UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO
CURSO DE BACHARELADO EM DIREITO

CLARA CORBAN BRITTO GUERRA

GENERAL DATA PROTECTION REGULATION X LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE COMPARATIVA DE ELEMENTOS FUNDAMENTAIS DAS ESTRUTURAS REGULATÓRIAS, DAS SANÇÕES PREVISTAS E PRINCIPAIS IMPACTOS DE ADEQUAÇÃO

CAMPINA GRANDE-PB
2020

CLARA CORBAN BRITTO GUERRA

GENERAL DATA PROTECTION REGULATION X LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE COMPARATIVA DE ELEMENTOS FUNDAMENTAIS DAS ESTRUTURAS REGULATÓRIAS, DAS SANÇÕES PREVISTAS E PRINCIPAIS IMPACTOS DE ADEQUAÇÃO

Trabalho de Conclusão de Curso apresentada à Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Direito e tecnologia.

Orientador: Prof. Dr. Cláudio Simão de Lucena Neto.

CAMPINA GRANDE
2020

G934g Guerra, Clara Corban Britto.

General Data Protection Regulation X Lei Geral de Proteção de Dados [manuscrito] : uma análise comparativa de elementos fundamentais das estruturas regulatórias, das sanções previstas e principais impactos de adequação / Clara Corban Britto Guerra. - 2020.

68 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2020.

"Orientação : Prof. Dr. Cláudio Simão de Lucena Neto , Departamento de Direito Privado - CCJ."

1. General Data Protection Regulation. 2. Lei Geral de Proteção de Dados. 3. Direito Comparado. I. Título

21. ed. CDD 342.02

Elaborada por Candice L. Brasileiro - CRB - 15/815 BSCCJ/UEPB

CLARA CORBAN BRITTO GUERRA

GENERAL DATA PROTECTION REGULATION X LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE COMPARATIVA DE ELEMENTOS FUNDAMENTAIS DAS ESTRUTURAS REGULATÓRIAS, DAS SANÇÕES PREVISTAS E PRINCIPAIS IMPACTOS DE ADEQUAÇÃO

Trabalho de Conclusão de Curso á Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Direito e Tecnologia.

Aprovada em: _7_/_12_/_2020_.

BANCA EXAMINADORA

Prof. Dr. Cláudio Simão de Lucena Neto (Orientador)
Universidade Estadual da Paraíba (UEPB)

Profa. Dra. Cynara de Barros Costa
Universidade Estadual da Paraíba (UEPB)

Profa. Dra. Ana Paula M. Canto de Lima
Escola Superior de Advocacia (ESA/PE)

AGRADECIMENTOS

2020 foi um ano difícil para toda a humanidade. Mas, como muitas situações adversas na vida, ele nos trouxe aprendizados. Neste ano, aprendi a ter resiliência para me reerguer e me reinventar diante das dificuldades.Também aprendi a valorizar ainda mais as pessoas que estão ao meu lado e me ajudam a crescer.

Por fim, mas não menos importante, aprendi a valorizar as pequenas conquistas. Pois, através delas alcançamos os maiores objetivos. Ao olhar para meu processo de construção deste trabalho, lembro das pessoas que me ajudaram a chegar até aqui. Diante disso, quero agradecer:

À Lemuel Guerra, meu querido tio que me acolheu, apoiou e proporcionou muitos momentos divertidos durante todos esses anos de graduação em Campina Grande.

Aos meus pais por todo o apoio e amor que deles tive durante toda a minha jornada, não só acadêmica, mas também de vida. E por terem me ensinado a importância de lutar por um mundo melhor e a olhar empaticamente para o próximo.

Às minhas irmãs, por terem sido um exemplo de busca por conhecimento e amor para mim.

Em especial, quero agradecer a minha irmã Clarissa, por todo o seu apoio em todos momentos que precisei, inclusive durante a construção desse texto.

À meu companheiro Dales. Por não ter me deixado desistir mesmo nos momentos mais difíceis e por acreditar que eu conseguiria chegar até o fim deste trabalho. E claro, por todos os lanches por ele fornecidos.

Às minhas queridas amigas de curso: Larah Diniz, Brunna Leite e Deborah Lourenço por terem tornado meus dias no CCJ mais leves, partilhando comigo a jornada da graduação durante todos esses cinco anos, com muito acolhimento nos momentos difíceis e com entusiasmo nos instantes mais felizes.

Quero agradecer ao meu orientador Dr. Cláudio Simão. Não só pelo seu apoio, como também pelo aprendizado adquirido durante o processo de orientação, mas principalmente por ter despertado meu interesse pelo Direito digital, durante a disciplina que tive oportunidade de ser sua aluna.

Por fim, gostaria de agradecer aos funcionários do Centro de Ciências Jurídicas e também da UEPB. Toda a equipe de professores com os quais tive oportunidade de aprender sobre as ferramentas jurídicas, mas também aos servidores, aos funcionários da limpeza, coordenadores e secretários que possibilitam ao CCJ funcionar e formar juristas competentes.

RESUMO

O presente trabalho tem como objetivo central analisar alguns dos elementos principais da Lei Geral de Proteção de Dados (LGPD - Brasil, Nº 13.709), em comparação com o *General Data Protection Regulation* (GDPR – EU, 2016/679). A metodologia proposta consiste em uma análise comparativa dos documentos nos quais as regulações acima citadas estão estabelecidas, investigando suas semelhanças e suas diferenças e observando os principais impactos do *General Data Protection Regulation* (GDPR – EU, 2016/679), que está em vigência desde março de 2018 até agora (dois anos). No primeiro momento será apresentada a relevância das tecnologias computacionais na sociedade ocidental nos dias de hoje. Em seguida, serão descritos os caminhos da privacidade na legislação brasileira até o advento da Lei Geral de Proteção de Dados Pessoais (LGPD - Brasil, Nº 13.709). Também serão observados os artigos das normas (brasileira e europeia) que tratam das sanções aplicáveis às infrações cometidas pelos agentes que lidam com o tratamento e armazenamento de dados pessoais. E por fim, um dos principais objetivos do trabalho será; a partir do estudo comparado das normas supracitadas e da análise dos impactos trazidos pelo *General Data Protection Regulation* (GDPR – EU, 2016/679) nos seus dois anos de vigência, traçar as expectativas sobre a aplicabilidade da Lei Geral de Proteção de Dados (LGPD - Brasil, Nº 13.709).

Palavras-Chave: Proteção de Dados. Privacidade. Sanções. Direito Comparado.

ABSTRACT

The main objective of this work is to analyze some of the main elements of the General Data Protection Law (LGPD - Brasil, Nº 13.709), in comparison with the General Data Protection Regulation (GDPR - EU, 2016/679). The proposed methodology consists of a comparative analysis of the documents in which the regulations mentioned above are established, investigating their similarities and differences and observing the main impacts of the General Data Protection Regulation (GDPR - EU, 2016/679), which has been in force since March 2018 so far (two years). In the first moment, the relevance of computational technologies in occidental society will be presented today. Then, the paths of privacy in Brazilian legislation will be described until the advent of the General Law for the Protection of Personal Data (LGPD - Brasil, Nº 13.709). The articles of the norms (Brazilian and European) that deal with the sanctions applicable to the infractions committed by the agents that deal with the treatment and storage of personal data will also be observed. And finally, one of the main objectives of the work will be, from the comparative study of the aforementioned norms and the analysis of the impacts brought by the General Data Protection Regulation (GDPR - EU, 2016/679) in its two years of effectiveness, to outline the expectations on the applicability of the General Data Protection Law (LGPD - Brasil, Nº 13.709).

Keywords: Data Protection. Privacy. Sanctions. Comparative Law.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados.
DPA’s	Data Protection Authorities.
UE	União Europeia.
GDPR	General Data Protection Regulation.
LGPD	Lei Geral de Proteção de Dados Pessoais.

LISTA DE SÍMBOLOS

% Porcentagem

€ Euro

§ Seção

SUMÁRIO

.

INTRODUÇÃO

É indiscutível o fato de que a sociedade atual é permeada pelos avanços das tecnologias digitais nas mais diversas áreas. Desde a criação e popularização dos computadores, a maneira de lidar com a informação tem se transformado constantemente. Antes, arquivos e informações eram guardados de maneira física, ocupavam bastante espaço e eram de difícil manuseio. Com a capacidade de armazenamento dos computadores, houve um aumento, tanto na quantidade, quanto na acessibilidade e manuseio dos arquivos. Sendo assim, passou-se a armazenar mais e de maneira otimizada.

O presente trabalho busca explorar o papel da legislação sobre privacidade no presente cenário, no qual a popularização da *internet* e dos meios computacionais se tornou um ponto central nas sociedades contemporâneas. A partir da revisão da literatura sobre legislações referidas à proteção de dados, pretendemos comparar as semelhanças e diferenças entre a *General Data Protection Regulation* (UNIÃO EUROPEIA 2016/679), da União Europeia e a Legislação de Proteção de Dados do Brasil (Lei Nº 13.709/ 2018). O presente estudo tem como objetivo analisar o texto das duas legislações (GDPR e LGPD), focalizando mais especificamente nas sanções nelas previstas para os agentes responsáveis pelo tratamento que não cumpram as normas estabelecidas.

A LGPD, depois de muitos adiamentos e divergências sobre sua entrada em vigor, passou a vigorar de maneira escalonada: em 28 de dezembro de 2018, quanto aos arts. que tratam da constituição da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD). E no ano de 2020, os demais artigos da Lei, com exceção dos dispositivos que tratam da aplicação de sanções administrativas, que ficaram previstos para agosto de 2021. Tendo em vista os tempos de vigência dos dois marcos regulatórios, faremos a análise dos principais impactos do primeiro ano da GPDR, para assim, traçar expectativas sobre a LGPD.

O texto da presente monografia se organiza da seguinte maneira: no capítulo 1 discutimos a crescente importância da *internet* e da produção, arquivamento e circulação dos dados nas atuais sociedades marcadas pela hiperconectividade. No

capítulo dois é dado foco a economia digital e os desafios da proteção à privacidade. No capítulo 3, é desenvolvido os cenários a partir dos quais emergem o GDPR e a LPGD e no capítulo seguinte finalmente apresentamos uma comparação dos dois marcos regulatórios. Na sequência, são apresentadas as considerações finais e as referências usadas no texto.

2 A IMPORTÂNCIA DA *INTERNET* E DOS DADOS NA SOCIEDADE DA HIPERCONECTIVIDADE

Neste capítulo será discutida a crescente importância das inovações computacionais e da presença da conexão com a *internet* vivida nos últimos 20 (vinte) anos pela sociedade globalizada na qual nos encontramos. introduzindo o conceito de hiperconectividade, que representa a realidade cotidiana dos indivíduos conectados diariamente a dispositivos eletrônicos.E finalmente, o conceito de dados pessoais e de *Big Data*.

As tecnologias eletrônicas e as inovações computacionais atravessam a vida do indivíduo na sociedade contemporânea globalizada. Há inúmeros aplicativos e *softwares* para as mais diversas atividades do cotidiano. De acordo com dados do IBGE (2018), no Brasil a internet já era utilizada em 79,1% dos domicílios brasileiros. Da população com mais de dez anos de idade 79,3% possuíam telefone móvel celular para uso pessoal, e em 99,2% dos domicílios nos quais havia acesso a *internet*, era através do mesmo aparelho móvel que se fazia o acesso à rede. Esses dados indicam o quanto a *internet* e os *smartphones* conectados a ela estão presentes no cotidiano dos indivíduos. Esses aparelhos são utilizados especialmente para a comunicação através das diversas redes sociais, mas também são usados para ouvir música, lembrar de compromissos importantes, fazer compras, trabalhar, estudar *etc* (BRASIL, 2018).

As diversas *telas* que possibilitam a conexão com a *internet* e o uso desta para os mais distintos fins, geraram mudanças relevantes não só na comunicação, como também na socialização dos indivíduos. Greenwald (2014, p.12) comenta existir “uma dimensão genuinamente nova”:

> [...]o papel desempenhado hoje pela *internet* na vida cotidiana das pessoas, e sobretudo para as gerações mais jovens, a grande rede não é um universo isolado, separado, no qual são realizadas algumas das funções da vida. A *internet* não é apenas nosso correio e nosso telefone. Ela é a totalidade do nosso mundo, o lugar onde quase tudo acontece. É lá que se fazem amigos, se escolhem livros e filmes, se organiza o ativismo político, e é lá que são criados e armazenados os dados mais particulares de cada um. É na *internet* que desenvolvemos e expressamos nossa personalidade e individualidade (GREENWALD, 2014, p. 12).

Além da mudança do modo de conviver e se relacionar em sociedade, a revolução digital que a contemporaneidade vivencia é notadamente marcada pela formação de conexão entre as pessoas, pessoas e coisas e até coisas e coisas (NASCIMENTO, 2015, *apud* CANTO *et al*., 2019, p. 31).

Não são só as novas formas de trabalho ou comunicação possibilitadas pela conexão com a *internet* que constituem a novidade da revolução digital, mas também, nas palavras de Canto *et al.* (2019, p. 31):

> Além da profunda mudança de sociabilidade, uma das grandes características desta nova dinâmica reside numa crescente participação de agentes não humanos nas mais variadas atividades do cotidiano: máquinas, sensores, Algoritmos e dispositivos conectados à *Internet* assumem o protagonismo das cadeias relacionais, exercendo funções cada vez mais relevantes na vida em coletividade.

Esse fenômeno, nomeado por Canto *et al* (*idem*) como hiperconectividade, é responsável pela geração de uma quantidade astronômica de dados pessoais. Magrani (2018, p. 20) define o termo supracitado da seguinte forma:

> O termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento. Esse termo possui alguns desdobramentos importantes. Podemos citar alguns deles: o conceito de *always-on*, estado em que as pessoas estão conectadas a todo o momento; a possibilidade de estar prontamente acessível *(readily accessible*); a riqueza de informações; a interatividade; e o armazenamento ininterrupto de dados (*always recording*). O termo hiperconectividade encontra-se hoje atrelado às comunicações entre indivíduos (*person-to-person, P2P*), indivíduos e máquina (*human-to-machine, H2M*) e entre máquinas *(machine-to-machine, M2M*) valendo-se, para tanto, de diferentes meios de comunicação. Há, neste contexto, um fluxo contínuo de informações e uma massiva produção de dados.

Como consequência do fenômeno da hiperconectividade, além de informações sobre o titular (nome, endereço, idade), outros dados são coletados através de diversas fontes. Num contexto no qual as pessoas estão sempre conectadas (*always-on*), os algoritmos presentes nos *softwares* e aplicativos,

coletam dados quase que a todo instante, quer seja nas comunicações entre os indivíduos, entre pessoas e máquinas e até mesmo máquinas e máquinas (*machine-to-machine*). Os *softwares* de levantamento de dados relativos ao uso da *internet* revelam sobre os usuários informações corriqueiras como: as músicas que mais escutam; quais os caminhos que o usuário do aplicativo prefere tomar para chegar aos lugares; que produtos têm interesse em comprar; preferências políticas; estéticas; orientação sexual; comportamento de consumo; dentre outras informações mais diversas que, juntas, podem traçar um perfil capaz da pessoa que fica diante das telas. Cabe aqui destacar a diferença entre dados e informações, que, apesar de serem conceitos entrelaçados e similares, são distintos.

> Dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável (...). Dados são os fatos brutos que quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação. (PADILHA & GARNIER, 2019 *apud* BIONI 2019, p. 59)

De acordo com o Art. 5º da LGPD (Lei Nº 13.709/2018) considera-se como dados pessoais toda informação relacionada à pessoa natural identificada ou identificável, dividindo-os em duas categorias: dados pessoais sensíveis e anonimizados (BRASIL, 2018).

Pohlmann (2019), define dado como: “qualquer informação relacionada a uma pessoa natural”. E em seguida explica o que caracteriza um dado pessoal sensível e um dado pessoal anonimizado, respectivamente:

> Dado pessoal que possa relacionar uma pessoa natural com algum tipo de associação, movimento, sindicato, partido político, ou questões de ordem étnica, religiosas, políticas, filosóficas, vida sexual etc. Estão incluídos nesta categoria, todos os dados médicos, biométricos e genéticos. [...] Podemos considerar que um dado sensível é aquele dado que pode gerar, em algum âmbito, a discriminação ou o preconceito por parte de outras pessoas (POHLMANN, 2019, p. 25).

O dado anonimizado, por sua vez, é por ele definido como:

> Dado pessoal pertencente a uma pessoa natural, mas que não possa ser identificado ou relacionado com a mesma, considerando a utilização dos meios técnicos razoáveis e disponíveis na ocasião do seu tratamento. (POHLMANN, 2019, p.26)

Todas as informações que se encaixam nas definições supracitadas são consideradas fatos brutos, que apenas quando analisados e tratados se constituem em dados. Para Silva (2007 *apud* REZENDE, 2015, p. 37):

> Dados são códigos que constituem a matéria prima da informação, ou seja, é a informação não tratada que ainda não apresenta relevância. Eles representam um ou mais significados de um sistema que isoladamente não pode transmitir uma mensagem ou representar algum conhecimento**.**

Para que se tornem dados, os códigos precisam ser estruturadas e organizadas (REZENDE, 2015). Só através do tratamento adequado é que eles podem se transformar em um minucioso conhecimento sobre determinado indivíduo, grupo, produto ou serviço, tornando-se uma ferramenta de conhecimento com valor de uso e de troca.

Como vimos acima, fica evidente a quantidade extensa de dados que os seres humanos contextualizados na era digital vivida hoje produzem. O que originou a expressão *Big Data* para nomear uma tecnologia capaz de processar uma grande quantidade de dados, como explica Bioni (2019, p. 34):

> Pesquisando assuntos *online*, acessando sites, aplicativos etc. Diante da produção gigantesca de dados a cada minuto, através da tecnologia denominada *Big Data* é possível que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades.

Segundo Doug (2012), os *Big Data* podem ser relacionados ao volume, à velocidade e à variedade, caracterizando uma situação em que excedem a capacidade das tecnologias "tradicionais" de processamento de dados, conseguindo ser organizados em quantidades antes inimagináveis - dos *bits* aos *yottabytes*[1]- e em diversos formatos - *e.g.*,textos, fotos, *etc*. Tudo isso em alta velocidade.

É evidente que antes mesmo da emergência da rede internacional de computadores, as pessoas já produziam dados. Porém, com o *Big Data,* a capacidade de processamento adquirida atualmente faz com que as informações

[1] Segundo Hamann (2011, *n. p*) "Bit vem de Binary digiT, ou seja, dígitos binários. Isso porque cada bit é exatamente isto: um dígito binário que pode corresponder aos valores "0" ou "1". O conjunto deles forma os dados na forma que nós conseguimos compreender. Unidade primária do processamento de dados dos computadores. Yottabytes representa um trilhão de terabytes ou um quadrilhão de gigabytes: não é possível (pelo menos por enquanto) atingir essa quantia. Disponível em: (https://www.tecmundo.com.br/infografico/10187-do-bit-ao-yottabyte-conheca-os-tamanhos-dos-arquivos-digitais-infografico-.htm).

pessoais coletadas em grande escala se tornem potenciais dados valiosos em termos mercadológicos, sociais e políticos.

O processamento desses dados tomou proporções inesperadas, como aponta Nascimento (2017, n.p.):

> Antes de existir qualquer meio digital e/ou tecnologias computacionais, os dados já eram gerados. A diferença é que nos dias de hoje geramos muito mais dados com dispositivos como celular e TVs. Além disso, temos as mídias sociais que geram a todo tempo informações majoritariamente públicas. Hoje já é realidade a existência de carros, geladeiras e dispositivos vestíveis (*wearable devices*) conectados entre si e gerando ainda mais dados para serem processados e transformados em informações úteis.

Ainda para Nascimento (2017), "o *Big Data* está atrelado à possibilidade e oportunidade de cruzar dados por meio de diversas fontes para obtermos *insights* rápidos e preciosos".

Na atual era da hiperconectividade, com a ajuda de ferramentas como o *Big data*, a captação e o tratamento de informações pessoais tomou uma proporção muito maior na quantidade e na sua importância mercadológica e política. Com a utilização do *Big Data,*

> [...] há um salto quanto ao volume de dados processados, tornando-se possível relacionar uma série de fatos(dados), estabelecendo-se padrões e, por conseguinte, inferir inclusive, probabilidades de acontecimentos futuros (BIONI,2019, p. 35).

Chul-Han (2018) aponta como o advento da ferramenta *Big Data* se relaciona com o conceito arquitetônico de *Panopticon*, apresentado por Bentham e comentado na obra de Foucault, *Vigiar e Punir* (1987). Tal conceito, se refere à emergência de uma subjetividade vigiada, em um estilo semelhante ao *Panopticon*, forma arquitetônica prisional através da qual os presos podiam ser constantemente observados, descrita por Foucault (1987, p. 223) nos seguintes termos:

> O Panóptico de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia uma construção em anel; no centro, uma torre; esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas

> da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode-se perceber da torre, recortando-se exatamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia. Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível. O dispositivo panóptico organiza unidades espaciais que permitem ver sem parar e reconhecer imediatamente. Em suma, o princípio da masmorra é invertido; ou antes, de suas três funções — trancar, privar de luz e esconder — só se conserva a primeira e suprimem-se as outras duas. A plena luz e o olhar de um vigia captam melhor que a sombra, que finalmente protegia. A visibilidade é uma armadilha.

Para Chul-Han (2018), o *Big Data* se aproxima da estrutura do *Panopticon,* porque há uma vigilância constante sobre os indivíduos conectados aos dispositivos eletrônicos, através da qual todos os seus passos, ações e até desejos são coletados através da imensa quantidade de dados gerados pela própria pessoa e sua inserção social, “oferecendo uma visão em 360º dos seus internos”. Em suas palavras:

> Os *Big Data* tornam possível uma nova forma de controle muito eficiente. “oferecemos uma visão 360º dos seus clientes” é o *slogan* da empresa digital que oferece uma visão 360º dos seus internos. O Panóptico de Betham está ligado a óptica perspectivista. Deste modo, são inevitáveis pontos cegos nos quais os prisioneiros podem perseguir seus pensamentos e desejos secretos sem serem notados. [...] A vigilância digital é mais eficiente porque é aperspectivística. Ela é livre de limitações perspectivistas que são características da óptica analógica. A óptica digital possibilita a vigilância a partir de qualquer ângulo. Assim, elimina pontos cegos. Em contraste a óptica analógica e perspectiva, a óptica digital pode explicar até a psique (CHUL-HAN, 2018, p.85).

Através do trecho acima é possível entender a analogia entre a estrutura do *panopticon* e as informações possibilitadas pelo *Big Data*. Para Chul-Han, a óptica digital pode explicar até a psiquê, permitindo aos que acessam os dados fruto da análise em grande escala de detalhes considerados corriqueiros. Podendo-se traçar o perfil do titular dos dados e através disso, descobrir, antes mesmo dele, o que o mesmo deseja consumir e com quais tendências políticas têm afinidades potenciais, dentre outras aplicações.

Pelo o até agora discutido é possível perceber o poder dos dados e de suas potencialidades na era da hiperconectividade, que instaura uma sociedade na qual não há pontos cegos, sendo as informações pessoais diuturnamente coletadas, processadas, compartilhadas, tratadas e armazenadas em bancos de dados, podendo ser utilizados para fins muito específicos, de maneira precisa e otimizada.

Essa conjuntura demanda do Direito uma reação, de modo a estabelecer limites e mecanismo de defesas de indivíduos e grupos, os quais possibilitem a salvaguarda de direitos em relação à privacidade. Os regulamentos aqui comparados são exemplos do que tem sido produzido pelas nações nesse sentido.

3 ECONOMIA DIGITAL E AS NOVAS RELAÇÕES DE NEGÓCIOS: DESAFIOS DA PRIVACIDADE NA ERA DO EXCESSO A INFORMAÇÃO

As mudanças trazidas pelas inovações computacionais e eletrônicas em curso tem indubitavelmente impactado o modo de vida humano como um todo, não só as relações pessoais. Neste segundo capítulo iremos tratar do impacto do usos dos dados digitais nas atividades econômicas em suas diversas escalas – produção, circulação e consumo –, nesse contexto, elas têm atravessado modificações significativas.

O *e-commerce*, uma das principais novidades desse novo sistema, e também toda a logística *offline* das empresas foram afetados pelas tecnologias e pela conexão disponibilizada pela *internet*. Sobre esse ponto, Castels (2003, p. 68) afirma que:

> A *Internet* está transformando a prática das empresas em sua relação com fornecedores e compradores, em sua administração, em seu processo de produção e em sua cooperação com outras firmas, em seu financiamento e na avaliação de ações em mercados financeiros. Os usos adequados da Internet tornaram-se uma fonte decisiva de produtividade e competitividade para negócios de todo tipo.

Não só a maneira de administrar ou os meios para comercializar produtos e serviços mudaram. Hoje é possível com uma simples pesquisa numa ferramenta de busca *online,* como o *Google,* comparar as melhores ofertas, e**,** com um simples cadastro, após um clique no aplicativo ou *web site* comprar o que se deseja. Mas, além da facilidade e variedade na hora de adquirir produtos, as relações de consumo, mercado e o papel do consumidor também se transformaram.

Para Bioni (2019, p. 12) “o consumidor saiu do lugar passivo no ciclo do consumo e passou a atuar como um assistente de vendas sem custos”, na medida que, diante da inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo, através do *marketing* e sua promoção via publicidade, os dados pessoais do titular assumiram papel vital na engrenagem da economia da informação (BIONI, *idem*).

A capacidade de processamento das informações coletadas pelo *Big Data faz* com que os dados dos consumidores sejam considerados valiosos na economia

digital. Através dos dados pessoais coletados e tratados dos usuários é possível formular o perfil dos indivíduos/consumidores e aplicar a publicidade direcionada, monetizando-os de maneira eficaz. Ainda nas palavras de Bioni (2019, p. 18):

> [...] As redes sociais acumulam os mais diversos dados pessoais dos seus *usuários*, que são extraídos ao longo de toda a sua interação com a aplicação. Uma vez logado, o usuário passa a fornecer um rico perfil de si, que é o que viabiliza o direcionamento da publicidade.

O usuário acredita ter o poder de escolha sob os conteúdos que consome nas redes sociais. Porém, na verdade, tudo que passa pela sua *timeline*[2] é previamente arquitetado pelos algoritmos alimentados através dos dados pessoais coletados, fornecidos pelo próprio titular, ao aceitar os termos de uso do *website*.

Casarotto (2019) define a publicidade como a "estratégia de *marketing* que envolve a compra de espaço em um veículo de mídia para divulgar um produto, serviço ou marca, com o objetivo de atingir o público-alvo da empresa e incentivá-lo a comprar". Ela pode ser entendida como a comunicação estabelecida entre o fornecedor e o consumidor. Antes, era muito comum que os anúncios dos produtos e serviços fossem feitos em veículos de comunicação em massa como jornais, revistas e a televisão. O objetivo da propaganda era atingir o máximo de pessoas possíveis e consequentemente, acabar chamando a atenção do seu consumidor almejado.

Os avanços nos estudos da ciência mercadológica perceberam a ineficácia desse método se comparado à abordagem mais direta que os dados proporcionam. Sobre isso, a *Reamp Academy* comenta:

> No período da década de 80, os anúncios tornaram-se cada vez mais segmentados, inclusive no Brasil, onde o mercado editorial passou por grandes mudanças. Só então, a partir dos anos 90, pudemos presenciar o surgimento da internet e da publicidade online, que vem evoluindo até os dias de hoje e se adaptando às novas tecnologias disponíveis (REAMP ACADEMY, 2017).

---

[2] *Timeline* é um termo em inglês que significa "linha do tempo". Na *Internet*, essa expressão passou a ser muito usada por causa das redes sociais, como Facebook, Instagram e Twitter. Nas redes sociais, a *Timeline* é o modelo utilizado para apresentar as postagens feitas por seus usuários (*Cf.* STEIN, Dicionário Popular, disponível em: (https://www.dicionariopopular.com/timeline).

Com a popularização da *internet*, e com a tendência de anúncios em veículos cada vez mais segmentados, nasce a publicidade direcionada/segmentada *online*. Vejamos como Braimis (2019) comenta sobre esse novo tipo de publicidade:

> Essa segmentação leva em consideração interesses previamente demonstrados pelo público-alvo, em que persona esse público se encaixa e outros comportamentos do grupo. Em vez de desperdiçar força de trabalho, tempo e dinheiro espalhando propagandas muitas vezes ineficazes por todos os cantos, foca em uma relação mais organizada de oferta e demanda, em busca do melhor resultado.

A publicidade direcionada/segmentada online tem como sua principal fonte os dados pessoais fornecidos pelos usuários de *websites* e aplicativos. Sendo assim, o consumidor, mesmo que passivamente, toma um papel fundamental para que a monetização dos seus dados seja realizada, uma vez que os fornece por livre e espontânea vontade.

Torres (2018) cita uma metáfora usada por Lee e Sachi LeFever (2016), denominada de ‘sorvete social’, para explicar o atual processo de transformação do consumidor e a importância da publicidade direcionada. *Scootville* era o nome da cidade na qual a empresa *Big Ice Cream* tinha uma fábrica que produzia seu sorvete havia mais de vinte anos. A referida empresa monopolizou o mercado de sorvetes por muito tempo com três sabores que eram o carro chefe das vendas: baunilha, morango e chocolate. Esse monopólio durou até que uma nova máquina chegou à cidade e fez com que qualquer um pudesse fazer com ela os seus próprios sorvetes a custo competitivo. Logo, várias pessoas da cidade começaram a fazer sorvete dos mais diversos sabores, e a vendê-los com um custo muito razoável.

A cidade que era famosa pelo sorvete da fábrica *Big Ice Cream*, ficou ainda mais conhecida, mas pela diversidade e quantidade de sorvete que era produzida e vendida pelos cidadãos de *Scootville*. Porém, diante de tanta diversidade, as pessoas que visitavam a cidade

passaram a considerar um problema escolher que sabores experimentar e onde comprá-los. Então**,** um dos vendedores de sorvete resolveu adotar um sistema no qual era deixado um painel com todos os sabores disponíveis na loja, no qual os clientes poderiam deixar suas avaliações e comentários pessoais sobre cada sabor experimentado. O sistema acabou se espalhando nas demais lojas.

De acordo com Torres (*idem*, p. 24) concluiu-se com a estória supracitada que:

> No final, algumas coisas ficam claras: os sorvetes melhoraram, por que os fabricantes aprendiam diretamente dos seus clientes; as opiniões nos painéis permitiam que os consumidores encontrassem exatamente os sorvetes desejados. A combinação da nova tecnologia com a nova maneira de se relacionar com as pessoas e os consumidores tornou *Scootvile* uma cidade única. A história da cidade de *Scootvile* ilustra bem o que ocorreu com a *internet*. Novas tecnologias e aplicações, como os *blogs*, as ferramentas de busca, os fóruns, as redes sociais e tantas outras aplicações online foram utilizadas pelos internautas para, literalmente, assumir o controle, a produção e o consumo da informação, atividades antes restritas aos grandes portais e as empresas (TORRES, 2018, p. 24).

Em síntese, é fundamental o papel do consumidor para a empresa quando ele fornece e propaga informações sobre os produtos consumidos. A informação facilitada pela hiperconectividade não só faz com que o usuário possa expressar sua opinião, mas também, através da coleta dos dados pessoais que produz e disponibiliza, torna possível ao fornecedor, direcionar o serviço ou produto tanto na publicidade, na produção do seu estoque e na sua qualidade. Ficando evidente a importância do consumidor, titular dos dados pessoais, para a economia na era digital.

3.1 Como os dados pessoais são monetizados: tipos de negócio na *internet*

Utilizar serviços de *websites* e aplicativos para *smartphones,* na maioria dos casos não impõe a necessidade de pagamento pecuniário, sendo as ferramentas *on line*, majoritariamente, gratuitas. Bioni (2020) aponta em sua obra como são raros os serviços e produtos *on line* nos quais se faz necessária a contraprestação monetária direta:

> Na tela dos computadores prevalece o acesso livre às redes sociais, *e-mails,* mecanismos de busca, *softwares,* portais de notícias e aos mais diversos aplicativos para *smartphones.* Raros são os serviços ou produtos em que *é* necessário despender alguma quantia de dinheiro, a título de contraprestação, para o seu download e/ou acesso (BIONI, 2020, p.22).

Esse autor questiona como esses modelos tão presentes no mercado atual podem ser lucrativos e aponta como resposta a inserção dos dados pessoais na economia da informação e como vetor central da publicidade comportamental.

No modelo de negócios tradicional, consumidores trocam uma quantia pecuniária certa e predefinida por um bem de consumo. Por exemplo, no supermercado, cada item que vai no carrinho tem o preço exato a ser pago para a sua aquisição, existindo uma relação bilateral entre consumidor e fornecedor. Já no novo modelo de negócios, nas exatas palavras de Bioni (2019, p. 22):

> Consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada. São os anunciantes de conteúdo publicitário que aperfeiçoam o seu arranjo econômico. Desta forma, tal relação torna-se plurilateral, uma vez que ela envolve, necessariamente, os anunciantes de conteúdo publicitário para haver retorno financeiro nesse modelo de negócio. Por essa lógica, o consumidor torna-se também um produto comercializável, já que seus dados integram a operação econômica em questão.

No trecho supracitado podemos verificar a mudança de paradigma da relação de consumo que a *internet* gerou. Antes, havia dois agentes diretamente ligados à operação financeira, o consumidor e o fornecedor. Nos negócios online, que são ditos "gratuitos" ao consumidor (*Youtube*, *e-mail, Google*), a prestação pecuniária trata-se de um modelo de negócios que é financiado e suportado pela publicidade direcionada. Como Bioni (2019, p. 23) ainda explica : "em um primeiro momento, atrai-se o usuário para que ele usufrua de um serviço e/ou produto para, em um segundo momento, coletar seus dados pessoais e, então viabilizar o direcionamento da mensagem publicitária, que é sua fonte de rentabilização".

Sobre o mesmo tema, afirma Tatang et al. (2020, n.p, tradução minha[3]):

> A publicidade continua sendo uma das principais fontes de receita para muitos sites, aplicativos e serviços online. Muitos modelos de negócios dependem de anúncios e serviços analíticos para personalizar seus produtos e poder oferecê-los "gratuitamente". Para direcionar individualmente os visitantes da

[3] Texto original: Advertising remains one of the main sources of income for many websites, apps, and online services. Many business models rely on ads and analytics services to personalize their products and to be able to offer them "for free". To individually target web site visitors with ads, tracking services gather personal data, mostly without users 'explicit consent . Personalized ads are based where collected by ad companies about Internet users through various mechanisms, mainly HTTP cookies . The gathered data is often seen as an economic asset of a company.

> web com anúncios, os serviços de rastreamento reúnem dados pessoais, principalmente sem o consentimento explícito dos usuários. Anúncios personalizados são baseados em dados coletados por empresas de publicidade sobre usuários de Internet por meio de vários mecanismos, principalmente cookies HTTP. Os dados coletados são frequentemente vistos como um ativo econômico de uma empresa.

Bioni (2019) aponta o "*zero-price advertisement business model"*[4] para resumir esse processo ele explica haver uma troca na qual os dados pessoais do usuário, de certa forma, paga pelos serviços ou produtos. Sendo assim, a monetização dos dados pessoais acontece, deixando claro que há contraprestação monetária, mesmo que de forma indireta, no uso de serviços e produtos *online.* Ela se dá através do fornecimento dos dados pessoais do usuário para fins de abastecimento dos bancos de dados, que buscam refinar cada vez mais a publicidade direcionada. Nas palavras de Ramos (2019, n.p): "a publicidade baseada em dados sustenta a ideia de uma internet em que o acesso a conteúdo é o mais aberto, livre e democrático possível". Sem dados de acesso liberado, vários serviços seriam pagos e a publicidade não seria tão personalizada e relevante para os usuários.

Mesmo as plataformas de negócios que impõem uma contraprestação pecuniária direta, também usam, em parte, a lógica da gratuidade. Para Bioni, são os chamados modelos de negócio *Freemium*. Nas suas palavras:

> *Freemium* é a combinação de gratuito (*free*) com o diferenciado (*premium)*. Nesses modelos de negócios, permite-se o acesso livre e "gratuito" a um determinado tipo de serviço on-line, mas em sua versão limitada ou básica. Para que se tenha acesso a versão completa de um software ou a íntegra de um portal de notícias - versão *premium* - é necessário contraprestação pecuniária direta - a versão "paga" (BIONI, 2019, p. 24).

É o mesmo produto ou serviço, porém maneiras de monetização diferentes. No entanto, mesmo pagando pela versão *premium* o usuário não deixará de fornecer seus dados pessoais, sendo a mesma a política de privacidade para os indivíduos que usam o *prime* e o *freemium*.

[4] Modelo de negócios de publicidade a preço zero.

É possível concluir que mesmo com a contraprestação pecuniária direta, os dados pessoais ainda assumem um papel importantíssimo para o negócio *online*, pois, podem ser uma fonte a mais de monetização. Através da publicidade direcionada também é possível otimizar o desempenho dos negócios *online*, traçando um perfil cada vez mais refinado do consumidor, investindo nos produtos e serviços que mais agradam e geram rentabilidade.

4 MARCOS REGULATÓRIOS DA PROTEÇÃO DE DADOS DIGITAIS – OS CAMINHOS DAS NORMAS ADOTADAS PELA UNIÃO EUROPEIA (GDPR) E PELO BRASIL (LGPD)

Um dos registros pioneiros da ótica do Direito sobre a importância da privacidade para ser humano moderno, ocorre em um artigo publicado por Louis D. Brandeis e Samuel D. Warren, em 1890, intitulado *The Right to Privacy* (O direito à privacidade). Neste artigo, a necessidade que o indivíduo tem à vida privada é ressaltada na máxima marcante que define a privacidade como o direito de estar só[5]. Para além disso, os autores também apontam a importância da mutabilidade do Direito, que deve corresponder às demandas da sociedade e do tempo, sob pena de não servir à sociedade:

> 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 tornaram-se mais essenciais para o indivíduo (BRANDEIS & WARREN, 1890, p. 5, tradução minha).[6]

O texto de Brandeis e Warren foi motivado pelo vazamento de informações íntimas referentes ao casamento da filha de um dos autores (DONEDA, 2000 *apud* CANCELIER, 2017, p. 2), levando-os a construir a doutrina do ‘direito à privacidade’.

Respondendo às demandas da realidade daquela época, essa doutrina refletiu os interesses e características da burguesia estadunidense do século XIX, e o período de inovações tecnológicas pelo qual passava a sociedade americana, no qual se destaca a invenção da fotografia instantânea e do telefone (DONEDA, 2000 *apud* CANCELIER, 2017, p. 2).

O direito à privacidade se democratizou apenas na década de 1960, período em que se estendeu para além das camadas da burguesia, graças também à “capacidade técnica de cada vez mais recolher, processar e utilizar a informação” (DONEDA, 2000 *apud* CANCELIER, 2017 p. 12), possibilitada pelo desenvolvimento dos veículos de informação nesse período.

---

[5] Termo de autoria do Presidente da Suprema Corte de Michigan, quem cunhou, em 1888, a expressão o direito de estar só (the right to be let alone).

[6] Texto original: The intensity and complexity of life, attendant upon advancing civilizacion, have rendered necessary some retreat from the world, and the man, under the refining influence of culture has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual.

4. 1 A consolidação do General Data Protection Regulation (UNIÃO EUROPÉIA, 2016/679)

Foi na década de 1980 que o Conselho da Europa se reuniu, na nomeada Convenção 108, em *Strasbourg*, para aprovar a norma que, no seu preâmbulo, se definiu como o:

> [...] primeiro instrumento internacional vinculativo que protege o indivíduo contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais e que visa regular ao mesmo tempo o fluxo transfronteiriço de dados pessoais (TREATY No.108, 1981).

Duas décadas mais tarde, é consolidada a Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC) pela União Europeia, na qual se manteve à correlação definida pela Convenção 108 supracitada entre o livre fluxo informacional e a proteção dos dados pessoais. A referida diretiva teve o objetivo de "traduzir, em normas mais específicas, a promessa antes firmada na Convenção de *Strasbourg* de assegurar aos indivíduos o controle sobre suas informações pessoais" (BIONI, 2019, p. 117), adjetivando o consentimento como "devendo ser livre, informado, inequívoco, explícito e/ou específico" (BIONI, *idem*, p. 117), e buscando "impor não só o direito do titular dos dados pessoais de os controlar, mas simetricamente, deveres aos *datas controllers* - quem processa os dados pessoais - para aperfeiçoar tal estratégia regulatória." (BIONI, *idem*, p. 118)

A diretiva 95/46/EC foi de tremenda importância na caminhada legislativa da proteção dos dados pessoais, tanto na União Europeia, quanto no mundo, na medida em que traçou diretrizes basilares sobre a matéria, como a definição do consentimento do titular e também os direitos do indivíduo e os deveres dos controladores dos dados[7].

Com o desenvolvimento das tecnologias computacionais, a informação tomou proporções cada vez maiores na realidade contemporânea. Pois, passou a ter sua circulação e processamento cada dia mais rápido e otimizado. Sobre o tema, Doneda (2011, p. 92) aponta que:

> A informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas. O

[7] Controlador de dados é toda pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Em outras palavras, trata-se daquele que ditará de que forma será tratado o dado pessoal coletado, sempre em observância aos dispositivos da GDPR e aos direitos do titular.

> que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação. Aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna elemento fundamental de um crescente número de relações e aumenta sua possibilidade de influir em nosso cotidiano.

Com as possibilidades advindas do aumento da capacidade de armazenamento e comunicação de informações, surgiu a necessidade de renovação da regularização dados pessoais.

Deste modo, após 20 (vinte) anos em vigor, a Diretiva 95/46/CE[8] foi substituída pela *General Data Protection Regulation* (GDPR). É destacado que além da necessidade de modernização da legislação, um dos principais motivos da substituição foram:

> as inconsistências na proteção de dados entre os Estados-Membros da União Europeia. Também foram destacadas pela a Comissão Europeia, a necessidade de uma regulamentação única e harmoniosa da proteção de dados abrangendo todo o território da União Europeia, em particular a fim de remover ou reduzir a margem de escolha dos legisladores nacionais, das autoridades de controle e dos tribunais (DIÁZ, 2016, n.p, tradução minha) [9].

Considerou-se que um texto normativo que tivesse a mesma base facilitaria o controle e o diálogo entre os países integrantes da UE.

Junto com os problemas que a legislação tinha em torno da não unificação do ordenamento ao longo do espaço comum da UE, vieram também os significativos avanços tecnológicos que facilitaram a comunicação instantânea de dados pessoais para além das fronteiras nacionais do espaço considerado.

Através da unificação da regulação referida à proteção de dados pessoais, seria possível lidar com proteção fora das fronteiras do Espaço Econômico Europeu.

---

[8] Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 195.9

[9] Texto original: The inconsistencies in data protection across the Member States of the EU have also been highlighted to the European Commission, the necessity for a single and harmonious regulation of data protection covering the whole of the territory of the EU, in particular in order to remove or reduce the margin of choice for national legislators, controlling authorities and the Courts.

Diáz (2016) argumenta que o ponto fundamental para a criação do GDPR seria as consequências sofridas pelo mercado interno dos países europeus pela configuração da 95/46/EC:

> A diversidade de abordagens nacionais sobre a eficácia da proteção de dados pessoais tem sido um obstáculo ao desenvolvimento e expansão do mercado interno. Conforme destacado pelo Tribunal de Justiça na Sentença Lindqvist de 2003, as diferenças entre os regimes nacionais de tratamento da proteção de dados podem afetar seriamente o estabelecimento e o funcionamento de um mercado interno (DIÁZ, 2016, n.p, tradução minha).[10]

A dificuldade do desenvolvimento da expansão do mercado interno europeu foi o fator decisivo para a unificação da legislação de proteção de dados na União Europeia. Em 2012, foi proposto pela Comissão Europeia a Reforma de Proteção de Dados o que:

> afetou dois instrumentos legislativos: o Regulamento Geral de Proteção de Dados foi criado para substituir a Diretiva 95/46/CE; e a Diretiva Proteção de Dados na área judicial e policial para substituir a Decisão-Quadro sobre proteção de dados de 2008.(DIÁZ, *idem*, n.p, tradução minha)[11]

Levando em conta as motivações acima expostas, “a União Europeia (UE) aprovou o Regulamento Geral de Proteção de Dados (GDPR) em abril de 2016, sendo iniciada sua vigência em 25 de maio de 2018, o que deu às empresas dois anos para se prepararem” (GOLDBERG *at al.*, 2019, p. 4).

Baseando-se em princípios como o do consentimento e a motivação, o GDPR abriu caminho para diversas leis de proteção de dados aprovadas subsequentemente em todo o mundo, dentre as quais a brasileira.

4.1.1 O surgimento da LGPD/Brasil

No Brasil, a normatização referente à privacidade aparece apenas na Constituição Federal de 1988, em termos da garantia legal à intimidade, à vida

[10] The diversity of national approaches on the effectiveness of personal data protection has been an obstacle to the development and expansion of the internal market. As highlighted by the Court of Justice in the Lindqvist Sentence of 2003, the differences between the national regimes for handling data protection can seriously affect the establishment and functioning of an internal market.

[11] It affects two legislative instruments: the General Data Protection Regulation is set to substitute Directive 95/46/CE; and the Data Protection Directive in the judicial and police area is set to substitute the Framework Decision on data protection of 2008.

privada, à honra e à imagem das pessoas, de acordo com o Art. 5º inciso X(BRASIL,1988). No entanto, o texto constitucional não conceitua tais termos. José Afonso da Silva (2005, p. 206) usa a expressão 'direito à privacidade' para "abarcar todas essas manifestações da esfera íntima, privada e da personalidade que o texto constitucional em exame consagrou". Ainda para esse autor (*apud* PEREIRA, 2005, p.206) a privacidade pode ser definida como "o conjunto de informação acerca do indivíduo, que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito."(OLIVEIRA, 1980, *apud* SILVA, 2005, p. 206).

A definição acima afirma a privacidade como a liberdade de escolher o que deve ser ou não divulgado sobre a intimidade do indivíduo. Em seguida, Silva (2005), citando Oliveira (1980, p.15) afirma que "a privacidade abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo". Assim, o conceito de privacidade contempla tanto o inciso X, quanto o inciso XI[12], que fala da casa como asilo inviolável do indivíduo.

Ainda na Constituição, há o dispositivo *habeas data,* que cumpre a função de garantir ao indivíduo o acesso e o conhecimento aos seus dados pessoais contidos nos bancos de dados, cadastros públicos ou de caráter público[13]. Cada sujeito pode reivindicar as informações pessoais quando necessário. O dispositivo *habeas data* pode ser considerada o embrião da legislação brasileira referida à proteção dos dados pessoais. Mesmo antes dos avanços tecnológicos computacionais, hoje conhecidos, já era uma preocupação dos legisladores desde a Constituição de 1988.

No Código Civil de 2002 a expressão direito à privacidade ainda não é utilizada, porém, é nele que a privacidade é reconhecida como um direito de personalidade e a vida privada da pessoa natural como inviolável[14]. Venosa (2013, p. 182) comenta que "os direitos da personalidade são os que resguardam a dignidade humana. Desse modo, ninguém pode, por ato voluntário, dispor de sua privacidade". O direito à privacidade é consolidado como direito de personalidade, inerente à pessoa natural.

---

[12] Artigo 5º, inciso X e XI, Constituição Federal, 1988.
[13] artigo 5º, inciso XXXIII, Constituição Federal, 1988.
[14] Artigo 21 do Código Civil, 2002.

O Código de Defesa do Consumidor (CDC) também traçou importantes delimitações quanto à privacidade e segurança das operações de consumo, dispondo de uma seção que trata dos bancos de dados e cadastros dos consumidores, a fim de garantir transparência e o direito à informação a respeito do que está sendo compartilhado sobre os indivíduos (CANTO, 2019). É garantido o acesso individual às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes[15].

Em 2011, foi promulgada a Lei nº 12.414/2011, bastante relevante na matéria da utilização de dados pessoais para fins específicos. Nasceu com o objetivo de formar um banco nacional de dados referidos às informações relativas a operações financeiras e de adimplemento para fins de concessão de crédito. Sobre esse tema, Bioni (2019, p. 122) afirma:

> Com isso, a situação econômica do postulante ao crédito não é mais, somente, analisada a partir de dados relativos a dívidas não pagas, mas também, a partir de outras informações que possam exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento.

A Lei supracitada ficou conhecida como ‘Cadastro Positivo’, por se tratar de banco de dados que aponta o histórico financeiro dos indivíduos baseado não nas suas dívidas, mas sim nos seus adimplementos. 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, 2019, p. 122).

Em 2019, a Lei Complementar nº 166/2019 veio para modificar alguns pontos da Lei do Cadastro Positivo. Segundo Bioni (*idem*) enquanto nesta, a inclusão de nomes dos consumidores só ocorria mediante consentimento do titular dos dados pessoais, naquela a inclusão dos consumidores no banco passou a ser automática. Assim, deixou de ser necessária a consulta aos indivíduos para que eles tivessem inseridos seus dados no banco de dados sobre o histórico financeiro pessoais, no cadastro positivo, sendo, porém, possível ao titular, de acordo com a norma, solicitar o cancelamento e a reabertura do cadastro quando desejar[16].

---

[15] artigo 47º, Código do Consumidor, 1990.
[16] LCP 166 art. 5º inciso I.

As alterações trazidas pela Lei Complementar também permitiram ao gestor o compartilhamento de informações cadastrais a terceiros, com a condição de também transferir as obrigações e responsabilidades de tratamento ao banco de dados que receber as informações[17]. Por fim, ainda é “dever do gestor da base de dados não coletar informações excessivas e sensíveis para fim de análise de crédito, bem como de não as utilizar para outra finalidade que não a creditícia” (BIONI, 2019, p. 124).

Conclui-se que as disposições trazidas na LC 166/2019, que modificaram a Lei do Cadastro Positivo (Lei 14.141/2011), consolidaram a necessidade de uma finalidade restrita para a coleta de dados a fins creditícios, não permitindo o excesso de levantamento de informações. Também firmou o direito à informação e controle do consumidor para com seus dados, dando mais um passo no caminho de uma legislação completa sobre a matéria.

Mais adiante, com Marco Civil da *Internet* (MCI) veio num período no qual os legisladores brasileiros reconheceram que não era mais possível adiar a regulamentarização das interações entre entes jurídicos referidas às inovações tecnológicas computacionais, buscando-se ampliar a atuação referente à proteção dos dados pessoais e da privacidade. Nos seus primeiros incisos, aponta diretrizes e princípios que giram em torno da liberdade de expressão e também da garantia à privacidade dos indivíduos.

O texto traz consigo a garantia da inviolabilidade do sigilo e do fluxo das comunicações *online* do usuário, que só poderá ser quebrado mediante ordem judicial[18]. Também são garantidas informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, necessitando essas operações de justificativa e do atendimento a finalidades que não sejam vedadas pela legislação[19]. O MCI também prevê que:

> 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 (Art 10º, Lei 12.965/2014).

[17] BIONI, 2019 p. 123.
[18] Artigo 7º, inciso II (Lei 12.965/2014).
[19] Artigo 8º (Lei 12.965/2014).

O Art 7º, IV da norma diz respeito ao consentimento quando cita a necessidade de clareza de informações dos contratos de prestações de serviços. Essa clareza remete a possibilidade do indivíduo de exercer o consentimento de maneira efetiva, ao saber com o que está concordando de maneira cristalina. O inciso diz ser um direito e garantia do usuário:

> informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade.

Sendo assim, o consentimento não era um dispositivo inédito na legislação brasileira que diz respeito ao uso da rede internacional de computadores. Porém, entende-se o inciso em questão procura proteger o consumidor, mostrando que mesmo com os avanços protetivos trazidos pelo MCI, o debate acerca de uma legislação específica para a regulamentarização dos dados pessoais se tornou cada vez mais relevante. Principalmente diante da realidade externa ao Brasil, na qual o tratamento abusivo de dados pessoais foi sendo crescentemente pautado no espaço público.

Em 2018 veio à tona o caso *Facebook*/*Cambridge Analytica,* cuja repercussão internacional deu ainda mais relevância à matéria. A ocasião:

> [...] acendeu o alerta sobre as chamadas tecnologias invasivas das grandes corporações digitais sobre a vida do cidadão, colocando como principal desafio a construção de barreiras legais. Calcula-se que 87 milhões de pessoas foram atingidas, incluindo, nesse universo, 443 mil usuários brasileiros. Tudo começou com um teste de personalidade sobre a vida digital aplicado aos usuários que concordaram com o teste. A Cambridge Analytica, contudo, coletou os dados dos amigos desses usuários para montar perfis voltados a influenciar eleitores (durante a última eleição americana) e para formar opinião (na campanha pela saída do Reino Unido da UE), em flagrante afronta ao direito à privacidade. A ferramenta propicia indevido e indesejável “controle social”, muito ao gosto dos regimes totalitários (CANTON, 2018 n.p).

De acordo com Sherr (2018, n.p):

> A *Cambridge Analytica* supostamente adquiriu os dados de uma forma que violou as políticas da rede social Facebook. Em seguida, teria aproveitado as informações para construir perfis psicográficos de usuários e seus amigos, que foram usados para anúncios políticos direcionados na campanha do referendo do *Brexit*, no Reino Unido, bem como pela equipe de Trump durante a eleição de 2016 nos EUA.

A utilização dos dados pessoais de usuários de um aplicativo não é o problema em questão, mas sim a maneira como foram coletados e utilizados sem a oportunização do consentimento dos indivíduos, através de uma definição clara dos objetivos almejados pela coleta. Os titulares dos dados não tinham conhecimento do fim almejado das informações que estavam fornecendo. Tal técnica já havia sido usada em eleições presidenciais anteriormente, como afirma Sher (*idem*, n.p):

> Os dados pessoais dos indivíduos já haviam sido usados numa campanha eleitoral dos Estados Unidos. O ex-presidente Barack Obama também utilizou técnica similar, no entanto, com uma grande diferença: o aplicativo utilizado para adquirir as informações deixava claro nos termos de uso que as mesmas seriam usadas numa campanha política. A campanha de Obama usou os dados dos amigos do usuário do *facebook* para descobrir quem poderia ou não estar disposto a votar nele e enviou mensagens aos usuários para persuadir seus amigos.

A situação descrita acima difere bastante da que envolveu a *Cambridge Analytica*, já que nesta os usuários da rede social respondiam questionários sobre sua vida e suas preferências sem ter ideia de que seus dados pessoais seriam usados para fins políticos.

A grande visibilidade dada aos episódios de usos abusivo dos dados pessoais dos indivíduos por empresas de tratamento de dados como a *Cambridge Analytica*, reacendeu a discussão sobre a privacidade na *internet* no cenário mundial e deixou empresas e líderes de muitos países em alerta. Ficou evidente como os dados pessoais coletados e usado à revelia dos indivíduos que os originam podem ser ferramentas poderosas quando recebem tratamento direcionado para fins específicos, como aconteceu no *Brexit* e nas eleições estadunidenses de 2016. Em ambos os casos a utilização dos dados pessoais foi decisiva para definir decisões políticas de alcance macrossocial.

Após quase dez anos de debates sobre o tema, diante da pressão externa e o desejo de continuar dialogando com empresas da União Europeia e de outras regiões, o Brasil se viu forçado a adaptar sua legislação referente à privacidade e aos dados pessoais, sendo aprovada a Lei de Proteção dos Dados Pessoais, a LPDP. O direito foi estabelecido como uma resposta às demandas sociais decorrentes das transformações pelas quais tem passado o mundo em geral, especificamente a sociedade brasileira. Como aponta Bobbio (2004, p. 37),

> 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.

O surgimento da LGPD representa o avanço legislativo no caminho do fortalecimento regulatório da matéria. Fazendo com que a legislação se moldasse as necessidades trazidas pela sociabilidade no contexto da era digital e da hiperconectividade no qual a realidade atual de muitas sociedades se encontra (CANTO, 2019).

5 PRINCIPAIS SEMELHANÇAS E DIFERENÇAS ENTRE O GDPR (EU) E A LGPD (BRASIL)

Para comparar as diretrizes da União Europeia e brasileira sobre a matéria da proteção dos dados pessoais, serão levados em consideração alguns pontos principais, tais como: (1) o alcance da Lei; (2) o papel do consentimento e do legítimo interesse; (3) os direitos do titular dos dados pessoais; (4) os deveres dos controladores; e, por fim, (5) a notificação de incidentes envolvendo dados pessoais.

Em primeiro lugar, sobre o alcance da Lei, o GDPR e a LGDP definiram que os dados anônimos estão fora da aplicabilidade da regulamentação[20]. Ambas definem critérios similares para definir quais são os dados tidos como anónimos, sendo um dado anonimizado na LGPD aquele "relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º inciso III). O GDPR afirma ser informação anônima a que não diz respeito a uma pessoa singular identificada ou identificável ou a dados pessoais tornados anónimos de forma que o titular dos dados não seja ou deixe de ser identificável[21].

Também é estabelecido nos dois textos o que deve ser levado em conta para verificar se o processo de anonimização não é reversível, e quais os ditos meios razoáveis que possibilitam à pessoa física ter seus dados anonimizados revertidos em dados pessoais. São esses meios: custo, prazo e tecnologia. Sendo assim, se não houver a possibilidade de utilizar esses meios razoáveis para associar os dados ao titular novamente, o mesmo será definido como anônimo.

No que diz respeito à aplicação do GDPR, os princípios, as regras, a proteção de pessoas naturais e seus dados pessoais servem para aqueles que se encontram

---

[20] Art. 26 do REGULATION (EU) 2016/679 in verbis: The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.
Art. 12 da LGPD/2018 in verbis: Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

[21] Art. 26 do REGULATION (EU) 2016/679 in verbis: The Data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

na União Europeia. Independente de nacionalidade, cidadania, domicílio ou residência[22]. A Lei brasileira, Tutela 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: operação de tratamento seja realizada no território nacional[23].

Sobre o consentimento, Bioni *et al.* (2018) afirmam existir um alto nível de convergência entre LGPD e GDPR quando se trata do tema: “ambos os ordenamentos atribuem o consentimento como apenas uma das fases pelas quais os titulares podem controlar os seus dados”[24] (BIONI *et al.*, 2018). No GDPR, o consentimento deve ser dado por um ato afirmativo claro e que estabeleça uma indicação dada livremente, específica, informada e inequívoca da concordância do titular com o processamento de dados pessoais relacionados a ele ou ela, como uma declaração por escrito, incluindo por meios eletrônicos, ou uma declaração oral[25].

Nem silêncio, *pre-ticked boxes*[26] ou inatividade devem constituir consentimento. O consentimento na LGPD é definido como manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.[27] O art 7º ainda indica como pré requisito para que seja realizado o processamento dos dados. “Além da qualificação ampla do consentimento, há atribuição de poderes aos titulares de dados pessoais, que devem ter escolha significativa em relação a suas informações” (BIONI *et al.*, 2018). Fica clara, portanto, a aproximação entre as normas quando o assunto é consentimento, elemento considerado central na proteção de dados pessoais,

22 Art 2º do REGULATION (EU) 2016/679 in verbis: The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

23 Art 3º da Lei Geral de Proteção de Dados Nº 13.709.

24 Texto original: Both regulations are concerned not only with an extensive qualification of consent, but also empowering data subjects with meaningful control and choice regarding their personal information.

25 Art 32º do REGULATION (EU) 2016/679 in verbis: Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

26 Caixa com opção de marcar.

27 Art. 5º da Lei Geral de Proteção de Dados Nº 13.709.

mesmo sendo apenas uma das ferramentas através das quais o titular deles pode proteger e ter ciência das informações sobre si.

Já o dispositivo do legítimo interesse não existia no sistema anterior de proteção de dados pessoais Brasileiro, sendo uma novidade relevante da LGPD (Lei Nº 13.709/2018). O controlador, na Lei nº 13.709, somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam ao apoio e promoção de atividades do controlador; e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

O GDPR define o reconhecimento de legítimo interesse “quando existe uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento em situações como quando o titular dos dados é um cliente ou ao serviço do responsável pelo tratamento”[28]. Além disso, pontua que a existência de um interesse legítimo exigiria uma avaliação cuidadosa, incluindo se o titular dos dados pode razoavelmente esperar, no momento e no contexto da coleta de dados pessoais, que o processamento para esse fim possa ocorrer[29].

Segundo o GDPR, os interesses e direitos fundamentais do titular dos dados podem, em particular, prevalecer sobre o interesse do responsável pelo tratamento dos dados quando eles são tratados em circunstâncias em que seus titulares não têm expectativa razoável de um tratamento posterior[30].

Bioni *et al.* (2018) consideram o legítimo interesse como possivelmente mais flexível na LGPD do que no regulamento europeu, na medida que o mesmo pode ser utilizado definido em relação à promoção das atividades do controlador, de certa maneira o priorizando, enquanto no GDPR os interesses do titular sempre ultrapassam os do controlador.

No que tange aos direitos do titular dos dados pessoais e os deveres dos controladores, é importante pontuar o direito à portabilidade dos dados pessoais, definido como:

---

[28] Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller (REGULATION (EU) 2016/679).

[29] The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place(REGULATION (EU) 2016/679).

[30] Texto original: the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.

> o direito do titular dos dados de controlar, gerenciar e reutilizar seus dados pessoais. Ou seja, o direito de requerer que dados cedidos para uma empresa controladora X sejam transferidos para outra empresa controladora Y, mesmo que elas sejam concorrentes, sem que a primeira empresa, inclusive, detenha esses dados (SETA, 2019, n.p, tradução minha).

No artigo 18º.da LGPD (Lei Nº 13.709) são previstos ao titular, por meio de requisição, diversos direitos, entre eles o da "portabilidade dos seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial" (Art. 18º inciso V, Lei Nº13.709/2018).

No regulamento europeu (GDPR), a portabilidade de dados aparece para reforçar ainda mais o controle sobre seus próprios dados:

> Quando o processamento de dados pessoais é realizado por meios automatizados, o titular dos dados também deve ser autorizado a receber dados pessoais que lhe digam respeito ou que tenham fornecido a um responsável pelo tratamento em um formato estruturado, comumente usado, legível por máquina e interoperável, e para transmiti-lo a outro controlador. Os controladores de dados devem ser incentivados a desenvolver formatos interoperáveis que possibilitem a portabilidade dos dados. Esse direito deve aplicar-se quando o titular dos dados forneceu os dados pessoais com base no seu consentimento ou se o tratamento for necessário para a execução de um contrato. Não deve ser aplicado quando o processamento for construído em uma base legal diferente de consentimento ou contrato (Art. 73, REGULATION (EU) 2016/679, tradução minha).[31]

Como explicado acima, o GDPR não deve ser aplicada quando o processamento tiver seus alicerces em uma base legal distinta do consentimento ou contrato. Bioni *et al*.(2018) apontam a divergência nesse quesito, quando comparado ao Brasil: "esse direito não se limita aos dados fornecidos com base no consentimento dos titulares"(tradução minha)[32]. Os autores também apontam que o

[31] Where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract.

[32] Texto original: In Brazil, this right is not limited to data provided based on data subjects' consent, making it different from the GDPR.

direito à portabilidade dos dados já existia no ordenamento brasileiro. Mesmo tendo uma nova roupagem com a legislação específica de proteção de dados pessoais: "já existia no Brasil desde 2007, quando foi possível solicitar à portabilidade de dados pessoais vinculados a um número de telefone (resolução 460/07), Chamado de Regulamento Geral da Portabilidade da Anatel (BIONI *et al.,* 2018, tradução minha)[33]". Por fim, se tratando da portabilidade de dados, a Lei brasileira se mostra mais abrangente na tutela da matéria, não se limitando somente aos dados fornecidos através de contratos e consentimento.

Sobre o direito de revisão da tomada de decisão automatizada, a LGPD garante ao titular dos dados o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade[34]. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Por fim, a lei também diz que "a defesa dos interesses e dos direitos dos titulares dos dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva" (Art. 22, Lei Nº13.709/2018).

O GDPR diz ser obrigação do responsável pelo tratamento de dados pessoais fornecer informações adicionais necessárias para garantir um tratamento justo e transparente, dentre as quais se encontra, na letra f do segundo parágrafo,

> [...] a existência de tomada de decisão automatizada, incluindo criação de perfis, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal tratamento para o titular dos dados[35].

---

[33] Texto original: In Brazil, since 2007 it has been possible to request the portability of personal data related to a telephone number, a right created by Resolution 460/07 better known as the General Portability Regulation of ANATEL.

[34] Art. 20 (REGULATION (EU) 2016/679).

[35] In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject(REGULATION (EU) 2016/679).

Nesse quesito a norma brasileira se faz mais abrangente ao não especificar a aplicabilidade da norma ao processamento de dados para uma finalidade específica, como faz a GPDR, ao limitar a aplicabilidade à criação de perfis digitais, mas sim para qualquer finalidade (BIONI *et al.*, n.p. 2018, tradução minha)[36].

Por ter vindo depois do GDPR, a Lei 13.709 é mais moderna e busca preencher lacunas deixadas pelo Regulamento que a inspirou. Em contrapartida, o Brasil postergou a criação da Autoridade Nacional de Proteção de Dados (ANPD), que, até o momento da finalização do presente trabalho, ainda não estava em funcionamento pleno. Por se fazer necessária em muitos pontos da Lei, a lentidão na efetivação de seu funcionamento pode acabar por atrapalhar a aplicabilidade da norma. A LGPD, que entrou em vigor em agosto de 2020, após dois anos de adaptação, teve finalmente a estrutura da ANPD aprovada pelo Governo Federal[37]. Nesse ponto, o GDPR apresenta uma vantagem, já que as Autoridade de Proteção de Dados Pessoais já existiam em âmbito nacional nos Países-membro e puderam auxiliá-los durante o período de adaptação ao Regulamento unificador da União Europeia.

[36] Texto original: However, compared to the GDPR, the impact on the data subject is presumed when automated decision making is based on profiling, and there is no limitation to situations when the data was provided by consent. Therefore, such rights provided for the LGDP may be considered broader (more protective) than the right as set forth by the GDPR.

[37] O governo federal aprovou a estrutura regimental e quadro de cargos para a criação da Autoridade Nacional de Proteção de Dados (ANPD). O órgão está subordinado à Presidência da República e tem a função de fiscalizar e editar normas sobre o tratamento de dados pessoais por pessoas físicas e jurídicas.
(https://agenciabrasil.ebc.com.br/geral/noticia/2020-08/governo-aprova-estrutura-da-autoridade-nacional-de-protecao-de-dados). O decreto foi publicado dia 27 de agosto de 2020. O mesmo remaneja e transforma cargos em comissão e funções de confiança da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital, do Ministério da Economia, para a ANPD (https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/08/2020&jornal=515&pagina=6)

5.1 Comparativo entre as sanções previstas no GDPR e na LGPD

Nesta seção será observado o Regulamento Europeu (UNIÃO EUROPÉIA, 2016/679), no trecho que trata das sanções. Em seguida, serão examinados os artigos da norma de Proteção de Dados Pessoais Brasileira que trata das Sanções aplicáveis nos casos de irregularidade ou inobservância da Lei 13.709 (LGPD). levando em consideração os mesmos aspectos. Como objetivo, pretende-se pontuar as semelhanças e afastamentos das normas no quesito das sanções, principalmente aquelas com impactos pecuniários.

Em vigor desde 2018, o Regulamento que rege a proteção de dados pessoais na União Europeia ((EU) 2016/679) foi um marco para os Países-Membro do grupo, sendo operacionalmente importante na medida que permitiu unificar o entendimento sobre a matéria no âmbito no bloco geopolítico aqui comentado. Como consequência do seu surgimento, os Países-membros passaram a ter normas e uma autoridade de proteção, superiores às locais.

Além da unificação, o Regulamento ((Eu) 2016/679) também foi o primeiro passo para a discussão sobre uma norma de proteção de dados pessoais em vários lugares do mundo, servindo como espelho para diversos países legislarem sobre o tema. Entre os países que se espelharam na hora de criar sua lei de Proteção de Dados Pessoais (Lei nº 13.709/2018), está o Brasil.

As sanções do regulamento europeu estão previstas no Capítulo VIII, intitulado de “remédios, responsabilidade e penalidades”[38]. Primeiro é garantido aos indivíduos o direito de apresentar uma reclamação a uma autoridade de supervisão[39], sem que seja causado qualquer prejuízo a outro eventual recurso administrativo ou judicial. A reclamação deve ser feita no Estado-membro no qual está localizada a residência habitual, trabalho de quem propôs a queixa ou no local onde a infração aconteceu. É obrigação da autoridade de controle manter o titular informado sobre a evolução e resultado judicial. [40]

Caso sinta que seus direitos não foram contemplados, o titular de dados tem direito a um recurso judicial efetivo contra o controlador e o processador[41]. Em seguida, o artigo 79 irá definir que tipo de processo contra o responsável pelo

[38] Remedies, liability and penalties.
[39] Right to lodge a complaint with a supervisory authority (Art. 77º, REGULATION (EU) 2016/679).
[40](Art. 77º, REGULATION (EU) 2016/679).
[41] (Art. 79º, REGULATION (EU) 2016/679).

tratamento ou seu subcontratante deve ser intentado nos tribunais do Estado-Membro no qual o agente do tratamento ou o subcontratante tiver um estabelecimento. O processo também poderá ser intentado nos tribunais do Estado-Membro onde o titular dos dados tem a sua residência habitual, a menos que o responsável pelo tratamento ou o processador seja uma autoridade pública de um Estado-Membro no exercício das suas atribuições[42].

Será direito do titular ser representado e assistido por uma organização ou associação sem fins lucrativos que tenha sido devidamente constituída de acordo com a legislação de um Estado-Membro. E tenha objetivos estatutários de interesse público e seja ativo no domínio da proteção dos direitos e liberdades dos titulares de dados no que diz respeito à proteção dos seus dados pessoais para apresentar a reclamação em seu nome[43].

Em seguida, igualmente a legislação brasileira, o regulamento europeu também garante a reparação de danos e dispõe sobre a responsabilidade dos agentes do tratamento. o ponto número 1 (um) do artigo 82 prevê que qualquer pessoa que tenha sofrido danos materiais ou morais em resultado de uma violação do presente regulamento tem o direito de ser indenizada pelo responsável do tratamento ou pelo transformador pelos danos sofridos.

No ponto 2 (dois) é dito que qualquer controlador envolvido no tratamento ressarcirá os danos causados quando suas condutas infringirem o citado regulamento vigente. Sobre o processador, é previsto que ele só será responsável pelos danos causados se não tiver cumprido as obrigações deste regulamento especificamente dirigidas aos processadores ou se tiver agido de forma contrária às instruções legais do responsável ditas pelo Controlador.

Ao observar os pontos 1 (um) e 2 (dois) do artigo 82 (UE), percebe-se que no tocante à responsabilidade dos agentes responsáveis pelo tratamento de dados pessoais, são evidentes as semelhanças advindas da inspiração do regulamento referido à EU trazida para a Lei brasileira sobre tal matéria. Sendo assim, as responsabilidades do controlador e do processador em ambas as legislações convergem perfeitamente.

No quesito isenção de responsabilidade, o regulamento europeu se mostra menos detalhado que o brasileiro. Naquele, o controlador ou o processador estará

[42](Art. 79º, 2, REGULATION (EU) 2016/679).
[43](Art. 80º, 2, REGULATION (EU) 2016/679).

isento de responsabilidade se provar que não é, de forma alguma, responsável pelo fato que deu origem ao dano[44]. Na Lei brasileira, o tema se divide em três possibilidades nas quais não haverá responsabilização. Porém, as duas normas se assemelham na necessidade de comprovação de culpa dos agentes do tratamento para que haja responsabilidade. Ambas garantem a proteção do controlador e do operador de dados pessoais que agiram de acordo com as normas de segurança estabelecidas.

Casos nos quais há mais de um controlador ou processador, ou um controlador e um processador, que estiverem envolvidos no mesmo tratamento e forem responsáveis por qualquer dano causado pelo processamento dos dados, ambos serão considerado responsáveis por todos os danos, a fim de assegurar uma indenização efetiva ao titular[45]. Sendo assim, há responsabilidade solidária entre os agentes, como também observado na lei brasileira.

Em seguida, no art. 83 são definidas as condições gerais para aplicação das sanções administrativas. No ponto 1 (um) é definido que cada autoridade de controle deve assegurar que a aplicação de multas administrativas por infracções ao regulamento seja eficaz, dissuasiva e proporcionada em cada caso específico[46]. As multas administrativas deverão ser aplicadas proporcionalmente às circunstâncias de cada caso individual.

Ao decidir sobre a aplicação de uma multa administrativa e o valor em cada caso individual, deverão ser levados em consideração alguns aspectos, dentre eles: (1) a natureza, gravidade e duração da infração, tendo em conta a natureza, âmbito e objetivo do tratamento em causa, bem como o número de titulares de dados afetados e o nível dos danos por eles sofridos; (2) o caráter intencional ou negligente da infração; (3) qualquer ação tomada pelo controlador ou processador para mitigar os danos sofridos pelos titulares dos dados; (4) quaisquer infrações anteriores relevantes por parte do controlador ou processador; (5) o grau de cooperação com a autoridade de supervisão; e (6) as categorias de dados pessoais afetados pela infração dentre outros previstos no artigo[47].

[44](Art. 83º, 3, REGULATION (EU) 2016/679).
[45](Art. 82º, 4, REGULATION (EU) 2016/679).
[46](Art. 83º, 1, REGULATION (EU) 2016/679).
[47](Art. 83º, 2, REGULATION (EU) 2016/679).

De maneira consecutiva, é previsto nos pontos 4 (quatro), 5(cinco) e 6 (seis) do art. 83º o limite das multas pecuniárias impostas. O valor delas são determinados de acordo com a infração desrespeitada. Sendo as infrações às seguintes disposições sujeitas a multas administrativas de até 10. 000.000,00 (dez milhões) de Euros ou, no caso de uma empresa, até de 2% (dois por cento) do volume de negócios anual total no nível mundial, como registrado no exercício anterior. Serão levadas em consideração: (1) as obrigações do controlador e do processador dispostas no regulamento em questão; (2) as obrigações do organismo de certificação de acordo com os Artigos 42º e 43º; e (3) as obrigações do organismo de controlo nos termos do n.º 4 do artigo 41º.

No ponto 5 (cinco) são previstas multas administrativas de até 20.000.000 (vinte milhões) de euros ou, no caso de uma empresa, até de 4% (quatro por cento) do volume de negócios anual total no nível mundial como registrado no exercício anterior, caso cometa as infrações de seguinte natureza: os princípios básicos do tratamento, incluindo as condições de consentimento, previstos neste regulamento; os direitos das pessoas em causa; as transferências de dados pessoais para um destinatário num país terceiro ou organização internacional; incumprimento de uma ordem ou limitação temporária ou definitiva do tratamento ou suspensão dos fluxos de dados pela autoridade de controle.

Por fim, o ponto 6 (seis) discorre sobre o incumprimento de uma ordem da autoridade de supervisão a que se refere o artigo 58.º, que pode acarretar multa ao sujeito a de até 20.000.000,00 (vinte milhões de euros) ou, no caso de uma empresa, até 4% (quatro por cento) do total do volume de negócios anual mundial do exercício anterior, o que for mais elevado.

No que diz respeito às autoridades e organismos públicos, o regulamento europeu prevê que: sem prejuízo dos poderes corretivos das autoridades de supervisão da união europeia, caberá a cada Estado-Membro estabelecer regras sobre em que medida podem ser aplicadas multas administrativas às autoridades e organismos públicos estabelecidos nesse Estado-Membro[48], divergindo da LGPD, na qual as entidades de natureza pública e estatal não sofrem multas administrativas pecuniárias. Já no GDPR, cabe a cada Estado-Membro legislar sobre o tema de maneira particular.

[48](Art. 83º, 7, REGULATION (EU) 2016/679).

O GDPR veio com o intuito de unificar o entendimento sobre a proteção de dados pessoais na União Europeia, de maneira conciliadora, garantindo uma certa autonomia aos países. Segundo o artigo 84, que trata das penalidades: os Estados-Membros devem estabelecer regras sobre outras sanções aplicáveis às infrações ao regulamento, em especial no que se refere às infrações que não sejam objeto de multas administrativas e tomar todas as medidas necessárias para garantir a sua aplicação. Essas sanções devem ser efetivas, proporcionais e dissuasivas.

Por último, ficou previsto no regulamento que cada Estado-Membro deveria notificar à Comissão as disposições da sua legislação específica adotadas até 25 de maio de 2018 e, qualquer alteração subsequente das mesmas[49]. Tal dispositivo deixa claro que há uma certa autonomia, embora exista um vínculo entre às autoridades de proteção de dados de cada País-Membro com a Autoridade de dados da União Europeia. Os estados membros estão vinculados com objetivo de obter maior unidade nos entendimentos sobre o tema, o que gera facilidades, principalmente econômicas, devido aos países serem regidos pela mesma norma referidas a transações que envolvam dados pessoais.

Observando ambas as legislações, a brasileira (13.709) e a europeia ((EU) 2016/679), fica evidente o quanto o texto da LGPD foi influenciado pelo regulamento da união europeia. Entre os principais pontos em comum estão a atribuição de responsabilidade pelos danos causados ao titular de dados devido ao tratamento e a necessidade de culpa dos agentes para que haja a reparação dos danos. Tais dispositivos trazem uma sensação de maior amparo para os controladores e operadores dos dados, evidenciando que a proteção trazida pela lei não busca amparar somente o titular, mas também aqueles agentes do tratamento que agem de acordo com as normas.

Dando continuidade, no tocante à aplicação das sanções administrativas, há bastante convergência entre as normas, observando-se que tanto na Lei 13.709/2018 (LGPD) como no Regulamento Europeu, faz-se necessário cumprir requisitos para que sejam aplicadas. Porém, quando o assunto são as multas pecuniárias, o GDPR se mostra mais específica, ao estabelecer o teto do valor à natureza da infração. Sendo assim, o limite da quantia da multa vai depender da

[49](Art. 83º, 9, REGULATION (EU) 2016/679).

violação cometida. Indo de 10.000.000 EUR (dez milhões de euros) até o teto de 20.000.000 EUR (vinte milhões de euros). Já no Brasil, independente da norma discumprida, o teto da multa tem o limite estabelecido de R$ 50.000.000 (cinquenta milhões de reais).

Algo também importante de se mencionar é que no regulamento da União Europeia, embora seja patente a intenção unificadora dos países-membros, fica a critério de cada país e da sua Autoridade Nacional de Proteção de Dados decidir em que medida caberão multas administrativas pecuniárias sobre às autoridades e organismos públicos. No Brasil é bem definida a norma que coloca como exceção a aplicabilidade de multas pecuniárias às entidades e aos órgãos públicos[50] (BRASIL, 2018).

A LGPD foi aprovada em 2018. Em seu texto, foi definido que após 18 (dezoito) meses da sua publicação oficial ela entraria em vigor.[51] Esse tempo serviria para a adaptação dos agentes que lidam com tratamento de dados pessoais no Brasil. A entrada em vigor da lei foi alvo de diversos adiamentos, resultado das discussões sobre a dificuldade de adaptação dos sujeitos que lidam com o tratamento de dados pessoais aos parâmetros do regulamento. Mesmo com turbulências e protelações, em meio à pandemia do COVID-19[52], no ano de 2020[53], a LGPD entra em vigor, com a condicionante do adiamento da aplicação das sanções previstas para agosto de 2021[54], 24 (vinte quatro) meses após sua publicação oficial.

De início, ao tratar das sanções previstas na Lei 13.709(LGPD), é necessário observar a Seção III, Capítulo IV, na qual se encontram os artigos que tratam da responsabilidade de ressarcimento aos danos causados pelo tratamento de dados pessoais. Nessa seção é determinado que o dano causado a outrem em razão do exercício de atividade de tratamento de dados pessoais, seja de natureza

---

[50] Art 52º, § 3º da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018.
[51] Art. 65º da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018.
[52] "A pandemia mundial de 2020 provocada pelo COVID-19 impulsionou mudanças de ordem estrutural nas organizações econômicas empresariais, impactando diversos segmentos da indústria e promovendo a aceleração do processo de digitalização nos seus modelos de negócios." o que tornou ainda mais urgente a atenção a proteção dos dados pessoais. AMORIM (2020).
[53] A decisão se deu por meio de emenda da MPV 959/2020 na qual: "Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020, de 6 de julho de 2020; e altera a Lei nº 13.709, de 14 de agosto de 2018."

[54]Art. 65º, inc. I-A, da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018.

patrimonial, moral, individual ou coletiva, em violação à Lei 13.709, será de responsabilidade do controlador ou do operador, que terá de repará-lo[55]. Em seguida, é prevista a possibilidade do operador responder solidariamente[56] pelos danos causados pelo tratamento quando descumprir as obrigações da Lei 13.709, ou quando não tiver seguido as orientações lícitas do controlador[57]. Também respondem de maneira solidária os controladores que estiverem diretamente envolvidos no tratamento dos dados que acarretou danos ao titular.

O artigo 49 da Lei 13.709, dispõe das ocasiões nas quais os agentes de tratamento não serão responsáveis caso provem: (1) que não realizaram o tratamento que envolve os danos causados ao titular; (2) que mesmo realizando o tratamento em questão, não houve violação à Lei de Proteção de Dados Brasileira; e (3) caso provem que o dano é recorrente de culpa do titular ou de terceiros.

Por fim, o artigo 44 da Lei 13.709 define que será irregular o tratamento de dados quando deixar de observar as medidas de segurança que o titular deve esperar. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que deixar de adotar as medidas de segurança previstas na Lei. Logo, a responsabilização dos agentes que lidam com o tratamento de dados, tem uma roupagem justa na Lei 13.709, pois a responsabilidade solidária por parte do operador só ocorrerá caso seja provado que o mesmo não agiu de acordo com a lei, ou divergiu das orientações lícitas do seu controlador.

Também é possível perceber que a responsabilização trazida pelos artigos da seção III, capítulo IV, garante aos agentes de tratamento o direito à ampla defesa e a certeza de que caso cumpram as normas de maneira correta, não serão responsabilizados de forma equivocada pelos danos causados ao titular dos dados. Sendo assim, a LGPD busca amparar os agentes que lidam com tratamentos de dados e que buscam estar em conformidade com a Lei.

Em seguida, o Capítulo VIII trata das sanções administrativas e das particularidades de sua aplicação. Logo no início, o artigo 52º traz as sanções administrativas em razão de infrações cometidas à Lei 13.709 (LGPD). Inicialmente,

---

[55] Art. 42º da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018

[56] Responsabilidade solidária ocorre quando há pluralidade de agentes, tanto no polo passivo quanto ativo, e sobre eles incorre a obrigação pelo débito todo, ou direito pela prestação inteira, como se cada um fosse o único credor ou devedor da obrigação (https://carolineborota.jusbrasil.com.br/artigos/437649443/responsabilidade-solidaria-no-direito-civil-comparada-ao-direito-do-trabalho).

[57] Art. 42º, §1º da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018.

deverá ser entregue uma advertência contendo prazo para adoção de medidas corretivas. Caso o Controlador responsável não corrija o motivo da infração, serão aplicadas as seguintes sanções: multas simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou aglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observando o limite supracitado; publicização da infração após devidamente apurada e confirmada a sua ocorrência; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador e por último, a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados[58].

É importante mencionar, o dispositivo da Lei que garante só serem aplicadas as sanções após procedimento administrativo que possibilite a ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as particularidades do caso concreto[59].

Posteriormente, também é mencionado que serão observados critérios para a aplicação das sanções, como, por exemplo, a necessidade de ter sido imposta ao menos 1(uma) das sanções mais suaves (previstas nos incisos II, III, IV, V e VI)[60] para que, assim, em seguida, sejam aplicadas as entendidas como mais gravosas (incisos X, XI e XII)[61], dentre elas a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

É previsto na norma que serão aplicadas as mesmas sanções a entidades e órgãos políticos, com exceção apenas das multas simples e das multas diárias

---

[58] Art. 52º da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018.

[59] Art. 52º, § 1º da Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018.

[60] II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI- eliminação dos dados pessoais a que se refere a infração; (Lei Geral de Proteção de Dados Pessoais, Nº 13.709/2018**).**

[61] X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei Nº 13.853, de 2019).
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

(previstas nos incisos II e III). Ou seja, a esses sujeitos, diferente das pessoas jurídicas de natureza privada, não serão aplicadas sanções pecuniárias.

No tocante aos prejuízos financeiros que as sanções da LGPD podem causar, se destacam os incisos II e III, nos quais são definidas as multas simples, que podem acarretar em, até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração e também as multas diárias, que devem observar o limite previsto no inciso anterior.

Para poder regular as multas a fim de que as mesmas não acarretam em perdas abusivas para empresas privadas, de acordo com a Lei, será indispensável o papel da Autoridade de Proteção de Dados Pessoais (ANPD), ente responsável por definir, por meio de regulamento próprio, sobre as sanções administrativas a infrações, as quais deverão ser objeto de consulta pública, e também estabelecerá as metodologias que orientarão o cálculo do valor-base das sanções de multa[62].

Do mesmo modo é papel da ANPD definir o valor da sanção de multa diária aplicável às infrações, observando a gravidade da falta e a extensão do dano ou prejuízo causado de maneira fundamentada pelo órgão. Os aspectos levados em consideração deverão ser devidamente fundamentados pela autoridade nacional.

Pelo observado nos dispositivos previstos na Lei, conclui-se que o papel da ANPD é fundamental para que se desenhem os impactos das sanções da Lei nº 13.709/2018 (LGPD), principalmente as que implicam em multas pecuniárias, direcionadas pela Lei 13.709 às entidades privadas que lidam com dados pessoais. Os valores, a metodologia utilizada para aplicar as multas e a fundamentação do emprego das mesmas às entidades serão definidos pela atuação da ANPD.

Quadro comparativo entre as sanções do GENERAL DATA PROTECTION REGULATION (UNIÃO EUROPÉIA, 2016/679) e da LEI GERAL DE PROTEÇÃO DE DADOS (BRASIL, Nº 13.709)

	GDPR	LGPD
Entrada em vigência e Período de adaptação	Maio de 2018 - 18 meses de adaptação	Agosto de 2020 - 24 meses de adaptação

[62] Art. 53º da Lei Nº 13.709/2018.

Reparação de danos e responsabilidade dos agentes de tratamento	Art. 82: Qualquer pessoa que tenha sofrido danos materiais ou morais em consequência de uma infração ao presente regulamento terá o direito de ser indemnizada pelo responsável pelo tratamento (controlador) ou pelo operador, pelos danos sofridos.	Igualmente ao regulamento europeu, a Lei brasileira também garante que: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (Art. 42, Lei 13.709/2018.
Responsabilidade solidária dos agentes de tratamento	Art. 82, 4: Quando mais de um controlador ou processador, ou um controlador e um processador, estão envolvidos no mesmo processamento e quando são, nos termos dos parágrafos 2 e 3, responsáveis por qualquer dano causado pelo processamento, cada controlador ou processador será responsabilizado por a totalidade dos danos, a fim de garantir uma compensação efetiva do titular dos dados.	Igualmente ao regulamento europeu irá existir responsabilidade solidária entre o (os) controlador (res) e o processador. Mas, o processador só irá responder responder solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador (Art 42º, § 1º, II, Lei 13.709/2018).
Isenção de responsabilidade dos agentes de tratamento	Art. 82º, 3: Um controlador ou processador está isento de responsabilidade se provar que não é, de forma alguma, responsável pelo acontecimento que deu origem ao dano.	A lei brasileira é mais detalhada sobre os casos nos quais haverá isenção de responsabilidade para os agentes de tratamento dos dados. De acordo com o Art. 49º da Lei 13.709/2018, não serão responsáveis caso provem: a) que não realizaram o tratamento que envolve os danos causados ao titular; b) que mesmo realizando o tratamento em questão, não houve violação à Lei de Proteção de Dados Brasileira; c) caso provem que o dano é recorrente de culpa do titular ou de terceiros.
Sanções administrativas aplicáveis	De acordo com o artigo 84º Os Estados-Membros devem estabelecer regras sobre outras sanções aplicáveis às infrações ao presente regulamento, em especial no que se refere às infrações que não sejam objeto de multas administrativas pecuniárias.	Diferente do GDPR, a LGPD no Art. 52º, define sanções administrativas aplicáveis, inclusive as de caráter pecuniário: I - advertência, com indicação

	Só há matéria legal previamente definida no regulamento para as multas de teor pecuniário no Art. 83º. No qual está previsto os valores máximos aplicáveis a depender da natureza da infração.	de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
Aspectos gerais da aplicação de multas administrativas	Cada autoridade de controle dos Países-Membro deve assegurar que a aplicação de multas administrativas ao abrigo do presente artigo por infracções ao presente regulamento a que se referem ao presente regulamento seja eficaz, proporcional e	A norma brasileira faz questão de frisar a importância da garantia da ampla defesa na hora de definir os aspectos levados em consideração para

	dissuasiva em cada caso específico.	a aplicação das sanções e multas administrativas.
Aspectos levados em consideração para a aplicação de multas administrativas	a) a natureza, gravidade e duração da infração, tendo em conta a natureza, âmbito ou objetivo do tratamento em causa, bem como o número de titulares de dados afetados e o nível dos danos por eles sofridos; b) o caráter intencional ou negligente da infração; c) qualquer ação tomada pelo controlador ou processador para mitigar os danos sofridos pelos titulares dos dados; d) o grau de responsabilidade do responsável pelo tratamento ou do subcontratante, tendo em conta as medidas técnicas e organizacionais por eles implementadas nos termos dos artigos 25.º e 32.º; e) quaisquer infrações anteriores relevantes por parte do controlador ou processador; f) o grau de cooperação com a autoridade de supervisão, a fim de remediar a infração e mitigar os possíveis efeitos adversos da infração; g) as categorias de dados pessoais afetados pela infração; h) o modo como a infração foi tomada pelo conhecimento da autoridade de controlo, nomeadamente se, e em que medida, o responsável pelo tratamento ou o subcontratante notificou a infração; i) sempre que as medidas referidas no artigo 58.º, n.º 2, tenham sido anteriormente decretadas contra o responsável pelo tratamento ou o subcontratante em causa relativamente ao mesmo objeto, o cumprimento dessas medidas; j) adesão a códigos de conduta aprovados de acordo com o Artigo 40 ou mecanismos de certificação aprovados de acordo com o Artigo 42; k) qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como benefícios financeiros auferidos, ou perdas evitadas, direta ou indiretamente, com a infração.	Art. 52º § 1º: As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. Mesmo assim, existem semelhanças neste ponto entre as duas.

Multas Administrativas Pecuniárias para Órgãos e Organizações Públicas/Estatais	Art. 83, 7: Sem prejuízo dos poderes corretivos das autoridades de supervisão da união europeia, caberá a cada Estado-Membro estabelecer regras sobre em que medida podem ser aplicadas multas administrativas às autoridades e organismos públicos estabelecidos nesse Estado-Membro.	Diferente do regulamento europeu, é previsto na Lei brasileira que serão aplicadas as mesmas sanções a entidades e órgãos políticos, com exceção apenas das multas simples e das multas diárias (previstas nos incisos II e III). Ou seja, a esses sujeitos, diferente das pessoas jurídicas de natureza privada, não serão aplicadas sanções pecuniárias.

5.1.1 Principais impactos do GDPR para empresas que lidam com dados pessoais no seu primeiro ano de vigência

Na presente seção serão discutidos dados preliminares de pesquisas sobre os principais impactos do GDPR no seu primeiro ano de vigência. Através da análise de artigos que reuniram dados sobre a repercussão da entrada em vigor do regulamento europeu nos seguintes aspectos: o nível de conhecimento do regulamento e dos direitos à privacidade dos cidadãos que moram nos Países-Membro; o efeito sentido pelas empresas em relação ao compliance; a influência do GDPR para outros países e por fim, os consequências na publicidade *on line*.

Segundo Breitbartch (2019), nos primeiros meses da vigência do GDPR, a maioria das DPAs (*Data Protection Autorities*), localizadas em cada País-Membro, ofereceu orientação e aconselhamento às empresas que violavam o regulamento e à comunidade empresarial em geral. Essa atitude deu margem para que as organizações pudessem preencher as lacunas existentes nas suas organizações, as quais, mesmo após o prazo de 24 meses de adaptação dado pela União Europeia, não conseguiram ser preenchidas.

Segundo esse mesmo autor, passada essa primeira fase, houve um aumento da fiscalização por parte das DPAs. Aponta ele que “houve diversos exemplos de violações sancionadas no ano de 2018, que vão de multas de alto nível aplicadas a gigantes da *internet* até outros exemplos que envolvem organizações menores e menos conhecidas” (BREITBARTCH, 2019, p. 11,tradução minha)[63].

A fim de apontar as consequências do primeiro ano de vigência do GDPR, o Conselho Europeu de Proteção de Dados Pessoais, que é composto pela Autoridade Europeia para Proteção de Dados e os representantes locais de cada País-Membro, disponibilizou a primeira visão geral da implementação e aplicação do GDPR em fevereiro de 2019.

Breitbartch (*idem,* p. 12, tradução minha) aponta no seu texto as principais conclusões sobre o primeiro ano de aplicação do GDPR, segundo o relatório supracitado:

> Haviam 206.326 casos relatados das DPAs nos 31 países do espaço económico europeu durante seus primeiros 9 meses. Quase metade desses casos (99.622)

[63] We have seen numerous examples of contraventions being sanctioned in the past year, rang-ing from high-profile fines levied against Internet giants to other examples involving smaller, less well-known organisations.

> estavam relacionados a reclamações, sendo um quarto (64.684) relacionados a violações de dados específicos. [64]

Segundo o trecho acima, a maioria dos casos relatados às DPAs dos Países-Membros tratavam-se de queixas de usuários. Sendo um número significativo para o primeiro ano de exercício da lei, apontando o quanto era necessário existirem meios para que os titulares pudessem reclamar seus direitos.

A Comissão Europeia também divulgou em 2019 um relatório chamado de *Eurobarometer*, focalizando, entre outros temas, o conhecimento dos entrevistados sobre a autoridade pública nacional responsável pela proteção de seus direitos de dados pessoais, bem como o conhecimento do Regulamento Geral de Proteção de Dados (GDPR) e os direitos que ele garante. Foi concluído que:

> A maioria (67%) dos entrevistados já ouviu falar do GDPR, embora haja uma divisão bastante uniforme entre aqueles que já ouviram falar e sabem o que é (36%) e aqueles que ouviram falar, mas não sabem exatamente o que é (31%) Quase um terço (32%) nunca ouviu falar dele. A maioria dos entrevistados em todos os países, exceto dois, já ouviu falar do GDPR, embora as proporções variem de 90% na Suécia, 87% na Holanda e 86% na Polônia a 53% na Bélgica e 58% em Chipre e Estônia. As exceções são França (44%) e Itália (49%). Existem seis países onde pelo menos metade de todos os entrevistados já ouviu falar do GDPR e sabe o que é: Suécia (63%), Holanda (60%), Polônia (56%), Dinamarca (51%), Irlanda e República Tcheca (ambos 50%) [65] (EUROBAROMETER 487a, 2019, pp. 20 e 21, tradução minha).

De acordo com o referido relatório dentre os países membros da União Europeia, o que apresentou maior sensibilização para com o GDPR e o com a menor, são, respectivamente, a Suécia, com 90% da sua população tendo noção do

---

[64] The findings revealed that there were 206.326 cases reported from the DPAs in the 31 countries in the European Economic Area during the first nine months since the GDPR came into effect. Close to half of these cases (96,622) were related to complaints, while over a quarter (64.684) were related to specific data breaches.

[65] The majority (67%) of respondents have heard of GDPR, although there is a fairly even split between those who have heard of it and know what it is (36%) and those who have heard of it but don't know exactly what it is (31%)11. Almost one third (32%) have not heard of it. The majority of respondents in all but two countries have at least heard of the GDPR, although proportions range from 90% in Sweden, 87% in the Netherlands and 86% in Poland to 53% in Belgium, and 58% in Cyprus and Estonia. The exceptions are France (44%) and Italy (49%).There are six countries where at least half of all respondents have heard of GDPR and know what it is: Sweden (63%), the Netherlands (60%), Poland (56%), Denmark (51%), Ireland and Czechia (both 50%).

que é o regulamento e para o que ele serve, enquanto a França totaliza 44% da sua população declarando não conhecer o regulamento.

Ainda aponta o relatório que:

> A análise sociodemográfica revela que respondentes com idade entre 25-54 (75%) são os mais propensos a ter ouvido falar do GDPR - e particularmente de ter ouvido falar dele e saber o que é - em comparação com respondentes mais jovens (66%) e mais velhos (58%). Os gerentes (86%) são os que mais provavelmente já ouviram falar do GDPR, principalmente em comparação com os aposentados (55%). Quanto menos dificuldades financeiras um entrevistado tiver, maior será a probabilidade de ele ter ouvido falar do GDPR (e em particular de saber o que é). Por exemplo, 71% das pessoas que têm menos dificuldades para pagar as contas já ouviram falar do GDPR, em comparação com 49% das que têm mais dificuldades. Os usuários diários da Internet (75%) têm mais probabilidade de ter ouvido falar do GDPR do que aqueles que o usam com menos frequência (60%) ou que nunca o usam (39%). Na mesma linha, os entrevistados que fazem compras online regularmente (79%) têm mais probabilidade de ter ouvido falar do GDPR do que aqueles que o fazem com menos frequência (74%) ou nunca (61%). A análise também destaca que os entrevistados que alteraram as configurações de privacidade em seu (s) perfil (s) de rede social têm mais probabilidade de ter ouvido falar do GDPR do que aqueles que não o fizeram (80% vs 65%). Talvez não seja surpreendente que aqueles que dizem que sempre (84%) se sentem informados sobre as condições em que seus dados são coletados e usados têm mais probabilidade de ter ouvido falar do GDPR do que aqueles que dizem que isso só se aplica às vezes (77%), raramente (70 %) ou nunca (56%).[66] (EUROBAROMETER 487a, 2019, p.21, tradução minha)

[66]The socio-demographic analysis shows no difference based on gender, but does illustrate the following: Respondents aged 25-54 (75%) are the most likely to have heard of GDPR – and particularly to have heard of it and know what it is – compared to younger (66%) and older respondents (58%). Managers (86%) are the most likely to have heard of GDPR, particularly compared to retired persons (55%). The less financial difficulties a respondent experiences, the more likely they are to have heard of GDPR (and in particular to know what it is). For example, 71% of those who experience the least difficulties paying bills have heard of GDPR, compared to 49% of those who experience the most difficulties. Daily Internet users (75%) are more likely to have heard of GDPR than those who use it less frequently (60%) or who never use it (39%). In a similar vein, respondents who regularly shop online (79%) are more likely to have heard of GDPR than those who do so less frequently (74%) or never (61%). The analysis also highlights that respondents who have changed the privacy settings on their social network profile(s) are more likely to have heard of GDPR than those who have not (80% vs 65%). Perhaps not surprisingly, those who say they always (84%) feel informed about the conditions under which their data is collected and used are more likely to have heard of GDPR than those who say this only applies sometimes (77%), rarely (70%) or never (56%).

De acordo com os resultados do relatório supracitado, podem ser pontuados alguns aspectos. Primeiro, destacam-se como pessoas que têm conhecimento sobre o regulamento de proteção de dados pessoais, aquelas com maior poder de compra *on line*, pessoas que têm mais acesso à *internet* e também níveis mais alto de renda, o que indica que conhecimentos sobre direitos fundamentais, em especial sobre a privacidade e os meios para preservá-la precisam ser mais democráticos e atingir o tecido social em sua inteireza.

Em relação ao impacto para as empresas se adequarem ao GDPR no primeiro ano de vigência, o relatório acima citado aponta que os recursos financeiros são extremamente significativos para a entrada em conformidade com o regulamento europeu (BREITBARTH, 2019, p. 12). Isso se dá, por exemplo à alta demanda pela contratação de profissionais específicos para a adequação da empresa à norma.

Quando se fala dos impactos do GDPR, a primeira pauta levantada são as multas e as sanções. Porém, de acordo com o relatório da IAPP-EY (Relatório de Governança e Privacidade), divulgado após um ano de vigência do GDPR e comentado no texto de Breitbartch (*idem*), os principais impactos financeiros para as empresas foram com contratações:

> Cerca de 89% das empresas da UE afirmaram que nomearam um responsável pela proteção de dados em resposta ao GDPR, e reportam ter aumentado a sensibilização para as questões da proteção de dados. O progresso no *complience* (83%), violações de dados (68%) e iniciativas de privacidade (61%) são os principais itens da agenda entre as salas de reuniões, enquanto o investimento em treinamento está aumentando[67] (BREITBARTH, 2019, p. 12, tradução minha).

Além do investimento é profissionais específicos para a adequação, vimos acima que durante o primeiro ano de vigência do GDPR, 83% das empresas relataram progresso no *compliance* com o regulamento, 68% de diminuição de violação de dados.

[67] Tradução livre do texto: Some 89% of EU respondents to the survey stated that they have appointed a data protec-tion officer in response to the GDPR, while awareness on the issues of data protection has risen. Progress on compli-ance (83%), data breaches (68%) and on privacy initiatives (61%) feature highest on the agenda among boardrooms, while investment in training is on the rise. Nearly eight in 10 respondents noted training investments as their top GDPR compliance priority for the coming year

Ainda de acordo com o supracitado relatório, a pauta de iniciativas de privacidade tornou-se mais relevante, com 61% de presença nas salas de reunião.

Finalmente, “quase oito em cada 10 entrevistados observaram os investimentos em treinamento como sua principal prioridade de conformidade com o GDPR para os anos seguintes” (BREITBARTH, 2019, p. 12).

Sobre os impactos para a publicidade *on line*, é sabido que existem empresas que coletam dados analíticos, detalhados sobre como os usuários navegam e chegam até os *sites* da *web*. “anúncios personalizados são baseados em dados coletados por empresas sobre os usuários da internet, por meio de vários mecanismos como *cookies*[68] *http*[69]”(URBAN, TATANG *et al.,* 2019, n.p, tradução minha). Esses dados analíticos coletados resultam num ID, uma identidade/perfil única do titular dos dados, a qual ajuda a direcionar anúncios de acordo com as preferências descobertas (NEGRINI, 2017).

Na sua pesquisa sobre o tema, Urban, Tatang *et al*. (2019) observaram o comportamento de compartilhamento de informações entres serviço de anúncio online que captam dados através de *cookies*. Segundo eles, após o GDPR diminuiu o compartilhamento de ID de usuários:

> Observamos uma queda estatisticamente significativa nas conexões de compartilhamento de ID no ecossistema de publicidade online. É provável que a mudança esteja relacionada ao GDPR, que impôs regras mais rígidas sobre o compartilhamento de dados e permite que as autoridades de proteção de dados multem as empresas que não cumpram os requisitos [70](URBAN, TATANG *et al.,* 2019, n.p, tradução minha).

Segundo esses autores, os números de sincronização de ID diminuiu cerca de 40% a partir do momento que o GDPR entrou em vigor (URBAN, TATANG *et al*., 2019).

Segundo Goldeberg, Johnson e Shiver (2019, p. 24, tradução minha), que pesquisaram o impacto inicial do GDPR nos resultados de tráfego da web e comércio eletrônico na Europa,

---

[68] Cookies são: Pequenos arquivos de texto que sites de visitados podem guardar no computador do usuário. (Negrini: https://www.kaspersky.com.br/blog/internet-ads-103/7045/).

[69] Tradução Livre do texto: Personalized ads are based on data collected by ad companies about Internet users through various mechanisms, mainly HTTP cookies.

[70]We observed a statistically significant drop in ID sharing connections within the online advertising ecosystem. It is likely that the change is related to the GDPR, which imposed stricter rules on data sharing and allows data protection authorities to fine non-compliant companies.

> Os efeitos médios encontrados sobre as visualizações de páginas online caíram em 4% e a receita semanal em 8% (que corresponde a 8.000 EUR). O trabalho concluiu que, da perspectiva dos reguladores, é consequência do alto custo da entrada em conformidade com os termos de privacidade.[71]

Diante do exposto na literatura sobre os impactos do GDPR aqui brevemente analisados, entende-se que as empresas que lidam com compartilhamento de informações/dados privados sentiram o impacto devido aos esclarecimentos sobre o acesso a dados pessoais compartilhados online possibilitados pelo início da vigência da norma Europeia. A GPDR fez com que os usuários tivessem mais ciência da quantidade de dados pessoais que compartilham ao acessar determinado *website* ou aplicativo. O que gerou mais atenção ao aceitar os termos de uso, situação na qual o usuário muitas vezes deixou até de realizar os acessos. Como consequência, pode haver uma menor captação de dados pessoais quando comparado ao período anterior à norma.

Também é possível concluir que negócios *online* que lidam com os dados do titular têm encontram dificuldades para se adequar à norma, seja pelo tipo de negócio em si, ou pelos custos necessários para a adaptação aos termos de privacidade exigidos.

[71]We find large mean effects: page views per week drop by approximately 4% and revenue per week falls by 8%. These are economically large numbers, with a 8% revenue per week drop corresponding to a $8,000 drop in weekly revenue for the median RSID in our sample. We provide some evidence that these results are not driven by changes in user behavior directly. From a regulator's perspective the above results clearly illustrate the difficulty and high costs of privacy regulation.

5 RESULTADOS E DISCUSSÕES

O presente trabalho se propôs a analisar comparativamente os principais elementos da *General Data Protection Regulation* (GPDR/União Europeia, 2016, 679) e da Lei Geral de Proteção de Dados Pessoais (LGPD/Brasil/ Nº 13.709), focalizando na comparação entre as sanções de ambos os textos normativos e também nos impactos das sanções provocados pela lei europeia no seu primeiro ano de vigência.

Com o que foi analisado até aqui, conclui-se que a iniciativa da União Europeia, ao reformar suas diretrizes e unificar as normas sobre proteção de dados pessoais num só Regulamento válido para todos os Países-Membros, foi de extrema importância para desenvolvimento da economia do Bloco e também serviu como inspiração normativa para diversos lugares do mundo. Inclusive o Brasil, que em 2018 criou sua norma sobre o tema. A Lei Brasileira se inspirou em diversos aspectos da Europeia, dentre os principais o referente a ressignificação do consentimento. Que já existia, porém com o advento da Lei Nº 13.709/2018, foi direcionado especificamente ao compartilhamento de dados pessoais. Além disto, também foram incorporados para a norma de proteção de dados pessoais brasileira o diversos pontos, dentre eles, destacam-se a finalidade, a responsabilização dos agentes de tratamento, a necessidade de tratamentos diferentes para dados pessoais de natureza diversa e a iniciativa de criação de políticas públicas sobre a matéria.

Nas sanções também foi possível achar algumas semelhanças. Como a responsabilização do processador apenas quando houver culpa. O regulamento europeu se destaca pela classificação mais detalhada das multas pecuniárias, definidas de acordo com os níveis de gravidade da infração cometida. O que torna a aplicabilidade mais propensa a proporcionalidade entre infração e pena.

Ainda sobre as sanções, a norma brasileira deixa em aberto no texto definições importantes das penalidades. Sendo assim, caberá a Autoridade Nacional de Proteção de Dados a ponderação e definição do montante da multa equivalente a cada caso. Logo, a ANPD será responsável por aplicar as multas pecuniárias visando a equidade através da análise do caso concreto. Tal conduta adotada pela Lei 13.709/2018 pode ser positiva se bem administrada pela Autoridade nacional. Se a mesma concretizar um cenário no qual não sejam abertas brechas a impunidade

para com os Controladores e Processadores, que priorize a equidade ao lidar com empresas de médio e pequeno porte. Uma questão a ser destacada é o fato de que até o presente momento, mesmo a LGPD tendo entrado em vigor em agosto de 2020, até o presente momento no qual esse trabalho foi concluído, já tenha sido confirmada a primeira diretoria da ANPD pelo Senado, é considerável afirmar que após 24 (vinte quatro) meses de adaptação a LGPD (Lei Nº 13.709) a Autoridade nacional brasileira ainda está a passos lentos de se tornar um órgão em pleno funcionamento.

Sobre os impactos observados do GDPR no seu primeiro ano de vigência (2018-2019), pode-se apontar a atuação das Autoridades Nacionais comunitárias dos Países-Membro da União Europeia, que se fizeram muito presentes nos primeiros meses de implementação do Regulamento. As empresas da Europa sentiram dificuldades para se adequarem à norma, devido, principalmente, à questão financeira que é demandada. Os gastos para contratações de profissionais que ajudem na adequação das empresas se mostrou um dos maiores impeditivos à adaptação das companhias ao GDPR.

Até aqui, o presente trabalho buscou através da observação das sanções, de outros aspectos das normas referentes a proteção de dados pessoais da União Europeia e do Brasil e também dos impactos apresentados no primeiro ano de vigência do Regulamento europeu, traçar expectativas para a aplicabilidade e os possíveis impactos da LGPD, em vigor desde agosto de 2020.

Há, até o momento no qual essa monografia foi concluída, pesquisas nacionais em andamento que buscam estimar os impactos da LGPD e explorar a importância do papel da Autoridade Nacional. É sabido que no Direito, leva-se tempo para que sejam evidenciados os reais impactos de uma norma na sociedade. Porém, se tratando de matérias que implicam o Direito Digital, devido a sua ligação com às inovações tecnológicas, o mesmo deve procurar acompanhar as necessidades advindas das novas tecnologias.

Projetos que implicam em transformações institucionais enfrentam desafios. Por isso será necessário frisar o diálogo entre os diversos sujeitos envolvidos no tratamento dos dados pessoais: os controladores, processadores, empresas, órgãos públicos e o próprio titular dos dados .

Cabe reforçar a responsabilidade da Autoridade Nacional de preencher pontos pendentes na regulamentação (Lei Nº 13.709/2018) nos seus primeiros anos.

E buscar atender as demandas de interpretação que vários artigos do texto carregam. Para um exercício eficiente da ANPD, também é de extrema importância que ela consiga estabelecer sua autonomia para atuar de maneira justa e eficaz, porém trabalhar com a articulação entre os demais órgãos reguladores e sancionadores. A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709) é de extrema importância para o Brasil em vários aspectos. Tanto econômicos, como também na efetivação do direito à privacidade como um direito fundamental que deve ser garantido pelo poder público.

Por fim, Ao olhar para as semelhanças entre o regulamento europeu e a lei brasileira, e analisar o até aqui exposto, é possível deduzir que os impactos positivos do GDPR se deram em parte, por uma atuação presente e eficiente das autoridades nacionais de proteção de dados de cada um dos Países-Membros nos primeiros meses de vigência. Sendo assim, é possível afirmar que a atuação eficaz da ANPD, principalmente nos meses seguintes à entrada em vigor da LGPD (Lei Nº13.709), será muito significativa para a obtenção de resultados positivos na aplicabilidade da Lei.

REFERÊNCIAS

ACADEMY BY REAMP. **A evolução da propaganda e sua importância nos meios digitais**. Disponível em:<https://www.reamp.com.br/academy/2017/12/a-evolucao-da-propaganda-e-sua-importancia-nos-meios-digitais/> Acesso em: 22 de jun. de 2020.

BOBBIO, Noberto. **A era dos Direitos**. 7. ed. Rio de Janeiro: Elsevier, 2014.

BIONI, Bruno Ricardo**. Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed, Rio de Janeiro: Forense, 2020.

BRAIMIS, Daiana. Publicidade direcionada: o que é e como aplicá-la no e-commerce?.**E-goi**, 2018. Disponível em: <https://blog.e-goi.com/br/publicidade-direcionada-o-que-e-aplicar-ecommerce/L>. Acesso em: 25, jul de 2020.

BRANDEIS, Louis; WARREN, Samuel. The right to privacy. **Harvard Law Review,** v. 4, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 22, jul. de 2020.

BRASIL. **Constituição** da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 21, jul. de 2020.

BRASIL. **Lei Complementar** nº 166. Promulgada em 8 de abril de 2019. Disponivel em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm>. Acesso em: 02, out. de 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709. Promulgada em 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10, jun. de 2020.

BREITBARTH, Paul. *The impact of GDPR one year on*. *In:* **Network Security.** v. 2019. Publicada em julho de 2019.

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.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. 1 ed. Editora Zahar, 2003.

CANTO, A. P. DE LIMA; CAIO, G. R SATERO; VASCONCELOS, M. G DE CABRAL; BARBOSA, M. B. SABOYA; MELO, R. CORREA; HOLANDA YANNE. **O que estão fazendo com os meus dados?** :A importância da Lei Geral de proteção de dados pessoais. Editora SerifaFina. Recife, 2019. P. 31-41.

CANTON, F. Filho. As barreiras legais do vazamento de dados. **Conjur**, 2018. Disponível em: <https://www.conjur.com.br/2018-abr-24/fabio-canton-filho-barreiras-legais-vazamento-dados>. Acesso em: 14 de agosto de 2020.

CASAROTTO, Camila.Saiba o que é Publicidade, para que serve e como é a carreira do publicitário. *In*: **ROCKCONTENT**, 2019. Disponível em: <https://rockcontent.com/br/blog/publicidade/>. Acesso em: 20, jul. de 2020.

CÓDIGO DE DEFESA DO CONSUMIDOR. Lei 8.078 de 11/09/90. Brasília, Diário Oficial da União, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 25, jul. de 2020.

CHUL-HAN, Byung. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Porto Alegre – RS: Editora ÂYNÉ, 2018.

DIÁZ, Efrén. The new European Union General Regulation on Data Protection and the legal consequences. *In:* ***Church, Communication and Culture***, 1:1, 2016, pp. 206-239.

DETAILS OF TREATY Nº108. **COUNCIL OF EUROPE**, 2020. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 12, outubro de 2020.

HAMANN, Renan. Do bit ao Yottabyte: conheça os tamanhos dos arquivos digitais. **Tecmundo**, 2011. Disponível em: <https://www.tecmundo.com.br/infografico/10187-do-bit-ao-yottabyte-conheca-os-tamanhos-dos-arquivos-digitais-infografico-.htm >. 2 de outubro de 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL]*, *12*(2), 91-108. 2011. Recuperado de https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. [tradução de Raquel Ramalhete]. Petrópolis: Vozes, 1987.

GOLDBERG, Samuel; JOHNSON, Garrett e SHRIVE, Scott. Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes (July 17, 2019). Available at SSRN: https://ssrn.com/abstract=3421731 or http://dx.doi.org/10.2139/ssrn.3421731

LIMA, Marina. Titular, Operador e Controlador – o que isso quer dizer?. **Tripla**, 2020. Disponível em: <https://triplait.com/titular-operador-e-controlador/>. Acesso em: 5, outubro de 2020.

MAGRINI, Eduardo. **Entre dados e robôs:** Ética e privacidade na era da Hiperconectividade. Porto Alegre – RS: Editora Arquipélago. 2019.

NASCIMENTO, Rodrigo. O que, de fato, é internet das coisas e que revolução ela pode trazer?. **COMPUTERWORLD**, 2015. Disponível em: <https://computerworld.com.br/negocios/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/>. Acesso em: 15 de agosto de 2020.

NASCIMENTO, Rodrigo. Afinal, o que é Big Data? *In:* ***Marketing*** **por Dados**, 2017. Disponível em: <http://marketingpordados.com/analise-de-dados/o-que-e-big-data-%F0%9F%A4%96/>. Acesso em: 17 de agosto de 2020.

NEGRINI, Flavio. Sorria, você está sendo monitorado pela propaganda online. KASPERSKY DAILY. 2017. Disponível em: <https://www.kaspersky.com.br/blog/internet-ads-103/7045/>. Acesso em: 02 de novembro de 2020.

PADILHA, T. M. e GARNIER, C. M. Ética, privacidade e novas tecnologias: o impacto da lei de proteção de dados na sociedade. *In:* **MIGALHAS**, 2019. Disponível em: <https://migalhas.uol.com.br/depeso/311142/etica-privacidade-e-novas-tecnologias-o-impacto-da-lei-de-protecao-de-dados-na-sociedade>. Acesso em: 8, jun. de 2020.

RAMOS, P. H. Soares. Publicidade em tempos de LGPD. **Meio e Mensagem**, 2019. Disponível em: <https://www.meioemensagem.com.br/home/opiniao/2019/10/30/a-publicidade-em-tempos-de-lgpd.html>. Acesso em: 10 de agosto de 2020.

SALDANHA, C. P.M. **O que estão fazendo com meus dados?** a importância da Lei Geral de Proteção de Dados.1. ed. Recife: SerifaFina, 2019.

SETA, Paduan. LGPD – O que é o Direito à Portabilidade de Dados?. **JusBrasil**, 2019. Disponível em: <https://paduanseta.jusbrasil.com.br/artigos/776530958/lgpd-o-que-e-o-direito-a-portabilidade-de-dados>. Acesso em: 15, outubro de 2020.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25. ed. São Paulo: Malheiras Editores LTDA, 2005.

SHERR, Ian. *Facebook, Cambridge Analytica and data mining: What you need to know***.** **CNET**, 2018. Disponível em: <https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/>. Acesso em: 15, setembro de 2020.

SNOWDEN, Edward. **Sem lugar para se esconder**: a NSA e a espionagem do governo americano. 1. ed. Nova York: LCC, 2014.

STEIN, Thaís. Timeline. **Dicionário Popular**, 2019. Disponível em: <https://www.dicionariopopular.com/timeline/>. Acesso em: 3, outubro de 2020.

REZENDE, Eliana. Dados informação e conhecimento. **ER Consultoria: Gestão de Informação e Memória Institucional**, 2015. Disponivel em: <https://eliana-rezende.com.br/dados-informacao-e-conhecimento-o-que-sao/>. Acesso em 02 de agosto de 2020.

TORRES, Cláudio. **A Bíblia do Marketing Digital**: tudo que você queria saber sobre *marketing* na internet e não tinha a quem perguntar. São Paulo: NOVATEC, 2018.

UNIÃO EUROPEIA. **Regulation (EU) on the protection of natural persons ith regard to the processing of personal data and on the free movement of such data.** Nº 679. Promulgada pelo Parlamento Europeu e Consulado dia 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 15, jun. de 2020.

URBAN, Tobias & TATANG, Dennis & DEGELING, Martin & POHL, Nobert. *Measuring the Impact of the GDPR on Data Sharing in Ad Networks*., 2020 [10.1145/3320269.3372194].

IBGE. **O Uso da internet**. 4. ed. São Paulo: Novatec editora LTDA: 2011

IBGE. Televisão e celular no Brasil. *In:* **IBGE Educa**, 2018. Disponível em: <https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html>. Acesso em: 22, junho de 2020.

VENOSA, S. D. S. **Direito Civil**: Parte Geral. 13. ed. São Paulo, Atlas, 2013.

487a. General Data Protection Regulation - 487b. Charter of Fundamental Rights. 487. Publicado em maio de 2019. Disponível em: <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222>. Acesso em: 10 de junho de 2020.