PONTIFÍCIA DA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

ANÁLISE COMPARADA ENTRE AS LEIS DE PROTEÇÃO DE DADOS DO BRASIL E DA UNIÃO EUROPEIA E SEUS RESPECTIVOS INSTRUMENTOS DE EXECUÇÃO

ORIENTANDA: ELISA FRIAÇA BALBINO

ORIENTADOR: PROF. DR. FAUSTO MENDANHA GONZAGA

GOIÂNIA-GO

2022

ELISA FRIAÇA BALBINO

ANÁLISE COMPARADA ENTRE AS LEIS DE PROTEÇÃO DE DADOS DO BRASIL E DA UNIÃO EUROPEIA E SEUS RESPECTIVOS INSTRUMENTOS DE EXECUÇÃO

Artigo Científico apresentado à disciplina de Trabalho de Curso I, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás. Prof. Orientador: Dr. Fausto Mendanha Gonzaga.

GOIÂNIA-GO

2022

ELISA FRIAÇA BALBINO

ANÁLISE COMPARADA ENTRE AS LEIS DE PROTEÇÃO DE DADOS DO BRASIL E DA UNIÃO EUROPEIA E SEUS RESPECTIVOS INSTRUMENTOS DE EXECUÇÃO

Data da Defesa:_____de_____de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. Fausto Mendanha Gonzaga Nota

_____

Examinador (a) Convidado (a): Prof. (a) Altamir Rodrigues Vieira Junior Nota

ANÁLISE COMPARADA ENTRE AS LEIS DE PROTEÇÃO DE DADOS DO BRASIL E DA UNIÃO EUROPEIA E SEUS RESPECTIVOS INSTRUMENTOS DE EXECUÇÃO

Elisa Friaça Balbino[1]

Com a evolução tecnológica, a troca e o armazenamento de informações ficou cada vez mais eficaz e ilimitado. Paralelamente, essa evolução trouxe novos desafios no âmbito jurídico, posto que a legislação já não resolvia os atuais conflitos. Nesse sentido, o presente artigo buscou apresentar um panorama geral sobre como foi desenvolvida as normas de conteúdo digital da União Europeia e do Brasil, com ênfase na legislação sobre proteção de dados pessoais, conhecidas como Regulamento Geral sobre Proteção de Dados (GDPR, em inglês) e Lei Geral de Proteção de Dados Pessoais (LGPD), respectivamente, realizando, assim, uma análise comparativa entre os regulamentos mencionados, destacando pontos convergentes e divergentes, ademais, demonstrando os seus instrumentos de aplicação. Outrossim, buscou-se ressaltar a importância da existência de tais dispositivos legais para transformar o mundo virtual em um ambiente seguro e democrático.

Palavras-chave: Dados pessoais; LGPD; GDPR; instrumentos de aplicação; União Europeia; Brasil.

SUMÁRIO

INTRODUÇÃO

Com a evolução da Internet, as relações humanas-tecnológicas se modificaram, uma vez que se democratizou o acesso à informação e à conectividade entre as pessoas. Hodiernamente, a internet é o principal meio de trocas de informações. Com isso, trouxe consigo novos desafios no âmbito jurídico para garantir segurança nas interações virtuais, estabelecendo direitos e obrigações por meio de regulamentações nacionais. Dessa forma, as leis sobre dados pessoais, presentes na interação virtual, tornaram-se cada vez mais necessárias para garantir a proteção dos titulares desses dados.

Em 2016, o *Facebook Inc.*, como era conhecido nesta época, um conglomerado de tecnologia e mídia social, vazou mais de 50 milhões de dados de seus usuários, sem o consentimento destes, pautado por uma brecha em sua política de dados. Essas informações foram utilizadas pela empresa de análise de dados *Cambrigde Analytica*, sendo que esta foi contratada pela campanha de Donald Trump nas eleições presidenciais deste mesmo ano e por uma empresa pró-*Brexit*. O impacto do trabalho realizado pela empresa de análise de dados refletiu nos resultados da eleição, com a vitória de Trump e a saída do Reino Unido da União Europeia. Desse modo, esse vazamento acabou por levar os Estados Nacionais a agilizassem a produção ou reformulação de uma legislação mais completa e minuciosa sobre o uso de dados, a fim de proteger de maneira mais ampla os dados e seus titulares.

Em 2012, a Regulamentação Geral de Proteção de Dados da União Europeia (GDPR, em inglês) foi proposta no Parlamento Europeu. Com o vazamento do *Facebook*, o Parlamento Europeu acelerou a aprovação da regulamentação e tornou-se a primeira lei de proteção de dados, servindo de modelo para outros países. Já no Brasil, em 2015, houve um debate público sobre o tema que resultou na elaboração do Anteprojeto de Lei de Proteção de Dados Pessoais. Em 2018, após o escândalo acima referido, o anteprojeto virou o Projeto de Lei da Câmara 53/2018 e, em agosto daquele mesmo ano, foi sancionado como Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD).

Portanto, tendo em vista que é um assunto recente e imprescindível, a presente pesquisa busca fazer uma breve análise comparada entre as leis de proteção de

dados do Brasil e da União Europeia, buscando demonstrar pontos de convergência e divergência entre elas, destacando os instrumentos de controle da aplicação das normas, com base em análises documentais das respectivas leis e artigos explicativos sobre o assunto.

1 ASPECTOS GERAIS DAS LEIS DE PROTEÇÃO DE DADOS (GDPR E LGPD)

Em 1981, na Europa, a Convenção 108/Conselho Europeu (CE) foi a primeira regulação transversal que estipulou um regime de governança para questões de proteção de dados pessoais. Em 1995, a Diretiva 95/46/CE foi implementada, dando uma aprofundada sobre o tratamento da matéria, estabelecendo diretrizes à proteção de dados entre os Estados-membros. Após a diretiva de 1995, seguiram outras diretivas adjacentes, como a Diretiva 2002/58/CE (única ainda em vigor) e a Diretiva de 2006/24/CE, versava sobre a proteção de dados em comunicação eletrônica.

Em pouco tempo, a internet passou a conectar bilhões de pessoas ao redor do mundo de uma forma nunca vista antes, a qual recolheu excepcional quantidade de dados. Assim, com o crescimento exponencial na complexidade do uso da internet, tornou-se necessária uma regulamentação que atendesse esses desafios. Em 2012, a *General Data Protection Regulation* (GDPR) foi proposta, levando quatro anos para ser elaborada, contando com 99 capítulos seu corpo de texto. Com o prazo de dois anos para que os setores públicos e privados se adaptassem a norma, sua vigência se deu em maio de 2018.

Já no Brasil, somente em 2009, o primeiro projeto de regulamentação envolvendo o mundo online, conhecido como Marco Civil da Internet, começou a ser elaborado pelo Ministério da Justiça em colaboração com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, bem como a participação direta da sociedade civil. Em 2011, o projeto foi encaminhado ao Congresso Nacional, como PL 2126/2011, mas somente em 2014, que o Marco Civil da Internet foi transformado em lei. Em seu corpo textual, essa legislação não possuía o foco em dados pessoais, no entanto, foi o primeiro na delimitação de direitos e deveres na Internet. No final de 2010, começaram a surgir propostas sobre a criação de uma regulamentação

específica sobre atividades envolvendo o uso e o armazenamento de dados pessoais. Com isso, em 2015, o Governo Federal realizou um debate público sobre o tema, resultando na elaboração do primeiro Anteprojeto de Lei de Proteção de Dados Pessoais. Em 2018, o então anteprojeto virou o Projeto de Lei 53/2018 da Câmara, e, em agosto, foi sancionado como Lei nº 13.709/2018, todavia, somente entrou em vigência em sua totalidade em agosto de 2021.

Em síntese, nota-se que as diretivas da União Europeia já tratavam sobre dados pessoais em comunicação eletrônica desde 1981, enquanto, no Brasil, o assunto foi tratado apenas em 2014, com o Marco Civil da Internet. Além disso, a GDPR e a LGPD tiveram seu sancionamento e vigência muito próximas.

2 CONVERGÊNCIA ENTRE AS LEGISLAÇÕES ANALISADAS

Um dos pontos fundamentais deste artigo é apresentar as semelhanças entre as legislações LGPD e GDPR para demonstrar que cada dispositivo legal possuem a mesma finalidade: proteção de dados pessoais. Para isso, será utilizado o método dedutivo para realizar a comparação entre as normas, tendo como foco as suas similaridades.

2.1 APLICAÇÃO DO PRINCÍPIO DA EXTRATERRITORIALIDADE

Ambas as normas aplicam o princípio da extraterritorialidade, isto é, são aplicáveis as entidades e organizações que estejam presente em seu território de jurisdição ou que utilizem dados de indivíduos pertencentes à UE e Brasil. Na GDPR, esse princípio se encontra no art. 4º, nos seguintes termos:

> qualquer operação ou conjunto de operações executadas com dados pessoais ou com conjuntos de dados pessoais, independentemente de serem automatizados, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição;

Na LGPD, encontra-se em seu art. 3º, na seguinte redação:

> Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - a operação de tratamento seja realizada no território nacional;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

2.2 DADO PESSOAL

A definição de dado pessoal é a mesma nos dois dispositivos legais, sendo que se refere a qualquer informação de uma pessoa natural identificada ou identificável (titular dos dados), excluindo-se de suas aplicações o tratamento de dados anônimos, a não ser que o processo de anonimização possa ser revertido.

Vale ressaltar que “por qualquer informação” significa literalmente qualquer informação que possa ser utilizada para identificar inequivocamente um indivíduo, seja direta ou indiretamente, podendo ser o dado físico ou virtual. Desse modo, essa definição dinamiza a legislação, uma vez que essa característica expansionista dificulta a obsolescência da norma em meio às mudanças sociais e desenvolvimento tecnológico.

2.3 AUTORIDADE NACIONAL

As legislações analisadas preveem o estabelecimento de uma autoridade nacional para supervisionar as atividades do tratamento de dados realizados por pessoas física ou jurídica, com poderes investigativos, consultivos e punitivos. Na LGPD, a autoridade nacional é referida como Autoridade Nacional de Proteção de Dados (ANPD), já na GDPR é a Autoridade de Controle Independente.

Em ambos diplomas legais, a autoridade nacional tem o caráter investigativo, podendo exigir que o controlador e o operador forneçam as informações necessárias para que a investigação seja feita. Além disso, caráter consultivo refere-se ao dever

de tratar as reclamações apresentadas pelos titulares dos dados e de cooperar com as autoridades de proteção de dados de outro país. Outrossim, possui poder punitivo, uma vez que podem emitir advertências, multas e bloqueio ou eliminação do tratamento ou dos dados pessoais a que se referem a infração.

2.4 DADOS ANÔNIMOS

Tanto na GDPR quanto na LGPD, dado anônimo é aquele que não se relaciona a uma pessoa natural identificada ou identificável.

2.5 TITULARIDADE DE PESSOAS NATURAIS

Ambas legislações definem como titular de dados pessoais somente as pessoas naturais, excluindo-se as pessoas jurídicas.

2.6 DADOS ESPECIAIS OU SENSÍVEIS

Dentre os dados passíveis de tratamento, tem-se os dados especiais ou sensíveis. Na GDPR, esses dados são chamados de sensíveis, já na LGPD, podem ser chamados tanto um como o outro. Esses dados em questão são aqueles relativos a origem étnica, ideologia política, crença religiosa ou filosófica, filiação em sindicatos, dados genéticos, dados biométricos, dados de imagens, ou seja, são todos aqueles que tem por objetivo identificar exclusivamente uma pessoa natural.

2.7 AGENTES DA LEI

Na GDPR, os agentes da lei são o responsável pelo tratamento (*Controller*), o subcontratante (*Processor*) e o encarregado da proteção de dados (*Data Protection Officer* ou DPO). Na LGPD, o primeiro é chamado de controlador, o segundo é equivalente ao operador e o terceiro é o mesmo do diploma legal europeu.

O controlador ou responsável pelo tratamento é a pessoa natural ou jurídica, de direito público ou privado, a quem compete decidir pelo tratamento de dados e os

procedimentos a serem adotados. Outrossim, o controlador/responsável pelo tratamento possui a obrigação de manter os registros de suas atividades de tratamento de dados que realizam.

O subcontratante ou operador de dados é a pessoas natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do responsável pelo tratamento ou controlador. Assim, o subcontratante/operador tem a liberdade de escolher os meios de tratamento de dados pessoas, por meio de autorização tácita ou expressa do responsável. Ademais, o operador tem a obrigação de manter registro das atividades de tratamento de dados que realizam.

O encarregado (DPO) é aquele que tem o papel de garantir que a organização trate os dados pessoais de seus funcionários, clientes, fornecedores ou qualquer outro titular de dados em conformidade com a norma, devendo ser indicado tanto pelo responsável pelo tratamento quanto pelo subcontratante. Vale ressaltar que o DPO é parte integrante da organização. No entanto, deve ser capaz de desempenhar suas funções de forma independente. O encarregado atua como canal de comunicação entre o controlador e os titulares dos dados e a autoridade nacional local.

2.8 TRATAMENTO DE DADOS

Em ambas legislações, o conceito tratamento de dados são similares. Na GDPR, o tratamento de dados, segundo seu art. 4º, nº 2º e considerando 15, corresponde:

> a qualquer operação realizada em dados pessoais, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou de outra forma disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

Já na LGPD, o tratamento de dados, em seu art. 5º, inciso X, se define como:

> coleta, produção, recebimento, classificação, uso, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, exclusão, avaliação ou controle da informação, modificação, comunicação, transferência, disseminação ou extração.

2.9 CONCLUSÃO DA CONVERGÊNCIA

Com os dados acima exposto, percebem-se vários pontos de convergência entre o Regulamento Europeu e a Lei Brasileira. Em destaque, o objetivo dos dispositivos legais – proteção de dados pessoais –; os conceitos de dados pessoais, dados anônimos, dados especiais ou sensíveis e o tratamento de dados; a aplicação do princípio da extraterritorialidade; a titularidade de pessoa natural; os agentes da lei; a definição da autoridade nacional e suas funções.

3 DIVERGÊNCIAS ENTRE LGPD E GDPR

Após o destaque das semelhanças entre LGPD e GDPR, cabe analisar os pontos diferentes entre ambos. Nesta seção, será utilizada a mesma metodologia da anterior: o método dedutivo.

3.1 PRINCÍPIOS PRIMORDIAIS ESPECÍFICOS

O GDPR estabelece seis princípios de tratamento, sendo eles: licitude, lealdade e transparência; limitação das finalidades e da conservação; minimização dos dados; exatidão; integridade e confidencialidade; e responsabilidade. Em contraposição, a LGPD define dez princípios primordiais: a finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilidade.

3.2 UTILIZAÇÃO DE DADOS PESSOAIS NA SAÚDE PÚBLICA

Na LGPD, é prevista a possibilidade de se utilizar dos dados pessoais para auxiliar nos estudos e pesquisas para saúde pública, autorizando que entidades de investigação científica possam fazer o uso desses dados pessoais, exclusivamente dentro da entidade e estritamente para efeitos de realização desses estudos cujo objeto é a saúde pública. Além disso, o tratamento de dados deve ser realizado em um ambiente controlado e seguro, devendo, sempre que possível, preservar a anonimização dos dados. Já no GDPR, essa possiblidade não é prevista.

3.3 RESPONSABILIDADE SOLIDÁRIA

O Regulamento Europeu 2016/679 não aborda a responsabilidade solidária entre o responsável pelo tratamento e pelo subcontratante. No entanto, isto não quer dizer que não possa ser estabelecida no contrato a ser firmado entre ambos. Note que o conceito de operador remete a ideia de delegação, assim, a sua atuação é limitada, visto que deve seguir as instruções do controlador. Caso não siga, os prejuízos causados pelo não cumprimento das instruções poderá recair sobre o operador.

Em contraposição, a LGPD prevê a responsabilidade solidária entre o controlador e o operador no tratamento de dados, estabelecendo, incluindo, a possibilidade de reparação dos dados patrimonial, moral, individual ou coletivo, principalmente quando se tratar de atendimento ao consumidor por força da aplicação do Código de Defesa do Consumidor (Lei nº 8.078/1990).

3.4 OBRIGATORIEDADE DE CONTRATO ENTRE O CONTROLADOR/RESPONSÁVEL PELOS DADOS E O OPERADOR DE DADOS/SUBCONTRATANTE

Conforme os termos do GDPR, a relação entre o controlador e o operador de dados deve ser regido por um contrato ou outro ato jurídico, que vincule o responsável pelo tratamento ao subcontratante, devendo apresentar o seguinte: o objeto e duração do contrato; natureza e finalidade do tratamento; tipo de dado pessoal e categoria de titulares envolvidos; obrigação do subcontratante de só tratar os dados pessoais de acordo com as orientações e autorizações expressas do responsável; garantia, pelo subcontratante, de que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade; garantia, pelo subcontratante, de adoção de medidas de segurança adequadas; obrigação do subcontratante de só contratar outro subcontratante mediante autorização prévia e escrita do responsável; obrigação do subcontratante de cooperar com o responsável pelo tratamento no atendimento de solicitações dos titulares de dados que queiram exercem os seus direitos; obrigação do subcontratante em prestar assistência ao responsável pelo tratamento no cumprimento das suas obrigações relativas à segurança do processamento, à notificação de violações de dados pessoais e às avaliações de impacto à proteção de

dados; obrigação do subcontratante de, ao final do contrato entre as partes, a depender da escolha do responsável, excluir ou devolver os dados que haviam sido comunicados em razão da contratação; obrigação do subcontratante de disponibilizar ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações assumidas e contribuir para as auditorias, inclusive, as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

Por outro lado, a LGPD não estabelece a obrigatoriedade da celebração de contrato ou outro ato jurídico equivalente que vincule o controlador e o operador ao tratamento de dados. Somente afirma que o operador deve seguir o tratamento de dados de acordo com as instruções fornecidas pelo controlador.

3.5 CONCLUSÃO DA DIVERGÊNCIA

Pelo que nos é possível observar na presente seção, as divergências principais entre o GDPR e a LGPD, se manifestam essencialmente nos seguintes pontos: os princípios primordiais específicos; a utilização de dados pessoais na saúde pública; a responsabilidade solidária entre o responsável pelo tratamento de dados e o subcontratante; e a obrigatoriedade de contrato entre o controlador e o operador.

4 INSTRUMENTOS DE *ENFORCEMENTS* DA LGPD E DA GDPR

Como já foi mencionado, o GDPR impõe a condição que os países possuam uma legislação abrangente e completa sobre proteção de dados e uma autoridade reguladora para garantir sua eficácia para os países que desejarem manter relações comerciais com EU. Isso é um instrumento de aplicação, visto que o GDPR conta com o peso da União Europeia no comércio internacional para instituir a obrigação dos outros países se atentarem quanto ao direito de privacidade e transparência no tratamento de dados pessoais.

Outro instrumento de *enforcement* é a criação de um cargo, tanto em empresas privadas quanto em órgão públicos, o chamado Diretor de Proteção de Dados (DPO), que é responsável por supervisionar as operações envolvendo os dados pessoais,

garantindo constantemente a conformidade com a lei. Da mesma forma, a LGPD prevê que as empresas tenham um encarregado pelo tratamento de dados, sua principal função é prestar esclarecimentos para as autoridades governamentais e tomar providências sobre a adequação dos processos institucionais e garantir o cumprimento da legislação. Desse modo, o encarregado é um instrumento de aplicação, posto que é o intermediário entre os titulares dos dados, as empresas e a Autoridade Nacional de Proteção de Dados (ANPD).

O principal instrumento de aplicação da LGPD é a ANPD, sendo que é a autoridade suprema de fiscalização do cumprimento da lei, caso necessário tem o poder de aplicar sanções pelo descumprimento. Já no GDPR, o regulamento delegou as mesmas funções ao *Data Protection Authority* (DPA, em português, Autoridade de Proteção de Dados) que cada Estado membro deve ter. Assim, cada país integrante da UE é responsável por selecionar o conselho que formará a autoridade reguladora, indicando, também os poderes garantidos à mesma, uma vez que cada país-membro possui leis nacionais sobre o assunto.

Outrossim, o GDPR criou o *European Data Protection Board* (EDPB, Conselho Europeu para a Proteção de Dados, em português) que é um organismo independente cujo objetivo é promover a cooperação e o intercâmbio eficaz de informações entre as DPA's de cada país-membro. Esse organismo é composto por representantes das DPA's e pelo *European Data Protection Supervisor* (EDPS, Autoridade Europeia para a Proteção de Dados, em português). De acordo com a Comissão Europeia, o EDPB tem como uma de suas funções fundamentais "governar por decisões vinculativas sobre disputas relacionadas ao processamento transfronteiriço, garantindo uma aplicação uniforme das regras na UE para evitar que o mesmo caso possa ser tratado diferente em várias jurisdições". Desse modo, o EDPF se torna relevante no que representa para à transferência eficiente de dados e à aplicação uniforme de decisões no bloco europeu.

Em suma, os instrumentos coincidentes de execução das legislações europeia e brasileira consistem basicamente no seguinte: necessária criação do cargo do Diretor de Proteção de Dados, que é responsável por intermediar os titulares dos dados, a empresa e a Autoridade Nacional de Proteção de Dados; criação da autoridade nacional responsável por fiscalizar se as empresas estão cumprindo as

normas de proteção de dados, punir aquelas que não cumprem e orientar as empresas sobre a lei em questão e aplicação da mesma. Além disso, a regulamentação europeia possui dois instrumentos de aplicação diferentes da lei brasileira, sendo eles a imposição de que países que queiram negociar com a União Europeia tenham uma legislação completa e ampla de proteção de dados e, além da criação de uma autoridade nacional, por ser um bloco econômico composto por vários países, criou um organismo independente com a função de promover cooperação e intercâmbio de informações entre as autoridades nacionais de cada Estado-membro.

CONCLUSÃO

Como já foi mencionado, no século XX, num ritmo colossal, a informação passou a ser transmitida e armazenada por meios cada vez mais eficientes, tendo como destaque a internet. Com isso, as normas ficaram obsoletas, pois já não resolviam os conflitos que começaram a surgir, resultando em um processo de aceleração na criação e aprovação de legislações de proteção de dados pessoais. A GDPR é a legislação pioneira que tratou especificamente sobre dados pessoais no mundo, inspirando outros países a seguirem o mesmo caminho – a exemplo do Brasil que, em 2018, também promulgou a sua regulação de proteção de dados pessoais. Tendo em vista, as legislações mencionadas, esta pesquisa procurou apresentar os pontos de convergência e divergência entre ambas (GDPR e LGPD), fazendo, ainda, o cotejamento entre seus instrumentos de execução.

Após a análise comparativa dos dois sistemas de proteção de dados pessoais, a conclusão que chegou foi que ambos buscam o aprimoramento de mecanismos que possam tutelar o mesmo bem jurídico, que não é outro, senão, a incolumidade dos dados pessoais.

COMPARATIVE ANALYSIS OF PERSONAL DATA IN BRAZIL AND EUROPE UNION E THEIRS ENFORCEMENT INSTRUMENTS

ABSTRACT

Keywords:

REFERÊNCIAS

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#:~:text=Art.%201%C2%BA%20Esta%20Lei%20disp%C3%B5e,da%20personalidade%20da%20pessoa%20natural. Acesso em: 17 mar. 2021.

CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais**: Uma análise comparativa dos quadros regulatórios brasileiro e europeu. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Pernambuco — UFPE- Recife, 2018. Disponível em: < https://repositorio.ufpe.br/handle/123456789/34357>. Acesso em: 18 mar. 2022.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3ª. ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN COMISSION. **What is the European Data Protection Board (EDPB)?** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and- -organisations/enforcement-and-sanctions/enforcement/what-european-data-protection- -board-edpb_en>. Acesso em: 25. Ago. 2022.

INCE. **Enforcement of the GDPR**. Disponível em: https://www.incegd.com/en/knowledge- -bank/enforcement-of-the-gdpr. Acesso em: 25. ago. 2022.

LORENZON, Laila Neves. **Análise comparada entre regulamentação de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos intrumentos de enforcement**. Revista do Centro de Excelência Jean Monnet da FGV Direito Rio, Rio de Janeiro, vol. 1, p. 39-52, mar. de 2021. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423. Acesso em: 18 mar. 2022.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Comentários ao GDPR**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 111-123.

NEVES, Rebeca de Aguilar Pereira. **GDPR e LGPD: Estudo comparativo**. 2021. Monografia; graduação em direito na UNICEUB. Brasília, 2021. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/15239. Acesso em: 18 mar. 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 18. mar. 2022.