim, a falta de controle destas informações pelo provedor do serviço em nuvem.

O presente trabalho concluiu como as principais implicações contratuais da computação em nuvem a dificuldade de definição específica das partes, localidade do fornecimento dos produtos ou serviços em *cloud* e a transferência de dados pessoais entre países distintos. A partir da literatura existente sobre os aspectos contratuais da nuvem e também das diretrizes da UNCITRAL sobre o tema, conclui-se possível sanar as demandas jurídicas consideradas problemáticas na computação em nuvem principalmente através das ferramentas contratuais.

Ao analisar as ferramentas contratuais descritas pela literatura como meio de lidar com os serviços de computação em nuvem concluiu-se ser de grande importância o uso do *Service Level Agreements* (SLA), documento utilizado nos negócios realizados entre o

provedor e o consumidor do serviço em *cloud* que junto aos contratos de serviço fazem parte do chamado processo de gestão de nível de serviço (SLM) o qual descreve as ações que determinam, documentam e acatam os requisitos para execução dos serviços contratados.

São fundamentais a previsão de cláusulas específicas sobre proteção de dados e também sobre a localização dos dados conforme a norma interna específica. A partir do entendimento da infraestrutura da instalação dos serviços de computação em nuvem, composta pelo edifício no qual se localiza o *Data Center,* a sala de servidores e toda a estrutura que possibilita o funcionamento da computação em nuvem, é possível delinear diretivas sobre a jurisdição na qual os dados e os provedores da *cloud computing* operam e solucionar questões que advêm da dificuldade de localização dos dados.

É essencial nos contratos desta natureza que as partes envolvidas no serviço conheçam e entendam os conceitos principais e também as relações-chave para a contratação de serviços de computação em nuvem. É indispensável a realização do acordo de serviço junto à definição das responsabilidades das partes envolvidas.

Sob o olhar dos tipos de convergência listados por Bennett, conclui-se como aplicável à adequação da proteção de dados brasileira e também a adequação das empresas como a *Amazon* à LGPD, a convergência por penetração. Nela, determinados ordenamentos internos, são coagidos a entrar em sintonia com ações normativas adotadas por outros Estados-Nação, geralmente guiadas por agentes privados, como as ETN's e as Organizações Internacionais de Direito Privado, a União Europeia, a OCDE e a UNCITRAL.

O caso do Brasil ilustra uma tendência global de que os países de fora do grupo membro de organizações internacionais relevantes economicamente precisam se adequar aos padrões internacionais exigidos pela OCDE. Para fazê-lo, o Brasil e outros estados-nação periféricos, visam espelhar-se no Regulamento Europeu. Isto se deu não só pela necessidade do país de estar apto a negociar com os países-membros da UE, mas, porque a União Europeia representa hoje uma das organizações com maior impacto nas áreas de regulamentação internacional, compondo uma elite global legislativa.

Bennett também descreveu as ETN's como parte do processo de convergência por penetração. O papel das empresas transnacionais seria o de operar uma força normativa através do capital, para impelir as OI's a legislarem de maneira favorável às suas atividades.

A presente dissertação conclui que há uma tendência de harmonização normativa através da convergência de diretrizes por parte das Organizações Internacionais sobre o tema da proteção da privacidade informacional. Isto se evidencia na crescente tutela por meio de documentos, diretrizes e discussões sobre o assunto e sobre computação em nuvem

disseminado através da produção de vasta literatura por organizações de direito privado como a UNCITRAL; OCDE; União Europeia e OEA.

Junto a isto, as *Big Techs* transnacionais passaram a enxergar a adequação e a proteção de dados pessoais como inevitáveis diante da economia informacional e, em certa medida, como uma vantagem comercial. Sendo assim, houve por parte delas a iniciativa de adequar-se às legislações internacionais (GDPR; UNCITRAL) e consequentemente às internas (LGPD) sobre o tema, para o fim de garantirem sua presença e o fluxo de transferência de dados no maior número de territórios possíveis, este foi o caso da empresa *Amazon*.

Também é perceptível ao longo do desenvolvimento da presente dissertação, o dúbio papel das *Big Techs* no processo de convergência do tema da privacidade informacional. Conclui-se que, ao mesmo tempo que elas dão causa à necessidade de tutelar suas atividades fortemente voltadas para a coleta massiva de dados, resultando na vulnerabilidade da privacidade dos usuários, elas também sofrem impactos das legislações advindas de OI como a União Europeia, e tem de se adequar às normas delas para continuarem suas atividades em países afetados pela Convergência de Diretrizes, como no Brasil.

REFERÊNCIAS

ABBATE, Janet. **Inventing the Internet**. MIT Press, 2000.

ALDÉ, Alessandra. O internauta casual: notas sobre a circulação da política na internet. **REVISTA USP**, São Paulo, n.90, p. 24-41, junho/agosto 2011.

AMAZON. Navegando na conformidade com a LGPD na AWS.**Amazon Web Services**. 2020. Disponível em: <https://aws.amazon.com/pt/compliance/brazil-data-privacy/>. Acesso: 11 de Mar. 2022.

AMAZON. About AWS Global Infrastructure. **Amazon Web Services**. 2022. Disponível em: < https://aws.amazon.com/pt/about-aws/global-infrastructure/?p=ngi&loc=0>. Acesso: 15 de Ago. 2022.

ALEMANHA, Embaixada da República Federal. **60 anos da Lei Fundamental de Bonn**. 25 de Maio de 2009. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaArtigoDiscurso/anexo/discAlemanha.pdf> Acesso: 10 de Nov. 2022.

AYOMAYA, Badrudeen Ajibola. **Designing Datacenters: data center design guide**. Estados Unidos: Badrudeen Ajibola Ayomaya, 2020. 161 p.

BAPTISTA, Luiz Olavo. **Comércio eletrônico: uma visão do Direito brasileiro**. Revista da Faculdade de Direito, Universidade de São Paulo, v. 94, p. 83-100, 1999.

BIANCO, Philip; LEWIS, Grace A.; MERSON, Paulo. **Service Level Agreements in Service-Oriented Architecture Environments**. Pittsburgh, Pensilvânia: Carnegie Mellon University, 2008. Disponível em: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8615. Acesso em: 17 abr. 2023.

BENNETT, Colin J. What Is Policy Convergence and What Causes It? In: **British Journal of Political Science**, vol. 21, no. 2, 1991, pp. 215–33. JSTOR. Disponível em: <http://www.jstor.org/stable/193876> Acesso em: 1 Dez. 2022.

BENNETT, Colin & RAAB, , Charles D. **The Governance of Privacy: Policy Instruments in Global Perspective**. London: Routledge, 2003.

BESSA, André. Cloud: falando um pouco sobre Infraestrutura. 2022. Disponível em: <https://www.alura.com.br/artigos/cloud-falando-sobre-infraestrutura> Acesso: 23 Out. 2022.

BIONI, Bruno Ricardo. **Proteção dos dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019.

BOBBIO, Noberto. **A era dos Direitos**. 7. ed. Rio de Janeiro: Elsevier, 2014.

BRANDEIS, Louis; WARREN, Samuel. The right to privacy. In: **Harvard Law Review**, v. 4, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm> Acesso em dez. de 2022.

BRASIL. Lei n. 8.078, 1990. Código de Defesa do Consumidor. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Acesso em: 10 de Mar. 2023.

BRASIL, Marco Civil da Internet. Brasília, DF, 2014. Disponível em: <https://www.planalto.gov.br/civil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 20 de nov. de 2022.

BRASIL, Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG). **LGPD na SEF**. Minas Gerais, 2022. Disponível em: <http://www.fazenda.mg.gov.br/transparencia/lgpd> Acesso em set. 2022.

BRASIL, Lei Geral de Proteção de Dados Pessoais, Brasília, DF, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em ago. de 2022.

BRICKMAN, Ronald. Science and the Politics of Toxic Chemical Regulation: U. S. and European Contrasts. In: **Science, Technology & Human Values,** Vol. 9, No. 1, 1984, pp. 107-111.

BRITTO-DA-SILVA, Vergilio Ricardo; LUCIANO, Edimara Mezzomo; MAGNAGNAGNO, Odirlei Antonio. Preocupação com a privacidade na internet: uma pesquisa exploratória no cenário brasileiro. **Anais do V Encontro de Administração da Informação**, 2015, Brasil., 2015.

BISSO, Rodrigo et al. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. **Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**, v. 3, n. 1, 2020.

BONELL, Michael J. The law governing international commercial contracts and the actual role of the UNIDROIT Principles, **Uniform Law Review**, Volume 23, Issue 1, March 2018, Pages 15–41, https://doi.org/10.1093/ulr/uny001

CANCELIER, Mikhail V. de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. In: **Sequência: Estudos Jurídicos e Políticos**. Santa Catarina. v. 38 n. 76., 2017.

CANO, Carlos Baldessarini *et al*. Organizações no Espaço Cibernético: estudo comparativo altavista e amazon books. 2. ed. São Paulo, Sp: **Rae-Eletrônica**, 2002. 24 p. Disponível em: <http://www.rae.com.br/eletronica/index.cfm?FuseAction=Artigo&ID=1132&Secao=INFORMAÇÃO & Volume=1&Numero=2&Ano=2002>. Acesso em: 13 mar. 2023.

CARVALHO, José Carlos. O Brasil e as empresas transnacionais: os novos rumos para a transnacionalização das empresas nacionais. **Scientia Iuris**, [S.L.], v. 15, n. 1, p. 89-104, 22 jun. 2011. Universidade Estadual de Londrina. http://dx.doi.org/10.5433/2178-8189.2011v15n1p89. Disponível em: <https://ojs.uel.br/revistas/uel/index.php/iuris/article/view/7586>. Acesso em: 13 de maio de 2023.

CARVALHO, Tereza M. B.; GONZALEZ, Nelson M.; MIERS, Charles C.; REDÍGOLO, Fernando F.; ROJAS, Marco A. T. Segurança das nuvens computacionais: uma visão dos principais problemas e soluções. Dossiê Computação de Nuvem. In: **REVISTA USP,** São Paulo, n. 97, p. 27-42, Março e Abril, 2013.

CASSINO, João Francisco *et al* (org.). **Colonialismo de Dados:** como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. 212 p.

COURT OF KING 'S BENCH, **Semayne's Case**. 1604. Disponível em: <https://groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2005/weeks/semayne.html >. Acesso em: Mai. 23 de 2023.

D'AVILLA, A. G.; DA SILVA, B. F.; DE ARAUJO, T. V. **LGPD: Muito Além da Lei**. 2021. DeServ Tecnologia e Serviços. Edição Kindle. Disponível em: <https://www.amazon.com.br/LGPD-análise-conjunto-segurança-informação-ebook/dp/B094W526GL/ref=sr_1_1?qid=1670861207&refinements=p_27%3ADeServ++Tecnologia+e+Serviços&s=digital-text&sr=1-1&text=DeServ++Tecnologia+e+Serviços> Acesso em ago. de 2022.

DAVIES, Nahla. **O fim do Privacy Shield pode levar a um desastre para os provedores de nuvem em hiperescala**. 2021. Disponível em: <https://www.infoq.com/br/articles/privacy-shield-hyperscale-clouds/#:~:text=No%20final%2C%20o%20ECJ%20acabou,o%20crescimento%20e%20o%20desenvolvimento.>. Acesso em: 10 jun. 2023.

DATA PRIVACY BRASIL. O Valor Social e Político da Proteção de Dados: Entrevista com Colin Bennett. 1ª Ed. - São Paulo, In: **Creative Design Studio**, 2019.

DE OLIVEIRA, Renata F. **Harmonização Jurídica no Direito Internacional.** 2008. Edição. 1ª; Editora. Quartier Latin.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. In: **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315> .

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. Ed. Thomson Reuters, In: **Revista dos Tribunais**. São Paulo, Brasil, 2019. Edição Kindle.

DREZNER, Daniel W. Globalization and Policy Convergence. **International Studies Review**, vol. 3, no. 1, 2001, pp. 53–78. JSTOR, Disponível em: <http://www.jstor.org/stable/3186512>. Acesso em: 2 Abril 2023.

ESPANHA, Agencia Española de Protección de Datos (ed.). Guia para clientes que contraten servicios de Computing. Madrid, Espanha: **Agencia Española de Protección de Datos**, 2013. 23 p. Disponível em: https://www.aepd.es/es/documento/guia-cloud-clientes.pdf. Acesso em: 5 dez. 2022.

FERREIRA, D. A. A.; PINHEIRO, M. M. K.; MARQUES, R. M. Privacidade e proteção de dados pessoais: perspectiva histórica. In: **Revista de Ciência da Informação e**

Documentação, [S. l.], v. 12, n. 2, p. 151-172, 2021. DOI: 10.11606/issn.2178-2075.v12i2p151-172. Disponível em: https://www.revistas.usp.br/incid/article/view/179778. Acesso em: 15 mar. 2023.

FERNANDES, Felipe Oliveira. **Desenvolvimento de um computador de propósito geral analógico-digital**. 2022. 203 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Instituto de Ciência e Tecnologia da Universidade Estadual Paulista, Universidade Estadual Paulista, São Paulo, 2022. Disponível em: https://repositorio.unesp.br/handle/11449/235989. Acesso em: 2 abr. 2023.

GÓMEZ, Gonzalo Andrés Moreno. Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana. **Revista de Derecho, Comunicaciones y Nuevas Tecnologías**, Bogotá, Colombia, v. 9, n. 9, p. 5-27, 18 abr. 2013. Disponível em: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Jurisdiccion-y-cloud-Gonzalo-Moreno-2013.pdf>. Acesso em: 7 abr. 2023.

GASSER, Urs, **Cloud Innovation and the Law: Issues, Approaches, and Interplay** (Berkman Ctr.
Research Pub. No. 2014-7, Mar. 17, 2014).<http://nrs.harvard.edu/urn-3:HUL.InstRepos:16460372>. Disponível em: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:16460372>. Acesso em: 25 de Mar. 2023.

HINCK, Garrett; MAURER, Tim. Cloud Security: Report Subtitle: A Primer for Policymakers. In:**Carnegie Endowment for International Peace**, 2020. Disponível em: <https://www.jstor.org/stable/resrep25787.9> Acesso em 24 de out. de 2022.

HURRELL, A. Sociedade internacional e governança global. In: **Lua Nova**, São Paulo, n. 46, p. 55-75, 1999.

KOH, Harold Hongju. Why Transnational Law Matters. In: **Penn State International Law Review**, Vol. 24: No. 4, 2006.

LIMA, Cínthia. **Comentários à Lei Geral de Proteção de Dados**. Ed. Almedina. São Paulo, Brasil. 2020.

LIMA, Renata A., MAGALHÃES, Átila de A., DIAS, Thaís A. Conflitos dos Direitos Fundamentais na Perspectiva da Transnacionalização do Direito: Proporcionalidade e ponderação à luz de Robert Alexy. In: Meritum, **Revista de Direito da Universidade FUMEC**, 2017.

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

MAGRINI, Eduardo. **Digital Rights: Latin America and the Caribbean**.Rio de Janeiro. Editora FGV Direito Rio, 2021.

MAGRANI, Eduardo. **Entre dados e robôs**: Ética e privacidade na era da Hiperconectividade. Porto Alegre – RS: Editora Arquipélago. 2019.

MARTINS, Leonardo. **Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais**. Volume 1: Dignidade humana, livre desenvolvimento da Personalidade, direito fundamental à vida e à integridade física, igualdade / Leonardo Martins. São Paulo :Konrad-Adenauer Stiftung – KAS, 2016.

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

MENDES, Laura Schertel; BIONI, Bruno. O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**. Vol. 124. Ano 28. p. 157-180. São Paulo: Editora RT, jul-ago 2019.

MODESTO, Jessica A. Breves considerações acerca da monetização de dados pessoais na economia informacional à luz da Lei Geral de Proteção de Dados Pessoais. 2020. In: **Revista de Direito, Governança e Novas Tecnologias**. V. 6, N. 1, junho, 2020.

MORELLI, Lucas. **Relação de Consumo e o Contrato de Cloud Computing**. 2018. 213 f. Dissertação (Mestrado) - Curso de Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, Sp, 2018. Acesso em: 19 de Maio, 2023. Disponível em: < https://doi.org/10.11606/D.2.2018.tde-25092020-165221>.

MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política**. São Paulo, Sp: Ubu Editora, 2018. 192 p.

NAVARRO, ANA M. LEONARDOS, Gabriela. **Privacidade Informacional**: origem e fundamentos no Direito Norte-Americano. Laboratório de Estudos Teóricos e Analíticos sobre o Comportamento das Instituições (LETACI). Programa de Pós-Graduação em Direito da Universidade Federal do Rio de Janeiro. 2011.

NAWAZ, Mohammad. **Data Center Management**: your guide to efficient data center operation. Estados Unidos: Amazon Digital Services Llc, 2019. 166 p.

OCDE. Policy, Committee On Digital Economy (org.). Measuring cloud services uses by businesses. Paris, França: **Oecd Publishing**, 2021. 304 v. Disponível em: https://www.oecd.org/sti/ieconomy/measuring-cloud-services-use-by-businesses-71a0eb69-en.htm. Acesso em: 12 mar. 2023.

OSHODI, Kayodi. **What is Cloud Computing**: cloud computing for dummies. Estados Unidos: Intzom, 2022.

PESSOA, Camila. **Decifrando Alan Turing**: sua vida e trajetória no mundo da tecnologia. 2022. Disponível em: <https://www.alura.com.br/artigos/decifrando-alan-turing-vida-trajetoria-tecnologia?gclid=Cj0KCQiAg_KbBhDLARIsANx7wAwo8u9MgtMjOPllmR1p_ZbvK5LG--KCEQSHvx0g_eWa5imyLXxsn6kaApPDEALw_wcB> Acesso: 12 Ago. 2022.

PEREZ, Camila Behrends. **Participação das empresas transnacionais no desenvolvimento tecnológico do Brasil e da China**. 2016. 74 f. TCC (Graduação) - Curso de Economia, Departamento de Economia e Relações Internacionais, Universidade Federal do Rio Grande

do Sul, Porto Alegre, Rs, 2016. Disponível em: <http://hdl.handle.net/10183/167295>. Acesso em: 15 abr. 2023.

PINTO, Álvaro V. **O Conceito de Tecnologia**. Rio de Janeiro. Editora Contraponto. v. 2. 2005.

RODRIGUEZ, Daniel Piñeiro; SARLET, Ingo Wolfgang. O direito fundamental à informação e um novo marco regulatório informacional. **Revista Direitos Humanos Fundamentais**, Osasco, São Paulo, v. 15, n. 1, p. 81-98, 18 nov. 2015. Disponível em:<https://repositorio.pucrs.br/dspace/handle/10923/11321>. Acesso em: 3 de Mar, 2023.

SAMPAIO, Vinicius. **Proteção de Dados Pessoais**: da privacidade ao interesse coletivo. Rio de Janeiro, Lumen Juris. 2020.

SALDANHA, Paloma M. (coord.). **O que estão fazendo com os meus dados?** A importância da Lei Geral de Proteção de Dados. Recife: Editora SerifaFina, 2019.

SATORELLO, Leandro. **O que é Cloud?**. 2022. Disponível em: <https://www.alura.com.br/artigos/o-que-e-cloud-e-seus-principais-servicos> Acesso em: 25 de Nov. 2022.

SINGH, Sk. **Cloud Computing**: Cloud Computing Fundamentals | IaaS | PaaS | SaaS | FaaS | Serverless Computing | Virtualization | Virtual Machine | Hypervisor | Docker. Estados Unidos: Knodax, 2022. 270 p.

SILVA, Rosane Leal da et al. A responsabilidade civil dos principais cloud computing providers em razão da perda de arquivos. **Revista da Faculdade de Direito Ufpr**, [S.L.], v. 63, n. 2, p. 89-113, 31 ago. 2018. Universidade Federal do Paraná. http://dx.doi.org/10.5380/rfdufpr.v63i2.58628. Disponível em: <https://revistas.ufpr.br/direito/article/view/58628>. Acesso em: 20 mar. 2023.

SILVEIRA, Leonardo; LIMA, Weldson Q. Um breve histórico conceitual da Automação Industrial e Redes para Automação Industrial. **Redes para Automação Industrial**. Universidade Federal do Rio Grande do Norte, p. 16, 2003.

SCHWARTZ, Paul M. Global Privacy Data: The EU Way, 94 New York, In: **University Law Review**, 771, 2019.

SCHLEEHAUF, Matthew. **The Strange Fruit of Semayne 's Case: No-Knock Warrants**. 2021. Disponível em <https://lawfully.usq.edu.au/tag/semaynes-case/#_ednref3> Acesso em: 12 de Mar. 2023.

SILVA, Luciana V. FINKELSTEIN, Maria E. A necessidade de regulação legislativa para utilização do serviço de computação em nuvem.

SONY, Reeta. SRI, Kan. BHUKYA, D. (2013). Data Protection and Cloud Computing: a Jurisdictional Aspect. Law. **Journal of the Higher school of economics**. Anual review, 2013. P. 81-91.

SUHR, Mario H. GROSS Rafael. A Personalização na Netflix: sistema de recomendação e interface. **XIII FATEC LOG**. Acesso em 3 de Mar. de 2023. Disponível em <https://fateclog.com.br/anais/2022/324-668-1-RV.pdf>.

TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil**: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

LYNN, Theo et al (ed.). **Data Privacy and Trust in Cloud Computing**: building trust in the cloud through assurance and accountability. Londres, Inglaterra: Palgrave Macmillan, 2020.

TURING, Dermot. **The story Of Computing**: from the Abacus to Artificial Intelligence. London: Ed. Arcturus Publishing Limited, 2018.

UNDHEIM, Astrid; BERNSMED, Karin; JAATUN, Martin Gilje. security in service level agreements for cloud computing. P**roceedings Of The 1St International Conference On Cloud Computing And Services Scienc**e, Trondheim,Norway, v. 1, n. 1, p. 636-642, 2011. SciTePress - Science and and Technology Publications. http://dx.doi.org/10.5220/0003391606360642.

UNCITRAL. **Notes On The Main Issues Of Cloud Computing Contracts: prepared by the secretariat of the United Nations Commission on International Trade Law**. Vienna International Centre: Uncitral Secretariat, 2019.

UNIÃO EUROPEIA. Diretiva n. 46, de 24 de outubro de 1995. **Directiva 95/46/CE do Parlamento Europeu e do Conselho**. Estrarburgo, França , 24 out. 1995. Disponível em:<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046&qid=1686862483642>. Acesso em: 3 dez. 2022.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 (General Data Protection Regulation). Disponível em: <https://gdprinfo.eu/pt-pt> Acesso em 25 de mar. 2022.

VASCONCELOS, Flávio Carvalho de; BRITO, Luiz Artur Ledur. Vantagem competitiva: o construto e a métrica. **Revista de Administração de Empresas**, [S.L.], v. 44, n. 2, p. 51-63, jun. 2004. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0034-75902004000200006.

VIEGAS, V. L. Teoria da harmonização jurídica: alguns esclarecimentos. **Novos Estudos Jurídicos**, Itajaí (SC), v. 9, n. 3, p. 617–656, 2008. DOI: 10.14210/nej.v9n3.p617-656. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/382. Acesso em: 19 Mai. 2023.

VIGGIANI, Tatiana S. VELLASCO Welton R. V. Aspectos Contratuais na Contratação de Nuvem. Disponível em: <http://publicadireito.com.br/artigos/?cod=04c0e78a0e5ff325>. Acesso em 12 Fev. de 2022.

WEBB, Amy. **The Big Nine**: how the tech titans and their thinking machines could warp humanity. Nova York - Ny: Publicaffairs, 2019. 336 p.

ZALAZAR, Ana Sofia et al. Un Modelo para Contratos de Cloud Computing. In: **argentine symposium on software engineering**, 14., 2013, Santa Fé. Artigo. Santa Fe, Argentina:

Ingar (Utn-Conicet), Avellaneda, 2013. p. 303-317. Disponível em: http://sedici.unlp.edu.ar/handle/10915/76711. Acesso em: 5 out. 2022.

ZUBOFF, Shoshana. **A era do Capitalismo de Vigilância**. Editora Intrínseca, 1ª edição. São Paulo. 2021.