UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

PATRÍCIA MILANO VAZ

AS REGRAS DE BOAS PRÁTICAS E GOVERNANÇA DAS POLÍTICAS DE PRIVACIDADE DAS DISTRIBUIDORAS DE GÁS NATURAL DE ACORDO COM O ART. 50 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Porto Alegre
2021

PATRÍCIA MILANO VAZ

AS REGRAS DE BOAS PRÁTICAS E GOVERNANÇA DAS POLÍTICAS DE PRIVACIDADE DAS DISTRIBUIDORAS DE GÁS NATURAL DE ACORDO COM O ART. 50 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Trabalho de conclusão de curso de Especialização apresentado ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Especialista em Administração Pública no Século 21.

Orientador: Prof. Dr. Ariel Behr

Porto Alegre
2021

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

CIP - Catalogação na Publicação
Milano Vaz, Patrícia
AS REGRAS DE BOAS PRÁTICAS E GOVERNANÇA DAS POLÍTICAS DE PRIVACIDADE DAS DISTRIBUIDORAS DE GÁS NATURAL DE ACORDO COM O ART. 50 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS / Patrícia Milano Vaz. -- 2021.
78 f.

Orientador: ARIEL BEHR.

Trabalho de conclusão de curso (Especialização) -- Universidade Federal do Rio Grande do Sul, Escola de Administração, ADMINISTRAÇÃO PÚBLICA PARA O SÉCULO XXI, Porto Alegre, BR-RS, 2021.

1. LEI GERAL DE PROTEÇÃO DE DADOS. 2. GOVERNANÇA E CONFORMIDADE. 3. GÁS NATURAL. I. BEHR, ARIEL, orient. II. Título.

Elaborado pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pela autora.

PATRÍCIA MILANO VAZ

AS REGRAS DE BOAS PRÁTICAS E GOVERNANÇA DAS POLÍTICAS DE PRIVACIDADE DAS DISTRIBUIDORAS DE GÁS NATURAL DE ACORDO COM O ART. 50 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Trabalho de conclusão de curso de Especialização apresentado ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Especialista em Administração Pública no Século 21.

Aprovada em _____ de _____ de 2021

Banca Examinadora

_____

Examinador (a): Prof. Dr. Everton da Silveira Farias

_____

Examinador (a): Profa. Dra. Fernanda da Silva Momo

_____

Orientador: Prof. Dr. Ariel Behr

RESUMO

Este artigo teve como objetivo examinar as Políticas de Privacidade das distribuidoras de gás natural canalizado na hipótese referente à observação das boas práticas previstas no art. 50 da Lei Geral de Proteção de Dados. Para tanto, analisou-se, forma qualiquantitativa, 12 empresas distribuidoras de gás, que constituíram a amostra desta pesquisa. Buscou-se traduzir, em números, o nível de adequação às boas práticas de proteção de dados, utilizando-se, igualmente, a abordagem descritiva dos itens examinados, estabelecendo-se uma relação entre as variáveis fixadas para análise encontradas na legislação, os achados na amostra e as referências apresentadas. Todos os dados coletados são públicos e estão disponíveis no *website* das empresas analisadas, no *link* Política de Privacidade, o que permite se caracterizar este estudo como documental. O referencial teórico utilizou casos paradigmas, decisões de autoridades nacionais de dados e referências documentais que abordam o tema em estudo. Analisando-se os resultados, é possível observar que a amostra detém preocupação para aplicar as boas práticas, previstas na legislação, em suas Políticas de Privacidade. Há ainda espaço para melhorias, principalmente na observação dos princípios da lei, os quais devem propiciar autodeterminação no que diz respeito aos dados de uma pessoa, algo precário, nos documentos avaliados. Destarte, este estudo contribui para uma reflexão quanto ao exercício de boas práticas no tratamento de dados pessoais consignados na Política de Privacidade, bem como a forma pela qual o mercado de gás natural vem interpretando estas regras para que sejam aplicadas de forma a traduzirem boas práticas. Esta pesquisa tem relevância pela atualidade do tema e por haver poucos estudos na área do mercado de gás natural,sendo pertinente identificar pontos de melhorias nas Políticas de Privacidade desta amostra.

Palavras-chave: LGPD. Privacidade de dados. Mercado de gás natural.

ABSTRACT

This article aimed to examine the Privacy Policies of the piped natural gas distributors in the hypothesis as to the observation of the good practices foreseen in art. 50 of the Data Protection General Law. To this end, 12 gas companies, the sample of this study, were analyzed quali-quantitatively. The goal was to translate, into figures, the level of adequacy to good data protection practices, using the descriptive approach of the items examined, establishing a relationship between the variables fixed for analysis found in the legislation, the sample findings and the references presented. All data collected is public and is available on the website of each company analyzed, on the link Privacy Policy, which allows to characterize this study as documentary. The theoretical reference used paradigm cases, national data authorities'decision and documentary references that address the subject under study. Analyzing the results, it is possible to observe that the sample is concerned to apply the good practices, provided for the legislation, in its privacy policies. There is still room for improvements, mainly in the principles of the law observation, which should provide a true self-determination regarding someone's data, something that is precarious, in the evaluated documents. This study contributes to a reflection on the exercise of best practices in the processing of personal data contained in the Privacy Policy, as well as the way in which the natural gas market has interpreted these rules so that they are applied in a way that translates good practices. This research is relevant because it is a current topic and because there are few studies in the area of natural gas market, it is pertinent to identify points of improvement in the Privacy Policies of this sample.

Keywords: LGPD. Data Privacy. Natural Gas Market.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
BYON	Bring your on device
CDL	Centro de Distribuição Local
DPO	Data Protection Officer
EUA	Estados Unidos da América
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
NSA	Agência de Segurança Nacional
PRISM	Procurement Information System for Management

SUMÁRIO

1 INTRODUÇÃO

Em um contexto social atual tem-se dependência de setores de energia propulsores de desenvolvimento de praticamente todos os setores econômicos. A falta deste insumo pode paralisar economias provocando perda de desenvolvimento social e econômico e com isso sérios impactos à sociedade. É nesse contexto que o mercado de energia do gás natural está inserido, como uma alternativa limpa na matriz energética do país que ainda conta com energia elétrica, eólica, carvão, solar, termelétrica, biometano, dentre outras. O setor do gás natural contribui na matriz energética por ser uma fonte natural e limpa, sendo menos poluente que tantas outras como óleo, carvão, termelétricas. As distribuidoras de gás natural participam do setor fazendo a entrega do insumo seja a indústrias, comércio ou residências o que atrai diversas regulamentações como a atual Lei sobre Proteção de Dados Pessoais, Lei n. 13.709/2018.

Nesse sentido, a proteção de dados pessoais surgiu de uma necessidade de adequação da comunidade internacional, em um movimento mundial ainda em curso, no qual vários países entenderam a importância de se regular a privacidade do uso das informações pessoais. No Brasil, desde agosto de 2021, está vigente a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual vem movimentando a sociedade para adequação de um novo cenário, onde o direito da privacidade está em primeiro plano. Nesse sentido, o mercado referente à distribuição de gás natural é participativo dessa dinâmica, razão pela qual se busca verificar as boas práticas desse mercado, em atenção às regras previstas na LGPD quanto às Políticas de Privacidade nos *websites* das empresas distribuidoras de gás natural.

A pesquisa se propõe a investigar, diante do novo cenário legal, se as empresas distribuidoras de gás natural têm observado, por meio de suas Políticas de Privacidade, se estão em conformidade com o que dispõe o capítulo sobre boas práticas da LGPD. As Políticas de Privacidade são documentos expressos que tratam sobre os procedimentos referentes aos dados pessoais que são acessados, uma ação que deve conter os requisitos previstos na lei.

Assim, elegeu-se uma série de requisitos presentes no art. 50 da LGPD, para se cotejar com o conteúdo das Políticas de Privacidade publicadas pelas distribuidoras de gás natural, a fim de se analisar se há conformidade com a lei. A relevância é que, diante das experiências anteriores à nova regulamentação, que permitiam o livre acesso aos dados pessoais, surge um novo paradigma da privacidade desafiando os programas de conformidade dos setores públicos e privados. O resultado é a gestão dos controladores do acesso e o tratamento de

dados pessoais, diante da manifestação de determinação do titular.

Diante do exposto, o objetivo geral deste estudo é analisar as boas práticas das distribuidoras de gás natural, disponíveis em seus *websites,* a fim de verificar a adequação das políticas internas à hipótese do art. 50 da LGPD, que trata das boas práticas na proteção de dados pessoais. Os dados foram classificados em categorias, a fim de se propor uma avaliação analítica.

Este estudo se justifica por ser um assunto novo nas relações sociais e negociais, quando o marco legal da privacidade inverte a ordem, estabelecida até 1° de agosto de 2021, no acesso aos dados pessoais. Em outras palavras, quando a eficácia da lei passa a produzir efeitos em um panorama de novas exigências, até então inexistentes, como: obediência a um bloco principiológico específico, existência de termos específicos ao tema, necessidade da existência da nova figura do *Data Protection Officer*, reconhecimento de que a propriedade dos dados é do titular e não mais de quem capturou os mesmos na rede mundial de computadores, existência das figuras do Controlador e Operador como agentes de tratamento, novas nomenclaturas constituindo um verdadeiro novo arcabouço de direitos e obrigações a serem observados.

2 REFERENCIAL TEÓRICO

Este estudo parte de um referencial teórico abordando os fatos que preparam o panorama que ensejou a edição da LGPD, destacando sua essencialidade no contexto social da atualidade, permeada pelo fluxo de informações pessoais, fazendo-se um comparativo com fatos ocorridos sob a regulamentação do GDPR. Em seguida, traz-se a referência das bases legais quanto às boas práticas no tratamento de dados, conforme a LGPD, bem como os conceitos que se entendeu pertinentes quanto à governança e privacidade.

2.1 PRIVACIDADE: Relevância e contexto histórico.

O cenário da *internet,* antes das regulamentações de privacidade, caracterizava-se por ser um ambiente absolutamente livre para o acesso a quaisquer dados pessoais que titulares desavisados mantinham na rede. Isso ocasionou diversas situações indesejadas, sem que os envolvidos tivessem ciência de que seus dados estavam sendo tratados, muitas vezes de forma maliciosa, revelando manipulação livre da informação. Algumas dessas práticas foram descortinadas pela primeira vez por Edward Snowden (2013), um agente contratado pela inteligência dos Estados Unidos da América (EUA), que prestou serviços como funcionário terceirizado para a Agência de Segurança Nacional (NSA) do país.

Ele, no início da década de 2013, entregou uma série de documentos sigilosos, os quais obteve enquanto trabalhava na NSA, na sede do Havaí, e fugiu logo em seguida para Hong Kong. Segundo Caldas (2014), os documentos vazados foram entregues para a mídia e mostraram ao mundo o uso pelo governo norte-americano do Sistema *Prism* de vigilância em massa, um sistema que coletava e-mails, localização, imagens e sites visitados pelos usuários, que operavam sem ciência ou supervisão pública, bem como fora dos termos da Constituição Norte-Americana, conforme ainda consta o registro no *website* mantido por Snowden. No *website* da Casa Branca, tem-se que PRISM é o acrônimo de *Procurement Information System for Management* e há a seguinte explicação:

> Usado para registrar e rastrear requisições emitidas por agências e escritórios dentro do Gabinete Executivo do Presidente, e para emitir e rastrear ordens de compra e contratos. PROPÓSITO: O PRISM é usado para registrar e rastrear requisições, ordens de compra e contratos emitidos por escritórios e conselhos dentro do Poder Executivo do Presidente. O sistema tem uma interface com o sistema Oracle Financials. (THE WHITE HOUSE, 2008, p. 01).

Conforme Caldas (2014), um ano após o vazamento por Snowden, alguns conceitos mudaram, dentre eles, o entendimento de que metadados importam na medida em que houve cinco bilhões de acessos a registros telefônicos de terceiros por dia, fotos e registros em *webcam* poderiam ser acessados (incluindo conteúdo sexual explícito) de milhões de usuários da *internet* que detinham contas no *Yahoo*. Empresas como *Google*, *Apple*, *Microsoft* passaram a adotar Políticas de Privacidade, governos anunciaram a redução da espionagem e legislações regulatórias, como o marco civil da *internet* no Brasil, políticas de *Bring your on device* (*BYON*) precisaram ser modificadas, já que Snowden utilizava seus próprios equipamentos no ambiente corporativo.

Considera-se que a privacidade entrou no cenário dos direitos da era digital a partir de então. O vazamento de informações, protagonizado por Snowden, inaugura um antes e um depois e pode ser considerado um dos primeiros eventos que alavancou a privacidade como item de relevância nos tempos em que o livre acesso a dados pela *internet* permitia a promoção velada de informações particulares (ou íntimas) dos cidadãos, as quais estão na rede para qualquer um acessar.

Mais recentemente, ocorreu um caso emblemático em uma empresa americana de pesquisas, a*CambridgeAnalytics* (FORNASIER; BECK, 2020), que utilizava a técnica de *microtargeting* dos usuários que os classificava como 'indecisos', utilizando notícias falsas (*fakenews*) disseminadas em redes sociais, pois pretendiam, principalmente, manipular a opinião pública nas eleições americanas de 2016. O mesmo *modus operandi* foi replicado na votação europeia pelo *Brexit,*no qual, por meio de aplicativos de redes sociais, foram delineados perfis psicológicos, com informações pessoais dos usuários do *Facebook*, para manipular os resultados da votação. No último fórum de Davos, em 27 de janeiro do corrente, o discurso do Presidente Vladimir Putin alertou para o poder das *Big Techs* atuando como concorrentes do Estado e fez menção às eleições norte-americanas:

> Gostaria de enfatizar mais um ponto importante. Gigantes tecnológicos modernos, especialmente empresas digitais, começaram a desempenhar um papel crescente na vida da sociedade. Muito está sendo dito sobre isso agora, especialmente em relação aos eventos que ocorreram durante a campanha eleitoral nos EUA. Eles não são apenas alguns gigantes econômicos. Em algumas áreas, eles estão competindo de fato com estados. Suas audiências consistem em bilhões de usuários que passam uma parte considerável de suas vidas nessesecossistemas. Na opinião dessas empresas, seu monopólio é ideal para a organização de processos tecnológicos e de negócios. Talvez sim, mas a sociedade está se perguntando se tal monopolismo atende aos interesses públicos. Onde está a fronteira entre negócios globais bem-sucedidos, serviços sob demanda e consolidação de big data e as tentativas de gerenciar a sociedade a critério próprio e de forma dura, substituir as instituições democráticas legais e essencialmente usurpar ou restringir o direito natural das pessoas de decidirem por si mesmas como viver, o que escolher e qual posição

> expressar livremente? Acabamos de ver todos esses fenômenos nos EUA e todos entendem do que estou falando agora. Estou confiante de que a esmagadora maioria das pessoas compartilha desta posição, incluindo os participantes do evento atual (SESSION OF DAVOS, 2021, p. 2).

Durante a Primavera Árabe, os olhos do público testemunharam a possibilidade de as autoridades dos governos rastrearem manifestantes para responsabilizá-los (BAUMAN; LYON, 2014, p.40), depois de os movimentos iniciarem pelas mídias sociais e se espalharem pelas ruas. Percebe-se, portanto, que diversas situações surgiram extravasando fronteiras, atingindo pleitos eleitorais, interferiram em decisões coletivas e movimentaram governos, não restando dúvidas quanto à necessidade de limites legais no uso dos dados pessoais disponíveis na *world wide web*.

Nesse contexto, alguns limites despontaram na tentativa de frear o acesso desmedido aos dados pessoais, sem consentimento, tendo-se a imposição de multa de cinco bilhões de dólares pelo *Federal Trade Comission* contra a empresa americana de mídia social *Facebook*, de Mark Zuckerberg, pela utilização de 82 milhões de dados pessoais capturados na rede social pela empresa *CambridgeAnalítica* (WAKKA, 2019, p. 5). A multa não somente é uma definição dos limites impostos ao acesso dos dados pessoais, mas também sinaliza a necessidade de haver uma finalidade lícita para o acesso. Da mesma forma que responsabiliza por eventual ofensa à privacidade para o eixo dos Controladores (agente que recebe os dados diretamente do titular, conforme LGPD), dentre outras decorrências que restaram por inspirar a Regulamentação Geral sobre Dados Pessoais da União Europeia, vigente desde 2018.

Shoshana Zuboff, em 2019, professora da Harvard University, em sua obra *The Age of Surveillance Capitalism* (ZUBOFF, 2019), na qual descortina as razões de mercado sobre o avanço do mundo digital no real e sua forte instrumentalização em sistemas tecnológicos. Ela estabelece que todo o comportamento humano pode ser traduzido em dados e com isso monetizado, sendo que, de forma mais grave, pode sofrer interferências como a predição de comportamentos, o qual fere o princípio da liberdade de expressão, que é o *modus operandi* tanto dos mercados quanto dos governos.

> Mais fascinante é que ao longo de todos esses anos de ansiedade e debate, era impossível imaginar os meios de modificação comportamental como algo diferente do que possuídos e operados pelo governo: uma modalidade privilegiada do poder do Estado. Um artigo de 1966 publicado no *Harvard Law Review* abordava questões de rastreamento eletrônico, vigilância e controle comportamental, com o seguinte raciocínio: 'Consideraria tentativas do governo de mudar condutas, *já que estas parecem mais prováveis do que tentativas privadas'*. O impulso democrático da sociedade americana, que se opõe a excessos das agências de inteligência, o apoio destas atividades criminosas executadas pela administração Nixon e a migração da modificação de comportamento como um meio de controle disciplinar em

> instituições estatais levaram à rejeição da modificação comportamental como extensão do poder governamental.
> Contudo, longe do conhecimento dos senadores, acadêmicos, ativistas de direitos civis, advogados e muitos outros cidadãos que se opunham às incursões antidemocráticas da visão da engenharia comportamental, esses métodos não haviam morrido. O projeto voltaria à tona numa encarnação totalmente inesperada como *uma criatura do mercado*, suas capacidades digitais sem precedentes, escala e escopo passam então a florescer sob a bandeira do capitalismo de vigilância. Durante os mesmos anos em que as forças democráticas americanas se juntaram para resistir à modificação de comportamento como forma de poder estatal, as energias da contra insurgência capitalista já estavam em funcionamento na sociedade. [...]
> Em sua encarnação mais recente, a modificação comportamental ganha vida como uma arquitetura global não limitada pela geografia, independente de restrições constitucionais e indiferente aos riscos que representa para a liberdade, a dignidade ou a sustentação da ordem liberal que a subcomissão de Ervin estava determinada a defender. O contraste é ainda mais aflitivo diante do fato de que, em meados do século XX, os meios de modificação de comportamento eram dirigidos para indivíduos e grupos considerados "outros": inimigos militares, prisioneiros e outros cativos de regimes disciplinares que viviam atrás de muros.
> Hoje os meios de modificação comportamental são dirigidos, de maneira descarada, a 'nós'. Todo mundo é arrastado por essa nova rede do mercado, inclusive os psicodramas de adolescentes comuns e desavisados, ansiosos pelo próximo fim de semana. Cada avenida de conectividade serve para reforçar a necessidade do poder privado que, em busca de lucro, apropria-se do comportamento (ZUBOFF, 2021, p. 481).

Assim, a predição comportamental não é algo novo na teia social, haja vista que representa uma poderosa ferramenta tanto para os ideais de crescimento dos países, diga-se de qualquer inclinação econômico política, quanto para os mercados. Desse modo, a regulamentação sobre acesso a dados pessoais, em proteção a todo o contexto de liberdade que representa, passou a ter urgência com a liberdade impressa da *internet*. Ainda que a informação dos Agentes de Tratamento para os titulares de dados seja que a retenção de dados é utilizada para aprimorar serviços que dão conforto para a sociedade de consumo, parte dela é explorada na sistematização de condutas virtuais padronizadas, transformando-se em objeto de mercantilização, ao prever e determinar comportamentos de mercados futuros, como apontou Zuboff (2021).

Taleb (2010, p. 239), compara que a *internet,* na esfera dos riscos, é um ambiente pródigo para o surgimento de Cisnes Negros[1], porque dela podem repercutir situações de significativo impacto, principalmente quando o assunto é privacidade de dados pessoais. A título de bem delinear os contornos ubíquos da situação tratada, bem como sua afetação pela importância de boas práticas em privacidade, como limitador às individualidades dos cidadãos e suas escolhas, é que se traz a notícia do jornal chinês *South China Morning Post*, em de 9 de

[11] O que chamamos aqui de Cisne Negro (com iniciais maiúsculas) é um evento com três atributos: um ponto fora da curva, exerce um impacto extremo, apesar do seu status de anormalidade pode ser explicável. (TALEB, 2010, p.08).

agosto de 2020, sobre predição de comportamento. Lee (2021)apresenta o *Social Credit System* da China, que é um sistema que monitora e avalia, desde 2014, informações e iniciativas de indivíduos, empresas e órgãos governamentais, para serem avaliados socialmente e, com isso, obterem pontuações, para que se possa ter acesso a políticas de governo.

Portanto, na dependência de haver bons resultados na avaliação social, é que cidadãos titulares de dados poderão ter prioridade de acesso em tratamentos de saúde, receber depósitos gratuitos de dinheiro para locação de imóvel público, preferência em matrícula de escolas, dentre outras vantagens; enquanto que, um resultado negativo, pontuado por multas na direção de veículos, contas pagas com atraso, dentre outras situações que conferem pontuação negativa, poderá significar inscrição em uma *blacklist,* com conseqüências que poderão resultar em proibição de acesso a viagens em aviões ou trens e a políticas públicas, proibição de hospedar-se em hotéis, etc. Ou seja, a lógica é acessar dados pessoais dos titulares para avaliar os resultados sociais enquanto cidadãos, premiando uns e punindo aqueles que não atingem os objetivos definidos pelo governo, tudo mediante um conjunto de informações obtidas de fontes tradicionais pessoais tais como financeiras, bancárias, criminal, registros oficiais de governo, registros oficiais obtidos com terceiras partes autorizadas, plataformas de crédito *online*, dentre outras.

Como se observa, as proporções da coleta de dados pessoais podem ser de diversos matizes e ordem de importância no contexto social, político, econômico e de consumo, razão pela qual normas e regulamentos em todos os países do planeta sobre o tema, começaram a espocar a partir de 2016. O pioneiro regramento, com impacto na comunidade internacional, veio da União Europeia, com a edição de 2016 do *GeneralDataProtectionRegulation,*que passou a vigorar em 2018, dando a partida para que um movimento regulatório do tema fosse desencadeado em cascata, com regulamentações em diversos países, dentre eles o Brasil (LGPD). Em 1º de novembro de 2021, passou a valer a regulamentação da China, aprovada em20 de agosto deste ano pelo Comitê Permanente do Congresso Nacional do Povo da China, denominada Lei de Proteção de Informações Pessoais (PIPL), conforme informação do site *OpiceBlum* (CHINA APROVA LEI, 2021).

A inquietação sobre o acesso a dados pessoais já era existente na Diretiva 95/46/CE do bloco europeu, entretanto, alguns países pertencentes ao bloco, como a Holanda e o Reino Unido, não haviam regulamentado internamente o tema fragilizando à proteção. Por outro lado, Alemanha e França já tinham medidas legais nesse sentido, conforme Autoridade Supervisora Européia (2018) informa no seu *website*. Nesse cenário, a diretiva já não se

mostrava suficiente frente a diversas situações que surgiram nos últimos anos, fazendo-se impossível trazer à lume o que se constituiu hoje no GDPR, ao se impor no art. 44 efeitos extraterritoriais, na hipótese em que um dado pessoal de cidadão europeu seja tratado fora do bloco ou quando houver transferência internacional dessas informações, o que provocou um movimento regulatório de toda a comunidade internacional. Ou seja, qualquer país que intencione manter relações negociais com o bloco europeu precisará ter vigente uma regulamentação sobre proteção de dados pessoais. Segundo o *website* de pesquisas Gartner (MOORE, 2020), até 2023, 65% da população mundial estará, de alguma forma, sobre a proteção de uma legislação a respeito de dados pessoais.

Sob esse contexto, a nova legislação brasileira foi editada como Lei Geral de Proteção de Dados, Lei nº 13.709 (BRASIL, 2018), acompanhando o movimento da comunidade internacional, liderado pela União Europeia. Essa lei atua sobre as administrações pública e privada, que passam a contar com novas necessidades obrigacionais, constituindo-se em importante marco legal da privacidade. Nesse sentido, a LGPD organiza o acesso às informações pessoais, principalmente em ambiente virtual, ditando algumas possibilidades de coletar, de compartilhar dados, de armazenar, de conferir novas definições de titularidade das informações e demais situações que devem reverberar tanto nas instituições públicas quanto nas entidades privadas, para que estejam em conformidade com a lei a cada acesso a dado pessoal de um titular.

Este estudo pretende analisar à luz da LGDP, somente as Políticas de Privacidade publicadas nos *websites* das distribuidoras de gás natural, sob o aspecto de serem consideradas boas práticas de regulamentação interna do tema.

2.2 BASES LEGAIS E AS REGRAS DE BOAS PRÁTICAS E GOVERNANÇA DO ART. 50 DA LGPD

No Brasil, a Agência Nacional de Dados (ANP) é o órgão responsável pelo regramento referente à fiscalização e, portanto, cominações de multas administrativas já estão em vigência desde 28 de outubro de 2021. Vale lembrar, conforme aponta Mendes (2018), que o direito à privacidade é um direito fundamental assegurado na Constituição Federal de 1988, previsto no artigo 5º, inciso X (BRASIL, 1988), e que outros instrumentos normativos vêm sendo utilizados para aplicação de sanções, nas hipóteses de violação da privacidade, como o Código de Defesa do Consumidor, que, na Seção VI, dedica ao banco de dados e cadastro dos consumidores. Também a Lei nº 12.965 - Marco Civil na internet, traz conceitos

de consentimento, de dados pessoais, tratamento de dados e o princípio da finalidade. A Lei do Cadastro Positivo (LCP), Lei nº 12.414, de 2011, havia introduzido o conceito de banco de dados e de tratamento de dados. Ou seja, antes da LGPD, outros regramentos do ordenamento já embasavam ações relativas ao uso de dados, sobrevindo a LGPD, que conferiu maior importância à proteção de dados pessoais, bem como a publicação das Políticas de Privacidade nas *websites*.

O art. 50 da LGPD estabelece, no *caput*,para os Agentes de Tratamento (controladores e operadores), *standarts* mínimos para fixarem um programa de *compliance* em privacidade de dados. Dentre os incentivos para que estes Agentes assim o façam, é que a adoção de boas práticas de governança seja considerada como aspecto de minimização na aplicação de sanção, na forma preconizada pelo art. 50 da LGPD. Assim, ao se implementar um Programa efetivo de *Compliance* de Proteção de Dados, além de prevenir e detectar os riscos de descumprimento da LGPD, servirá como atenuante na responsabilização das empresas em eventuais casos de infração. Ao se abordar o entendimento de Taleb (2010), de que os riscos da globalização inovam, na medida em que criam uma fragilidade interligada, ao mesmo tempo em que reduzem a volatilidade e dão aparência de estabilidade, é que se entende necessária a detecção prévia dos riscos de descumprimento da LGPD neste seu aspecto integrante do mundo globalizado.

Desse modo, o referido art. 50 estabelece padrões mínimos que os agentes de tratamento (controladores e operadores) e as associações que os representem possuem a faculdade de formular regras de boas práticas e de governança (em privacidade e proteção dos dados pessoais), para as atividades de tratamento. Nesse sentido, analisa-se a Seção II sobre a formulação de regras de boas práticas e governança no contexto legislativo, que determina que os *websites* devem observar ao construírem suas políticas:

> **Seção II Das Boas Práticas e da Governança**
> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas

> operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> I - implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
> II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
> § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.
> Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais (BRASIL, 2018, p. 1).

Nesse sentido, o art. 50, ao definir o que são as boas práticas em Políticas de Privacidade de governança, trouxe um *framework* a ser explorado. Vale referir, antes de qualquer item a ser analisado, o conceito de boas práticas de governança corporativa. Para isso, colaciona-se a definição do Instituto Brasileiro de Governança Corporativa (IBGC), que em seu Código de Melhores Práticas, dispõe:

> Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum (IBGC, 2018, p. 20).

Importante também é a referência sobre governança corporativa da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que entende ser a governança quem detém a tarefa de ser a guardiã da correta aplicação dos direitos das partes:

> A governança corporativa é o sistema segundo o qual as corporações de negócio são dirigidas e controladas. A estrutura da governança corporativa especifica a distribuição dos direitos e responsabilidade entre os diferentes participantes da corporação, tais como o conselho de administração, os diretores executivos, os

> acionistas e outros interessados, além de definir as regras e procedimentos para a tomada de decisão em relação às questões corporativas. E oferece também bases através das quais os objetivos da empresa são estabelecidos, definindo os meios para se alcançarem tais objetivos e os instrumentos para se acompanhar o desempenho. (OCDE, 1999, p. 02).

Portanto, estabelecer um programa de governança de privacidade assegura à administração um comprometimento de se adotar regras de boas práticas referentes ao tema dados pessoais envolvendo a alta administração, as lideranças, os colaboradores, os *stakeholders* e as áreas parceiras. É sobre esse critério que se entende que a Governança Corporativa deve ser compreendida, como consta no *caput* do art. 50 da LGPD. Reis (2020) aponta que ao se adotar uma política de LGPD, permite-se a prevenção de incidentes com dados pessoais funcionando como um instrumento de contenção de riscos, na medida em que a empresa que o adota se compromete a cumprir o ordenamento jurídico e as imposições dos órgãos de regulamentação, dentro dos padrões exigidos para o seu segmento de atuação, razão pela qual a construção de um programa de *compliance* é de relevante importância, fazendo parte dele as Políticas de Privacidade dos *websites*.

2.3 O IMPACTO DA REGULAMENTAÇÃO SOBRE DADOS PESSOAISNO MERCADO DO GÁS CANALIZADO EUROPEU, UM REFERENCIAL PARA APLICAÇÃO DA LGPD

O mercado de gás canalizado brasileiro não dispõe de pesquisas específicas referentes a dados pessoais, a fim de traçar um referencial específico para o mercado nacional. Em atenção a essa abordagem é que se buscou alguns paradigmas na União Europeia e se buscou o referencial de situações que vêm ocorrendo nesta, após a implementação do GDPR, como um paradigma de situações que poderão se replicar no ambiente nacional.

Em razão da lei brasileira ter similaridade com aquela legislação e aquele mercado, justificando-se a utilização deste paradigma às situações do tratamento de dados pessoais no mercado de distribuição de gás natural canalizado, utiliza-se igualmente como referencial teórico para análise desta pesquisa. Sob esse aspecto, Doneda (2020) leciona que todo o arcabouço legislativo brasileiro segue o modelo do direito romano-germânico, em que vale a aplicação da lei e não de decisões jurisprudenciais, como ocorre no direito da *Common Law*, que seguem os países como EUA, Canadá, Austrália, dentre outros. Nesse sentido, o compartilhamento de dados com terceiros é bem explorado no mercado europeu com o que se pode obter um aprendizado, uma vez que a aplicação do GDPR é uma experiência inovadora

de ajuste dos mercados ao tratamento de dados pessoais, vigente desde 2018, ou seja, tem mais tempo que a regulamentação brasileira, com já alguns resultados da experiência no compartilhamento de dados com terceiros.

Em 2018, a consultoria Capgemini (HUSSEINI, 2019) fez uma pesquisa que se encontra no *website* P*ower-Technology,* onde revela as vantagens que o ramo da energia tem encontrado expandindo o mercado de serviços no compartilhamento de informações com mercados adjacentes. Nessa pesquisa, ela demonstrou que 84% das maiores empresas de energia do Reino Unido estão no processo de identificar novas oportunidades, e 52% planejam usar as informações coletadas para expandir seu valor atual de mercado, transformando o modelo de negócio em colaboração, com outras empresas de mercados adjacentes. As conclusões encontradas foram:

> Quanto tempo você leva para tomar banho, e é da conta de alguém? Com uma nova pesquisa da consultoria Capgemini revelando as principais empresas de energia compartilhando dados para maiores oportunidades de receita, os clientes do Reino Unido devem se preocupar que seus dados pessoais possam ser repassados sem o seu conhecimento? A Capgemini descobriu que 84% das principais empresas de energia do Reino Unido estão em processo de identificação de novas oportunidades, e 52% planejam usar dados para ampliar sua cadeia de valor atual, transformando seus modelos de negócios e colaborando com empresas em mercados adjacentes (HUSSEINI, 2019, p. 03).

Portanto, o compartilhamento de dados pessoais com terceiros é um agente modificador do modelo de negócio, em que uma determinada cadeia produtiva se reúne em colaboração, para oferecer novos produtos e serviços. Esse posicionamento no mercado, agora conta com a regulamentação do tratamento dos dados pessoais, mas ainda não demonstra ser um impeditivo para que esse novo modelo se imponha.

A pesquisa apontada pela Capgemini (HUSSEINI, 2019) afirma que a maioria dos fornecedores de equipamentos de energia do Reino Unido concorda que o rompimento digital irá revolucionar a indústria da energia nos próximos cinco anos, com 86%, citando a imposição governamental de 2020, sobre a exigência de medidores inteligentes como um pivô nessa direção. E que o *In-HomeDisplay,* inserido nos medidores inteligentes, irá informar ao consumidor a intensidade de uso da energia, a comparação de consumo com outras famílias em casas similares, a fim de saber se estão acima ou abaixo da média consumida por estas. E, em um nível mais sofisticado, poderão identificar o padrão de consumo dos eletrodomésticos, propiciando que o usuário possa planejar seu consumo.

Husseini (2019) sugere que a indústria da energia ingresse na cultura de colaboração, compartilhando informações das residências com empresas de seguro, por exemplo,

confirmando a tendência de compartilhamento de dados pessoais com terceiros. Outro dado interessante, como fonte de dados para esta análise, é quanto ao compartilhamento dos dados com terceiros, 70% das empresas concessionárias de energia no Reino Unido já dispõem de equipamentos para medir informações de consumo de seus clientes, sendo que 68% dos pesquisados entendem que compartilhar a informação pode levar o usuário a uma experiência de serviços mais rica, pois acreditam que as concessionárias de serviço público são muito rigorosas no tratamento de dados.

Giovani Butarelli, *Data Protection Supervisor* da União Europeia, na mesma entrevista do *website Power Technology* (HUSSEINI, 2019) informou que a implantação em toda a Europa de medidores inteligentes pode trazer benefícios significativos, ao mesmo tempo em que pode colocar em risco a proteção de dados. Nesse sentido, entende-se que o caráter de vigilância na obtenção ostensiva de informações dos titulares dos dados pessoais ainda é um fator preocupante para os atores do mercado europeu, mesmo, após a vigência do GDPR. A preocupação com a cultura de vigilância tem nome certo na área da proteção de dados, Zaboff (2019) é uma das autoras mais preocupadas com a cultura de vigilância, pois entende ser pernicioso o novo modelo de mercados que impõe um inusitado padrão de comportamento, por meio do tratamento dos dados pessoais. A predição de comportamento é a cultura da atualidade, como jamais se tem registrado, tudo se iniciou com o acesso e o compartilhamento de informações pessoais dos titulares.

Nessa esteira, o mercado de energia não está fora desse contexto, como já mencionado. No Brasil, não há ainda essa realidade com informações tão granulares no mercado, mas é uma tendência que provavelmente será seguida. O *website* de pesquisas da *Orbes Research* (2021) revela que o mercado de gás canalizado atende o nicho residencial da União Europeia, que vem sendo conscientizado quanto às questões de escassez energética e, com isso, onúmero de casas inteligentes ou *smarthomes* vem crescendo, aliando as informações obtidas pelos sistemas que oferecem conforto e economia. Os medidores inteligentes que vêm sendo instalados na área de energia atuam de forma eficiente no controle de consumo, entrando como ferramenta útil no controle de gastos com a energia, regulamentados por força da Diretiva Europeia (UE) 2018/2001, quanto à diminuição de emissão de carbono em 80% até 2050.

Em 19 de fevereiro de 2018, informa o *website Marketers Midia* (2018, p. 1) que, por ordem legal, o Reino Unido, o país de Gales e a Inglaterra foram obrigados a instalar medidores inteligentes até 2020, em 26 milhões de casas, com objetivo de controlar o consumo energético, reduzir a emissão de carbono e cumprir a diretiva. Da mesma forma,

Rússia, França, Itália e Alemanha começam um movimento no mesmo sentido, incluindo medidores inteligentes como item obrigatório de controle do consumo de energia. Essas situações sinalizam o início do movimento nos países do bloco europeu quanto ao compartilhamento de informações com terceiros, que surge por força da necessidade de controlar a escassez energética e se expande na formatação de um novo modelo de negócio em colaboração.

Nesse cenário, a pesquisa acima da *Marketers Midia* (2018) sobre casas inteligentes registrou que, em 2017, esse mercado estava avaliado em USD35,7 bilhões, apontando para uma expectativa de alcançar o valor de US$150,6 bilhões até o ano de 2023. Esse mercado cresce por força das preocupações com o clima, que repercutem no mercado de energia, favorecendo o compartilhamento de dados com terceiros. Entretanto, o receio das questões sobre privacidade já atinge os consumidores que têm evitado os serviços que têm compartilhamento de dados com terceiros, com receio do controle das informações pessoais pelo mercado. Isso permite o acesso a diversas informações pessoais, que são trocadas intermitentemente para manter a inteligência doméstica atualizada.

Nessa linha, a obrigação que dispõe as legislações sobre proteção de dados, para informar o quanto de dados se compartilha com terceiros, é medida necessária. A transparência nessa relação se faz essencial na construção de boas práticas de privacidade, pois é nesse manancial de troca de informações que o direito à privacidade é vilipendiado e é essa preocupação que trouxe a legislação para um cenário de relevância, não só no contexto pátrio, mas também no internacional.

Portanto, o compartilhamento de dados pessoais com terceiros não se trata de uma preocupação somente da LGPD, já que o novo modelo globalizado de negócio pode tornar relevante a preocupação com o compartilhamento dessas informações, diante da quantidade de dados compartilháveis e da forma fácil e ubíqua que a informação pode chega. Desse modo, a preocupação da LGPD com os compartilhamentos de dados se assenta na seara da proteção legal ao titular, pois enquanto este não detém conhecimento do quanto é rastreado na *internet* e para que seus dados são utilizados, a indústria de dados pessoais investe fortemente no mercado adjacente de colaboração de informações.

Zeng et al. (2015) alertam que a maioria dos titulares sequer sabe que ao acessar o *website* ou utilizar um aplicativo de celular são coletados sem seu conhecimento ou sua anuência até dados comportamentais, e que estes são ainda compartilhados com terceiros. Esses dados podem ser informações a respeito do emprego, do círculo de amizades, de medicamentos utilizados, dados de procura na rede, *username*, localização e até mesmo a

senha. O compartilhamento de dados com terceiros pode ocorrer de várias maneiras, por exemplo, podem ser repassados dados pessoais obtidos na compra de uma medicação na farmácia para indústria de seguros saúde, podendo alterar as condições contratuais de mercado para o consumidor.

Também, é possível a interferência nas opiniões, desejos de compras ou necessidades das pessoas, por exemplo, como explica o diretor da Microsoft Sam George, em entrevista transcrita no *website BusinessInsider* (WEINBERGER, 2015, p.2), que, ao utilizar um GPS, o aplicativo poderá compartilhar dados pessoais do usuário com seguradoras de automóveis, sem que ele saiba, informando a velocidade que dirige, para onde vai, se dirige de forma perigosa ou não, enfim, são diversas informações trocadas sem o seu conhecimento, que ao serem compartilhadas com terceiros serão monetizadas, na medida do impacto no negócio que essas informações podem representar. Portanto, mesmo sem que o titular tenha consciência, estavam sendo usados todos os seus dados particulares, até o ingresso da proteção pela LGPD no cenário legislativo, que trouxe em seu arcabouço o princípio da transparência, fundamentalmente.

Assim, rastrear e transformar dados em dinheiro de forma sutil é o novo modelo de negócio inserido no mercado de hoje e vem se utilizando de fórmulas e meios de obter essas informações de maneira imperceptível ao titular, razão pela qual é boa prática a informação clara e precisa do quanto está sendo compartilhado, a partir da vigência das normas regulamentadoras. Acquisti, Taylor e Wagman (2016) apontam a pouca transparência adotada por Agentes de Tratamento que chega as vias da falta de lealdade, em que até dispositivos ocultos são aplicados com o fim de obter dados particulares, o que justifica o receio do titular europeu ao aderir os medidores de gás inteligentes:

> Além disso, existem preocupações sobre o rastreamento de tecnologias entre os consumidores em relação à extensão, natureza e técnicas de segmentação (McDonald e Cranor, 2010). Mesmo consumidores sofisticados podem não ser capazes de evitarem ser rastreados, já que a indústria de publicidade e dados muitas vezes encontra novas formas de rastrear e identificar usuários depois que os consumidores aprenderam e adotaram medidas para combater as formas existentes de rastreamento (Hoofnagle et al., 2012). [...] A Diretiva de Privacidade (Considerando 24) afirma explicitamente que [s]o tão-chamado spyware, web bugs, identificadores ocultos e outros dispositivos semelhantes podem entrar no terminal do usuário sem o seu conhecimento, a fim de obter acesso às informações, armazenar informações ocultas ou rastrear as atividades do usuário e podem se introduzir seriamente na privacidade desses usuários (Acquisti, Taylor e Wagman 2016, p. 35,tradução nossa).[2]

[2] Additionally, concerns exist over the fact that tracking Technologies exists among consumers regarding the extend, nature, and depth of targeting techniques (McDonald and Cranor, 2010). Even sophisticated consumers may not be able to avoid being tracked, as the advertising and data industry has often found new

O compartilhamento internacional vem previsto no Capítulo V da LGPD, estando no art. 33 (BRASIL, 2018, p. 12) as possibilidades para que esse ocorra:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos–
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; –II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos;
> –II - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; –IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros–
> V - quando a autoridade nacional autorizar a transferência; –VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> –II - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> V–II - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou–IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Contata-se que a transferência internacional dos dados poderá ser realizada, desde que: o país ou organismo internacional destinatário possua leis de proteção de dados com os mesmos padrões de segurança por ela assegurados; quando o controlador comprovar estar de acordo com os padrões da LGPD; em casos de cooperações jurídicas internacionais; proteção à vida ou incolumidade do titular ou terceiro, com autorização expressa do titular; ou em casos excepcionais previstos no corpo da lei.

A hipótese de transferência internacional de dados sem nenhum tratamento não está na

---

ways of tracking and identifying users after consumers had learned about and adopted measures to counter existing forms of tracking (Hoofnagle et al., 2012). *(...) The EU Privacy Directive (Recital 24) explicity states that [s]o-called spyware, web bugs, hidden identifiers, and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users*

esfera de proteção da LGPD, ou seja, se a empresa utiliza um provedor de *internet* estrangeiro e os dados são apenas transportados sem tratamento, não caracteriza transferência internacional de dados. Em se tratando de *e-mails,* que contêm dados pessoais trocados com empresas parceiras estrangeiras ou fora do país, tem-se, nessa hipótese, a configuração da transferência internacional de dados. A pandemia de covid-19 obrigou muitas pessoas a realizarem as suas atividades na modalidade *homeoffice.* Assim, caso o colaborador exerça a atividade fora do país, com acesso diário ao sistema de rede da empresa e acessando informações referentes a dados pessoais de clientes para exercer suas atividades, não se trata de transferência de dados pessoais, consoante previsto na LGPD, uma vez que não houve tratamento de dados. Enquanto seguidora do modelo do GDPR, a LGPD prevê, igualmente, a hipótese de se manter a proteção dos dados do cidadão nacional e, mesmo na hipótese de haver transferência internacional, a proteção se manterá. Tal situação, nas palavras de Vieira (2019), é salutar quando há verdadeiras possibilidades de haver coleta em massa de dados e faz um comparativo entre os dois, apresentado no Quadro 1.

Quadro 1 - Quadro ComparativoLGPD e na GDPR

LGPD	GDPR
LGPD brasileira permite a transferência de dados pessoais para países ou órgãos internacionais que proporcionem o grau de proteção de dados pessoais adequados ao previsto. A lei é breve quanto a este procedimento e elementos a serem considerados como adequados. A LGPD estabelece apenas diretrizes genéricas a serem observadas pelas autoridades nacionais e as hipóteses de transferência internacional estão previstas no art. 33 da LGPD.	Conforme, disposição do GDPR, a transferência internacional dos dados pode ser realizada independentemente de autorização específica caso a comissão europeia reconheça que o país terceiro assegure um nível de proteção adequado. Não havendo nível de proteção adequado, a transferência internacional estará condicionada a garantias adequadas, que devem ser asseguradas pelo Agente. Todos os procedimentos e elementos que são levados em consideração pela Comissão para a autorização da transferência estão descritos na GDPR.

Fonte: Vieira (2019, p. 42).

Conclui Vieira (2019) que, assim como a LGPD, o GDPR possui alcance extraterritorial, uma vez que sua aplicabilidade se estende às empresas que tiverem filial na União Europeia, por exemplo, e se aplica na hipótese de serviços prestados fora da UE por empresas que coletem dados de pessoas residentes lá ou em trânsito. Nesse contexto, o Guia de Boas Práticas em LGPD editado pela empresa Data Diligence (2020) confirma esse entendimento quanto à previsão do item transferência internacional de dados pessoais no rol das boas práticas. Vale dizer que a transferência, nesses casos, somente deverá operar entre países que igualmente tenham algum tipo de proteção a dados pessoais, hoje mais comum em razão de serviços de nuvem ou de *datacenters* em outro país.

> A Lei Geral de Proteção de Dados estabelece limitação à transferência internacional de dados pessoais para países que não ofereçam grau de proteção de dados pessoais adequados aos previstos na LGPD. Tais limitações se aplicam inclusive às transferências internacionais decorrentes de serviço de *cloud* (nuvem) e *datacenters* localizados em outros países. Esse sistema é conhecido como "adequação", e sua intenção é evitar que os dados pessoais protegidos pela Lei sejam enviados para países que ofereçam risco à privacidade dos seus titulares, sem que a Autoridade Nacional de Proteção de Dados possa intervir. Por isso a ANDP deverá indicar quais países considera que oferecem grau adequado de proteção aos dados pessoais. (DATA DILIGENCE, 2020, p.37).

O aspecto internacional de tratamento de dados tem sua importância resguardada no contexto das boas práticas, razão pela qual prever a forma de tratamento internacional ou mesmo informar a sua exclusão na política de privacidade é uma boa prática. Hoje, tanto a LGPD como a GDPR fazem referência à possibilidade desta transferência, o que de certa forma ratifica a preocupação com a ubiquidade da *internet*.

Os *cookies* são arquivos que permitem armazenar temporariamente o que o internauta está visitando na rede, como se fosse seu percurso em determinada página de *internet* capturando interesses e preferências (REDECKER *et al.,* 2021). Para Ishitani (2003), os *cookies* têm por objetivo gravar dados, ações e preferências do usuário, para solucionar a característica de ausência de estado do protocolo HTTP. Furlaneto, Carmo e Scarmanhã (2018) explicam que a análise de comportamento de consumidores em *websites* tem sido utilizada enquanto ferramenta para tornar o modelo de negócio eletrônico mais rentável, de modo que, para que isso fosse possível, foram necessárias a criação e a inclusão de informações de controle de estado nas comunicações entre clientes e servidores, batizadas como *cookies*. Explique-se que esses estão situados nos navegadores ou *browsers* e ali ficam registrados, facilitando o retorno do visitante à página. Veja-se a explicação de Rohr (2017, p. 01):

> O cookie é um recurso básico da web. Ele é criado quando um site solicita ao navegador que uma informação seja armazenada. Por exemplo, quando você faz login em um site, o site pede que o navegador armazene um código. Toda vez que você visitar outra página naquele site, o navegador enviará o código. O site estará preparado para saber que o internauta com aquele código é você e o manterá logado no sistema. É por esse motivo que o chamado roubo de cookies é problemático. Se um site tem alguma brecha que permite o roubo dos cookies, o código armazenado pode ser injetado no navegador do criminoso, que irá acessar a página como se fosse você. Por motivos de segurança, cada site só pode ler os próprios cookies, ou seja, a Globo.com só pode ler os cookies criados por sites dela mesma. É preciso uma falha de segurança nos sites para permitir a leitura dos cookies.

Além das questões de segurança que suscitam os cuidados com os *cookies*, vale lembrar que estes possibilitam informações de predileção, que se relacionam aos anúncios de

publicidade referente a produtos que os usuários demonstram interesse na navegação. Há possibilidade de se ter um mercado mapeado, e uma acuracidade para se alcançar o consumidor, que até a utilização destas ferramentas de cookies não se tinha. Por isso, a publicidade comportamental *online* reduz os custos da ação publicitária e é cirúrgica ao atingir de forma certeira os interesses do consumidor (BIONI, 2021).

Os cookies são registros eletrônicos que ficam no computador do usuário e tem por objetivo, além de trazer determinadas facilidades ao internauta, fazem o registro da navegação. Conforme explicação de Klaus Peter Laube (2012, p. 1)[3] o HTTP é *stateless*, ou seja, ele não mantém uma conexão a cada solicitação do usuário, logo toda a vez que o usuário pedir uma informação na página, o servidor a recebe e encerra a sessão, perdendo todos os dados, mesmo que venham duas solicitações do mesmo usuário ao servidor não irá reconhecer que é do mesmo navegador, a solução dessa situação está nos *cookies*, visto que mantém as informações entre o computador do usuário e do *website* sem que se perca a conexão.

Portanto, os *cookies* estabelecem essa relação de informação entre o navegador e o servidor para que não se percam as informações a cada mudança de sessão na página, por exemplo saindo da informação de preço do produto e indo para o carrinho de compras, as informações se mantém na página, através dos *cookies*, o usuário não precisa digitar tudo de novo, ou quando retorna a página o servidor reconhece pelo navegador, permitindo autenticação, porque o usuário já está registrado, por exemplo. Existem várias espécies de cookies que poder-se-ia classificar entre necessários, persistentes, de sessão, primários, de terceiras partes. Veja-se abaixo um quadro ilustrativo que fizemos dos tipos de cookies, que observamos são mais utilizados na nossa amostra, suas atividades e os riscos:

Quadro 2–Quadro Cookie

RISCOS	CLASSIFICAÇÃO	COOKIE	ATIVIDADE
Falsificação de autenticação. O site recebe a solicitação e não consegue identificar onde foi iniciada a sessão, se o falsificante tiver o cookie o site faz a autenticação[4]. (GRUPO BINÁRIO, 2021)	Quanto ao ciclo de vida	*Cookie* de Sessão	*Cookie* de sessão não tem data de validade, permanecem no dispositivo temporariamente. É apagado quando fecha a página
	Quanto ao ciclo de vida	*Cookie* Persistente	Permanecem por um período ou até serem excluídos
Invasor impele o usuário a usar o ID de sessão do invasor ou de outro. Isso pode ser feito usando o caminho da diretiva do navegador do *cookie*,	Quanto definido pelo domínio visitado	*First Party*	Criam os cookies diretamente no domínio com o usuário
	Quando pertencem a outro domínio e são	*Third Party*. A partir de 2022 não	Os *cookies* são criados em *website* que o usuário não

portanto, o usuário finge ser outra pessoa. Usando esse método, um invasor pode solicitar que o usuário efetue *login* como invasor em vários níveis de aplicativo. Utilização de informações para segmentação de mercado digital, remarketing, rastreamento de informações para formação de perfil, sem consentimento do usuário. .	incorporados à página	serão mais utilizados, pelo Google. Alguns navegadores não usam mais como, Apple Safari, Firefox.	está fazendo a conexão. Por exemplo, um ícone de rede social na página
	Quanto a sua finalidade	*Cookies* Essenciais ou Necessário	São necessários para manter a navegação, não é recomendável que sejam desabilitados por dificultar ou impedir a navegação.
	Quanto as preferências do usuário (por exemplo, idioma)	*Cookies* de Funcionalidade	Identificam as páginas mais acessadas dos Sites, permitem a exibição dos Sites conforme as configurações selecionadas, ajudama registrar dificuldades nos Sites e mostram o nível de eficácia da publicidade
	Quanto as possibilidades de oferecer publicidade relevante ao usuário.	*Cookies* de Marketing	Estes *cookies* fazem o rastreio de suas atividades, com a finalidade de oferecer publicidade relevante.

Fonte: elaborado a partir dos dados da pesquisa (2021).

Em 2019, diante de toda movimentação em favor da privacidade, o Google que representa mais de 70% do share quanto a navegador mais utilizado pelos usuários segundo o *website Publya* (2021, p. 2) anunciou que não usará mais *cookies* de terceiros e passarão a introduzir o *Privacy Sand Box*, que está em teste. Segundo a *Publya* (2021) o principal destaque desta categoria de *cookies* de terceiros é informar a localização do usuário e dados comportamentais, movimentando um mercado de U$7,8 bilhões/ano. Pela quantidade de informações que os *cookies* coletam conclui-se, incontestavelmente, que são fatores de criticidade de avaliação para o ambiente da privacidade, pela LGPD. Veja-se como o Google se posicionou sobre a decisão de não utilizar mais os *cookies* de terceiros, concluindo ao final o risco sobre a liberdade na internet, *verbis:*

> É difícil conceber a internet que conhecemos hoje — com informações sobre cada tema, em cada língua, na ponta dos dedos de bilhões de pessoas — sem a publicidade como base econômica. Mas, como nossa indústria tem se esforçado para entregar anúncios relevantes aos consumidores em toda a web, ela criou uma proliferação de dados individuais de usuários em milhares de empresas, normalmente coletadas através de cookies de terceiros. Isso levou a uma erosão da confiança: na verdade, 72% das pessoas sentem que quase tudo o que fazem online está sendo rastreado por anunciantes, empresas de tecnologia ou outras empresas, e 81% dizem que os riscos potenciais que enfrentam por causa da coleta de dados superam os benefícios, de acordo com um estudo do Pew Research Center. Se a publicidade digital não evoluir para resolver as crescentes preocupações que as pessoas têm sobre sua privacidade e como sua identidade pessoal está sendo usada, arriscamos o futuro da web livre e aberta.

> É por isso que no ano passado o Chrome anunciou sua intenção de remover o suporte para cookies de terceiros, e por isso temos trabalhado com a indústria mais ampla no Privacy Sandbox para construir inovações que protejam o anonimato e ainda ofereçam resultados para anunciantes e editores. Mesmo assim, continuamos a obter perguntas sobre se o Google se juntará a outros na indústria de tecnologia de anúncios que planejam substituir cookies de terceiros por identificadores alternativos de nível de usuário. Hoje, estamos explicitando que uma vez que os cookies de terceiros sejam eliminados gradualmente, não construiremos identificadores alternativos para rastrear indivíduos à medida que navegam pela web, nem os usaremos em nossos produtos(TEMKIN, 2021, p. 2).

Observe-se que tal posicionamento, apenas surge com as preocupações trazidas pelos titulares, na medida em que passa a existir diversos regulamentos a respeito da privacidade que espocaram mundo afora, modificando o comportamento do mercado quando o tema tratado é privacidade de dados pessoais. A LGPD estabelece que o consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Nesse sentido, para a LGPD o consentimento deverá ser expresso, destacado, que represente uma vontade afirmativa do titular dos dados, ou seja, não há consentimento implícito ou genérico. Importante considerar-se que o consentimento poderá ser alterado pelo titular a qualquer momento, o que lhe dá uma conotação de temporalidade.

Certo, que tal reconhecimento decorre a partir da edição da Lei Geral de Proteção de Dados, visto ter sido esse marco legal que provocou o movimento e um olhar para esta questão. Vale trazer à baila, sobre esse tema, a decisão do Tribunal Constitucional Alemão (BIONI, 2021, p. 142) a respeito da utilização de dados pessoais definidos na lei do recenseamento de 1983, que previa a possibilidade de um cruzamento genérico dos dados pessoais coletados. A importância dessa decisão reconhecendo a inconstitucionalidade do uso de dado pessoais de forma genérica alcança relevância no tema da privacidade, como destaca Bioni (2021) no seguinte sentido:

a) a proteção de dados pessoais como um direito de personalidade autônomo e a compreensão do termo autodeterminação informacional para além do consentimento; e
b) a função e os limites do consentimento do titular dos dados.

Veja-se que o reconhecimento do Tribunal Constitucional Alemão foi essencial para estabelecer uma orientação do entendimento da questão, constituindo-se numa verdadeira bússola a apontar o sentido da interpretação da regra construindo a titularidade dos dados e a determinação do uso dos dados ao indivíduo, que mesmo diante de um interesse público relevante, ou seja: informar que os direitos à personalidade do indivíduo representado pelos

seus dados pessoais têm maior relevância, mesmo diante da formação de um interesse coletivo que pode ser alcançado de outra forma. Essa construção se mostra significativa na medida em que, passados muitos anos após 1983 (ano da decisão) o excesso de preenchimento de formulários na *worldwideweb*, nas redes sociais, nas *websites* foi tão vulgarizado que os dados pessoais jogados na web passaram a ter a conotação de titularidade pública, de informação apropriável a qualquer um para fins daquele que se apropriar da informação.

O art. 5º, XII da LGPD dispõe que o consentimento é a manifestação livre, informada e inequívoca de que o titular concorda com o tratamento de seus dados pessoais, segundo Bioni (2021, p. 39) o consentimento deve ser voluntário, certo, explícito, claro, documentado. Essa amostra, apontada por Bioni (2021) investigada cumpre esse requisito, excetuando-se uma empresa da amostra que não deixa explícita a questão do consentimento, as demais incluem clareza quanto ao consentimento do titular no uso dos dados. Desde 2018, a empresa Uber detém processo administrativo junto a *Garante per La Protezione Dei Dati Personale* autoridade italiana[5] por fazer tratamento de dados pessoais sem o consentimento de 295 mil titulares usuários do serviço, a fim levantar um índice de risco de fraude dos usuários. Outra recente decisão pela autoridade italiana, multou em €$8.500.000,00 (oito milhões e quinhentos mil euros) a empresa de energia *Gas e Luce*, dentre outras razões pela falta de controle no consentimento do titular na utilização dos dados pessoais, em ações de telemarketing. Interessante verificar o teor da interpretação da autoridade italiana a respeito do tratamento que deve ser dado pelo Controlador do consentimento:

> A natureza significativamente negligente do processamento (artigo 83, parágrafo 2º, letra. b) do Regulamento), com especial referência à não adoção de sistemas de controle de consentimento e televendas que, por padrão, deveriam ter garantido a gestão correta do mesmo, bem como à adoção de procedimentos e diretrizes interpretativas em contraste com o atual marco regulatório. (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2019, p. 2/9)

Doneda (2011) afirma que a opção pela não revelação dos dados pessoais pelo titular costuma ser uma - por vezes, brutal renúncia, a determinados bens ou serviços. O mesmo autor também refere que muitas das vezes o consentimento parece ser inócuo e o titular não tem condições de avaliar as conseqüências. No mercado de medicamentos revelar os dados pessoais rende ao titular descontos que podem reduzir o preço até quarenta por cento. No cenário de pouca informação aos titulares, o consentimento dá-se através de um *click* do usuário em um *check-b*ox ou em *link* confirmando que concorda com o tratamento dos dados

pessoais, mas a pergunta que fica é será que ele realmente concorda. Sobre o tema, Zuboff (2021, p. 79) comenta no artigo *The University of Chicago Press Journals* em que faz um questionamento a respeito da validade dos *check-box*, após uma pesquisa identificar que as pessoas clicam sem se importar ou saber quanto ao resultado do conteúdo ou sobre o que estão clicando, portanto, o item consentimento provável que seja um requisito que em breve deverá ser revisto, para que seja mais eficaz à luz do que dispõe a LGPD.

2.4 FERRAMENTAS DE CONTROLE DAS BOAS PRÁTICAS DA POLÍTICA DE PRIVACIDADDE

Com a disseminação de serviços online, é que a Lei Geral de Proteção de Dados aponta algumas ferramentas de proteção aos dados pessoais que devem estar inclusas nas boas práticas em Políticas de Privacidade, e nesta análise se considera a utilização de princípios nas Políticas de Privacidade, a indicação de um DPO, a previsão de descarte de dados, existência de glossário de termos e previsão de atualização constante. Nesse contexto, foi publicado pelo CERT - Centro de Estudos de Respostas e Tratamento de Incidentes no Brasil em sua Cartilha de Segurança para Internet (2020) uma série de situações em que dados pessoais podem ser vazados, em que as ferramentas de controle pelas boas práticas poderiam auxiliar a proteger o titular de dados. Veja-se os exemplos trazidos na Cartilha:

> Furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas, pelo acesso a contas de usuários, por meio de senhas fracas ou vazadas através da ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros, pelo furto de equipamentos que contenham dados sigilosos, através de erros ou negligência de funcionários ao realizar o descarte de mídias (discos e pen drives) sem os devidos cuidados (CENTRO DE ESTUDOS, RESPOSTA E TREINAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT, 2021, p. 2).

O art. 50 da LGPD aponta itens que identificamos como ferramentas às boas práticas, a fim de evitar que situações como as acima apontadas ocorram ou se ocorrerem produzam menores impactos, na medida em que se tem a presença de ferramentas no controle da manutenção da privacidade. Aponta Pinheiro (2021, p. 43) que a LGPD é uma lei principiológica porque ela precisa ter um rol de princípios atendidos. Quanto aos princípios elencados na lei da privacidade, tem-se que a própria LGPD ao se referir o quanto considera boas práticas elencando no §2º do art. 50 de que no mínimo devem estar presentes os princípios da Segurança e da Transparência. Portanto, ainda que não se trouxesse todo o

elenco de princípios da legislação, mas minimamente o da segurança e da transparência, ainda assim estar-se-á no patamar das boas práticas, os incisos VI e VII do art. 6º da Lei trazem a definição destes princípios:

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (BRASIL, 2018, p. 04).

Nesse diapasão, tem-se que os princípios declarados são garantias de que os dados pessoais serão pautados com a observância de serem direitos dos titulares, visto que criam um framework informativo sob qual prisma os dados pessoais eventualmente capturados serão tratados. Em recente decisão preliminar de 06/10/2021, a autoridade da Irlanda se manifestou a respeito de uma reclamação realizada por um cidadão austríaco contra a falta de transparência na Política de Privacidade manejada pelo *Facebook*, cuja sede fica na Irlanda.

No caso, o *Facebook Ireland Limited* prevendo o ingresso do GDPR no bojo obrigacional da União Europeia solicitou uma renovação de consentimento aos usuários elencando como consentimento todas as hipóteses do dispositivo legal do Regulamento europeu, sem determinar qual hipótese o usuário conferia consentimento ao clicar que aceitava os termos de processamento de dados pessoais da página, razão pela qual o processamento de dados pelo *Facebook* estava ilegal. Veja-se o texto da autoridade irlandesa na decisão preliminar de representação contra o *Facebook*, *verbis:*

> Além disso, o Reclamante alega que não está claro qual base jurídica específica está sendo utilizada pelo Controlador para cada operação de processamento. Na verdade, ela argumenta que "[i]t permanece, no entanto, obscura sob quais operações exatas de processamento o controlador escolhe basear em cada base jurídica específica" 4 como "[t]ele controlador **simplesmente lista todas as seis bases para processamento legal sob o artigo 6 do GDPR em sua política de privacidade sem indicar exatamente em que base legal o controlador se baseia para cada operação de processamento específica."**[...] Como o GDPR exige que os controladores forneçam informações detalhadas aos usuários no momento em que dados pessoais são obtidos, incluindo o fornecimento de informações sobre os propósitos do processamento, bem como as bases legais para o processamento, o Reclamante argumenta que essa falta de informações violam as obrigações de transparência no GDPR (Autoridade de Dados da Irlanda, 2019, p. 8/96, grifo nosso, tradução nossa) [6]

No Brasil, a LGPD permite dez possibilidades de tratamento de dados, dentre estes o consentimento do usuário que demonstra deter uma fragilidade maior, diante da falta de

conhecimento do próprio usuário quanto ao seu '*check-box*', como antes pontuado, bem como traz instabilidade ao Controlador, em razão de que pode ser alterado a qualquer momento. Zuboff (2019) aponta, quando a finalidade é demonstrada com a declaração de que o acesso aos dados pessoais é necessário para a prestação de um melhor serviço ou produto, seguidos pelos princípios da segurança e transparência desta anuência, é uma situação entendida por lícita sob o ponto de vista do capitalismo. Ou seja, mesmo havendo a anuência do usuário, na medida em que é um hipossuficiente nesta seara, é que não se afasta a importância do dever de informar quanto aos princípios da transparência e da segurança que devem estar sempre presentes em todas as hipóteses, porque são espécies de proteção ao titular dos dados razão pela qual configuram como boas práticas de governança.

A Política de Privacidade do *website* faz parte da estrutura de documentos de proteção de dados, ou seja, é um dos instrumentos de implementação do *privacy by design* razão pela qual incluir os princípios traz transparência quanto aos métodos utilizados pela empresa. Pinheiro (2021) explica que se entende por *privacy by design* o conjunto de documentos que dispõe sobre o tratamento de dados pelo Controlador, sob o ponto de vista de todo o negócio. A figura do Encarregado de Dados ou DPO no cenário corporativo e público é novidade, e vem prevista no artigo 5º, inciso VIII, da LGPD dispõe que o Encarregado será uma "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), (BRASIL, 2018, p. 04). Logo adiante no texto, o *caput* do artigo 41 da LGPD dispõe que "o controlador deverá indicar encarregado pelo tratamento de dados pessoais" (BRASIL, 2018, p. 13). Como se depreende do dispositivo o Encarregado ou DPO deve estar constituído na figura de uma pessoa determinada física ou jurídica, interna ou representado por terceiros através de contratação deste serviço, mas deve estar evidenciada enquanto uma figura para realizar as questões a respeito da privacidade. A LGPD além de informar que o Encarregado ou DPO deve ser uma pessoa física ou jurídica destacada para atividade de proteção de dados pessoais, também impõe que suas informações de contato devem ser absolutamente claras e de fácil acesso, conforme consta no 1º do art.41

> **Seção II**
> **Do Encarregado pelo Tratamento de Dados Pessoais**
> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. ((BRASIL, 2018, p. 13) grifo nosso.

A falta de cumprimento na observância dos requisitos legais na constituição do DPO, decorreram sanções no âmbito da aplicação do GDPR. Na medida em que, a LGPD utilizou esse regramento como inspiração é de se esperar pela possibilidade de sanções pela mesma causa, quando iniciada a fiscalização da lei. Vale trazer à baila o caso retratado pelo *European Data Protection Officer* (EDPO, 2020), ocorrido em 2020, em razão da repetição de modelos. Trata-se de uma empresa espanhola Glovo, que ao invés de nomear um DPO nomeou um Comitê de Proteção de Dados, bem como não prestou informações no prazo legal à Autoridade Espanhola quando demandada. Por essa razão foi denunciada e multada ao final em 25 mil euros, por ofensa ao art. 37 do GDPR. Conforme o site GDPR *Enforcement Tracker* (2021), também na Espanha a empresa *Aconcagua Juegos* foi multada em 10 mil euros, por ofensa ao mesmo dispositivo por não nomear um Encarregado de Proteção de Dados. Confira-se trecho da decisão da autoridade espanhola sobre o caso:

> Neste caso, o réu não apresentou alegações ou provas que contradigam os fatos denunciados no prazo para tanto. Esta Agência constatou que a conduta do reivindicado não está de acordo com as normas de proteção de dados, uma vez que a falta de designação de DPO, ao se envolver em jogos online, conforme indicado em seu site (www.aconcaguapoker.es), dá origem à violação do artigo 37.1 b b) do RGPD em relação ao artigo 34.1 n) do LOPDGDD. [...]O Diretor da Agência Espanhola de Proteção de Dados RESOLVE: PRIMEIRO: IMPOR na ACONCAGUA JUEGOS S.A., com NIF A73972010, por infração ao artigo 37 do RGPD, tipificado no artigo 83.4 da RGPD, multa de € 10.000 (dez mil euros). SEGUNDO: EXIGIR ACONCAGUA JUEGOS S.A., com NIF A73972010, nos termos do disposto no artigo 58.2 d) do RGPD, para que, no prazo de um mês a partir da notificação desta Resolução, informe esta Agência sobre a nomeação do Delegado de Proteção de Dados. Tradução nossa. [...] (AGÊNCIA ESPAÑOLA DE PROTECCIÓN DE DADOS – AEPD, 2021, p.1).

Confira-se outra decisão da Autoridade Espanhola, de 13/02/2020 que impõe multa de EUR 50 mil por falta de indicação de DPO em uma empresa de saúde por utilizar sistema de gravação de imagens na sede, *in verbis*:

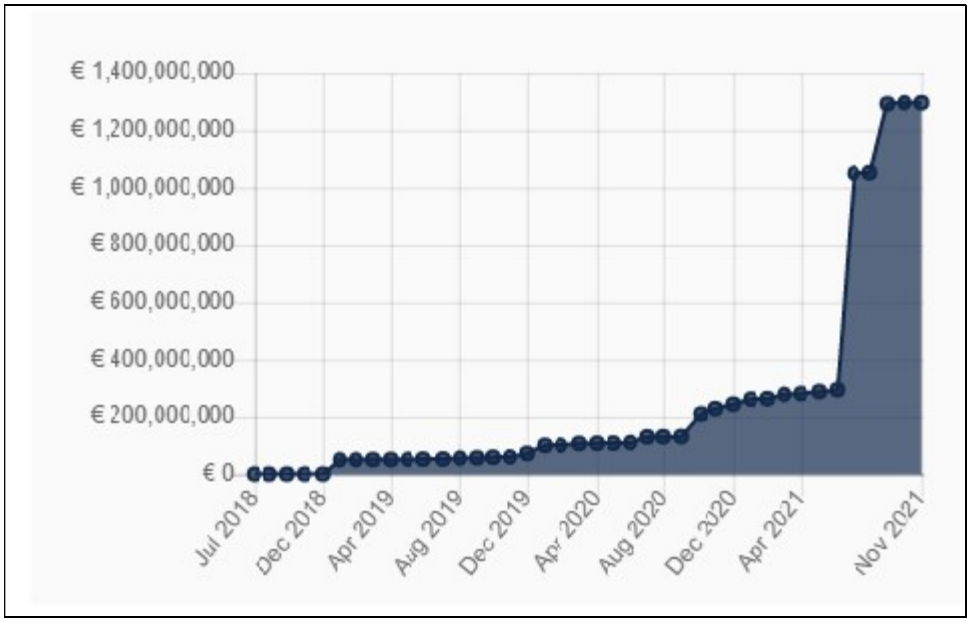
> PRIMEIRO: FESMC UGT MADRID (doravante, o requerente) em 13 de fevereiro de 2020 entrou com uma reclamação na Agência Espanhola de Proteção de Dados. A reivindicação é dirigida contra a CONSEGURIDAD S.L. com NIF B85937902 (doravante, o alegado). As razões pelas quais a reivindicação se baseia são que a reivindicação tem um sistema de CCTV, onde registra as imagens de todas as

> pessoas que entram e trabalham nas instalações. No entanto, a parte reclamada não tem um Oficial de Proteção de Dados (doravante DPO) nomeado e, portanto, nenhum direito pode ser exercido. Junto com a alegação, fornece gravações das câmeras de videomonitoramento. PRIMEIRO: IMPOR à CONSEGURIDAD S.L., com NIF B85937902, por infração ao artigo 37.1 b) do RGPD, em relação ao artigo 34.1 ñ) do LOPDGDD, tipificado de acordo com o artigo 83,4 do RGPD, multa de € 50.000 (cinquenta mil euros) (AEPD, 2021, p. 01/5).

Segundo o site *Enforcement Tracker* (2021) foram multadas por falta de observância do art. 37, indicação de DPO, empresas na Itália, Espanha, Luxemburgo, Bélgica, Alemanha e Áustria. Como se depreende há uma interpretação rigorosa pelas autoridades dos membros da União Europeia na interpretação do GDPR, impondo relevantes multas pela aplicação inadequada do regramento, ainda que a ofensa ao art. 37 do GDPR não se verifique multas tão altas como ocorre em outras hipóteses de violação, portanto consideradas de maior gravidade ainda. Nessa esteira, recentemente o aplicativo *Whatsapp* sofreu multa pela autoridade de proteção de dados na Irlanda em 225 milhões de euros por falta de transparência aos usuários, conforme o site *Enforcement Tracker* (2021) traz a íntegra da decisão.

A estatística publicada pelo site *Enforcement Tracker* (2021), sobre o curso de aplicação de multas na União Europeia desde 2018 até novembro/2021, em razão da não observância de indicação do Encarregado/DPO, na forma como preconizada no regulamento, e as multas que deram causa, formam um dado relevante espelhando a pouca atenção do mercado sobre esse regramento. Continuando sobre a observação da estatística do quadro, a quantidade de multas em 2018 era inexpressiva em relação ao número de multas em novembro/2021, por falta de indicação de Encarregado/DPO na forma correta. Veja-se que nos primeiros 06 (seis) meses, apesar de ter havido violação do regramento não houve multa pecuniária, apenas após o prazo de 06 (seis) meses as multas começaram a ser fixadas em dinheiro verificando-se que não somente aumentaram em volume, mas também aumentaram em relação ao valor. O Regulamento n. 01 de 28/10/2021 da Autoridade brasileira, em seu art. 15 aponta que a fiscalização adotará atividades de monitoramento e prevenção, mas não fixa um prazo para que isso ocorra, portanto de regra as multas já estão aptas para serem aplicadas desde a vigência do regulamento em outubro/2021.

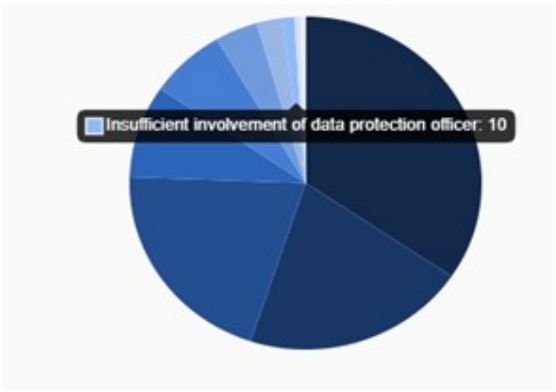
Gráfico 1 - Índice de Multas em euros no período entre julho/2018 a novembro/2021 na União Europeia



Fonte: *EnforcementTracker*(2021, p. 1).

Também se confira abaixo estatística elaborada pelo site *Enforcement Tracker* (2021, p.01) em que se pode visualizar a representação de ausência de indicação de DPO ou Encarregado de Dados, em relação a outras ofensas legais ao GDPR, em que pese ser ainda em número bem menor ainda presente, diante de um regulamento imposto desde 2018.

Gráfico 2 - Pesquisa pelo número total de multas: envolvimento insuficiente do Encarregado:



VIOLAÇÃO	NÚMERO DE MULTAS
Base Legal Insuficiente	299 MULTAS
Medidas técnicas e organizacional insuficientes	179 MULTAS
Não conformidade com os Princípios de Proteção geral de dados	178 MULTAS
Preenchimento insuficiente de direito a informação	78 MULTAS
Preenchimento insuficiente de obrigações	61 MULTAS
Cooperação insuficiente com a autoridade supervisora	34 MULTAS
Preenchimento insuficiente nas notificações	20 MULTAS
Envolvimento insuficiente do Data Protection Officer	10 MULTAS
Preenchimento insuficiente de acordo de processamento de informações	5 MULTAS
Desconhecido	4 MULTAS

Fonte: *Enforcement Tracker* (2021, p. 1).

Outro ponto que se destaca a respeito do DPO é trazido por Lima e Alves (2021), que apontam a diferença entre a definição das atividades do DPO no *General Data Protection Regulation* em que o art. 37, §5º define com maiores detalhes as atividades de um DPO, diferente do que ocorre na LGPD em que as atividades são mais genéricas e vêm prescritas ao se observar o art. 41 na íntegra, tendo-se a obrigatoriedade no GDPR de que o Encarregado/DPO tenha conhecimentos jurídicos (art. 37, n.5) enquanto que na LGPD não há esta obrigatoriedade, o que se entende poderia facilitar a indicação dessa figura.

Do ponto de vista, do descarte de dados a análise aqui busca identificar no *website* não somente a informação do direito ao descarte, mas a possibilidade da efetiva execução do pedido de descarte pelo titular. O exercício do direito de descarte de dados, através do pedido do titular vem sendo regiamente observado pelos Controladores da União Europeia, no paradigmático GDPR. Nesse sentido, em recente decisão (julho/2021) a AEPD (2021) multou

a empresa *Personal Mark* em €$10.000,00 (dez mil euros), por não respeitar a regra de descarte de dados diante da solicitação reiterada pelo titular de expressa solicitação de descarte. O caso tratava de ligações repetitivas de *Call Center*, após a solicitação do descarte dos dados pelo titular.

Na mesma linha de entendimento, a autoridade francesa *Commission Nationale de l'Informatique et des Libertés* (2020, p. 1/17) multou a empresa Carrefour em razão da coleta de dados pessoais, sem permissão no site da empresa, para posterior utilização em telemarketing, ainda que houvesse a solicitação de descarte dos titulares. Nessa situação, a autoridade francesa multou o Carrefour em €$2.500.000,00 (dois milhões e quinhentos mil euros), conforme a fonte do site da autoridade reguladora francesa.

Atualmente, a prática comum e reiterada de utilização de *robocalls* que cercam titulares de dados pessoais dia e noite, provocam um sem número de dissabores muito além do poderiam agregar qualquer valor a bens ou serviços, com as ligações em geral inoportunas. Esta operação com *robocalls* poderia ser amenizada caso houvesse a preocupação com o descarte dados, após cumprida a finalidade da relação com o titular o Agente de Tratamento deveria descartar os dados. Esse cenário de práticas abusivas fica bem característico, quando se analisa as estatísticas logo após a vigência do GDPR pelo site Enforcement Tracker (2021) que aponta 37 (trinta e sete) multas entre os anos de 2019 e 2021, por ofensa ao não descarte de dados pessoais e sua consequente utilização em ações de telemarketing. Nesse período, a Itália é o país com multas mais significativas pelo não descarte de dados, sendo a empresa de telefonia TIM a maior multa no valor de €$27.800.000,00 (vinte e sete milhões e oitocentos mil euros), seguida da empresa de energia *Eni Gas e Luce* em €$8.500.000,00 (oito milhões e quinhentos mil euros).

Em julho de 2020, a autoridade italiana multou a empresa MAPEI S/A por não descartar dados após a solicitação de titular. O caso refere-se à solicitação de descarte feita por um ex funcionário da empresa que requereu o descarte dos dados pessoais de e-mail após terminada a relação de emprego. A não observância do descarte dos dados do titular rendeu multa à empresa de €$15.000,00 (quinze mil euros). Veja-se que a Autoridade Brasileira, em 28 de outubro último publicou a Resolução n. 01/2021 em que o titular pode se valer de meios administrativos junto a ANDP para pedir o descarte dos dados, sem precisar recorrer à Justiça. Portanto, a partir da publicação da regra regulatória os titulares poderão fazer valer sua autodeterminação informativa.

Bioni (2021), ao explicar sobre as conseqüências de os dados permanecerem no big data traz o emblemático caso da empresa americana Target, em que o pai de uma adolescente

descobriu que iria ser avô, pelos algoritmos utilizados pela Target que mapeavam os consumidores de produtos para gravidez. Pelos regulamentos atuais menores de idade tem proteção especial à privacidade devendo espelhar erro de maior gravidade o incidente com menor. A única forma de fugir da mineração dos dados é através do direito de descarte, caso os dados se mantenham no *big data*, e esta providência deve ser feita pelo Agente de Tratamento tão logo termine a sua relação negocial com o titular. Conforme Bioni (2021), permanecendo os dados no *big data* será possível uma série de identificações de comportamentos padrão tais como: surto de gripe, risco de inadimplência de um tomador de crédito, riscos de segurados, etc. Desta forma, a única garantia de não ser rastreado é requerendo a eliminação, conforme art. 18, VI da LGPD ou a eliminação automática pelo Agente de Tratamento, art. 15 e art. 16 da LGPD quando alcançada a finalidade do tratamento.

Diferente do GDPR, o Brasil não instituiu o direito ao esquecimento, como está previsto no art. 17 da lei alienígena. No Brasil, o direito de o titular requerer a eliminação dos dados é distinto do direito de esquecimento, que tem relação com o *"right to erasure*" or "*right to be forgotten*" previsto no GDPR, art. 17 (UE, 2016, p. 01). Entretanto, o direito ao esquecimento existe no Brasil, inclusive com manifestação recente no STF no Recurso Extraordinário (RE) 1010606 sob outro enfoque na legislação brasileira, entendendo que o direito ao esquecimento é incompatível com a Constituição porque ofende a liberdade de expressão.

2.5 CONCEITO DE PRIVACIDADE

Para que o presente estudo alcance seu desiderato em verificar as boas práticas nas Políticas de Privacidade publicadas nas *websites* das distribuidoras de gás natural canalizado, é que se entende importante antes de tudo trazer à luz o conceito do quanto se entende por privacidade. Nesse sentido, é a partir do entendimento do limite conceitual do termo privacidade é que se busca a validação das Políticas de Privacidade objeto deste estudo, através da verificação do seu conteúdo cotejando-se com a Seção II da LGPD como limitador dos elementos analisados.

Como aponta Machado (2014, p. 5) a privacidade, como direito fundamental e da personalidade, passou por uma transformação desde a sua noção do direito de ser deixado em paz até os dias de hoje em que a privacidade é entendida pela concepção de controle pessoal das informações. Gomrey (1992), ao revisar o centenário do reconhecimento do direito à

privacidade nos Estados Unidos, comenta o festejado artigo escrito por Samuel Warren e Louis Brandeis relembrando o marco do principal precedente sobre o conceito de privacidade publicado pela *Harvard Law Review*, em 15 de dezembro de 1890, no artigo intitulado O Direito à Privacidade. Nesse contexto, aponta o autor em celebração ao centenário da existência do reconhecimento deste direito o quanto a seguir se reproduz, *verbis:*

> Foi há cem anos, no inverno de 1890 91, que Samuel Warren e Louis Brandeis publicaram seu agora-famoso artigo na Harvard Law Review, intitulado simplesmente: O Direito à Privacidade. Nesse compacto trabalho de vinte e sete páginas, aparecendo quatro anos após a Revisão de Direito ter sido estabelecida em Harvard através dos esforços de Brandeis e outros, os autores argumentaram que o direito comum havia alimentado um novo direito, conhecido simplesmente como privacidade, que exigia aceitação na jurisprudência americana. "Mudanças políticas, sociais e econômicas implicam o reconhecimento de novos direitos", escreveram Warren e Brandeis "e o direito comum, em sua juventude eterna, cresce para atender às demandas da sociedade.(Gomrey, 1992, p.01, tradução nossa).

Bahri, Carminati e Ferrari (2018), lembram que as primeiras discussões sobre o conceito de privacidade realizadas em 1890 por Samuel Warren e Louis Brandeis tratavam o tema, sob o ponto de vista normativo, onde a legislação deveria proteger o escopo da privacidade, que se definia em um espectro maior do que a proteção física, defendida como o direito subjetivo de ficar sozinho. Diante das possibilidades dos novos inventos da época, como a fotografia e os jornais distribuídos em larga escala, é que o efeito da publicação sobre pessoas passou a ser analisado. Desse modo, apontam Bahri, Carminati e Ferrari (2018), que já naquela época Warren e Brandeis realçaram a hipótese da possível invasão de privacidade por uma vasta disseminação de publicação de assuntos pessoais, referindo-as como informação privada. Trazendo o tema para o presente, as autoras argumentam, que diante de novas tecnologias é que se tornou essencial explicitar e reconhecer um direito geral à privacidade, que confere o direito das pessoas de ter controle sobre determinados temas que só dizem respeito a si próprias.

A principal conclusão é de que pela nova tecnologia faz-se essencial reconhecer um direito geral à privacidade, que supera o direito das pessoas de estabelecer controle sobre seus pensamentos, seus sentimentos e emoções a ponto de poderem decidir serem ou não compartilhados com terceiros. Nesse ponto, Bahri, Carminati e Ferrari (2018, p. 20) apontam também que os precursores Warren e Brandeis defenderam quanto a necessidade de novas regras para proteção da privacidade, *in verbis:*

> Eles argumentaram que a nova tecnologia tornou essencial reconhecer explicitamente um direito mais geral à privacidade, que cobria o direito das pessoas

> de ter controle sobre como seus pensamentos, sentimentos e emoções poderiam ser compartilhados com os outros. Recentemente, algumas novas leis e regulamentos começaram a reconhecer a privacidade das informações como um direito formalizado que está sob a proteção da lei. Por exemplo, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) 4 no Canadá, ou o mais recente Regulamento Geral europeu de Proteção de Dados (GDPR) que entrará em vigor a partir de 25 de maio de 2018 (Bahri, Carminati e Ferrari, 2018, p. 20).

No contexto histórico quanto ao surgimento do direito à privacidade como algo a ser observado, José Sampaio (*apud* MACHADO, 2014) vai mais longe e aponta como marco do conceito de privacidade o "*Grundzugedesnatrurrechts*", de David Augusto, em 1846, onde o autor define como ato violador do direito à privacidade: incomodar alguém com perguntas indiscretas ou entrar em um aposento sem se fazer anunciar. O segundo marco histórico que aponta o mesmo autor é o caso Affaire Rachelix c. O'Connell, em que uma famosa atriz do teatro clássico francês, do século XIX, ao pedir que fosse fotografada no leito de morte teve de forma não autorizada sua imagem disponibilizada para terceiros. Assim que, alguns fotógrafos entregaram a imagem da atriz morta para elaboração de um desenho, que foi publicado no seminário L'Illustration. A família da atriz ajuizou ação em face do desenhista e o Tribunal Civil de Sena proferiu sentença no sentido de que não seria dado a ninguém o direito de reproduzir e dar publicidade a traços de uma pessoa em seu leito de morte, sem autorização formal da família.

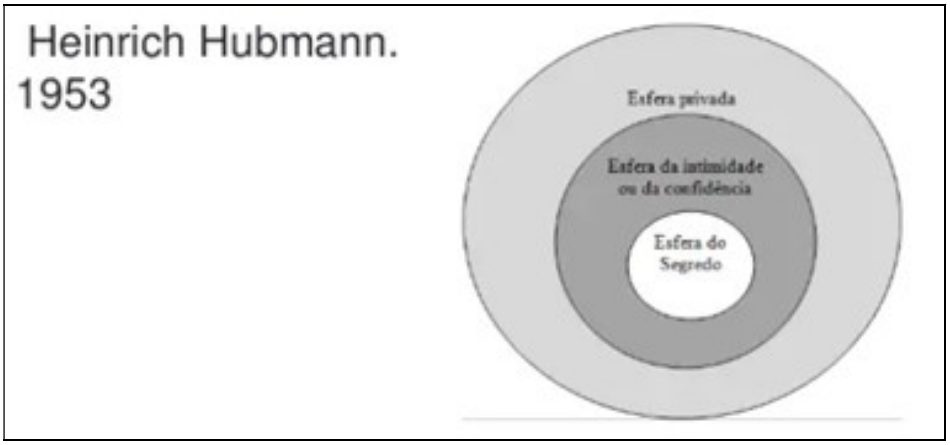
Apesar dos precedentes listados por José Adércio Leite Sampaio (*apud* MACHADO, 2014), a maior parte dos autores é unânime em apontar o trabalho dos norte-americanos Warren e Brandeis, como precursores do reconhecimento do conceito de privacidade, mesmo que a definição não venha a se justapor exatamente a privacidade dos dias de hoje, em razão que se constituía, na época, tão somente a um 'direito a ser deixado só', que surge quando Warren casado com a filha de um senador é vítima de escândalo conjugal. Conclui Machado (2014, p. 6), que a privacidade naquele contexto passa a ser entendida como prerrogativa de individualidade do cidadão, sob o ponto de vista de uma sociedade burguesa para proporcionar isolamento.

Ainda nesse contexto sobre a definição da privacidade, Bahri, Carminati e Ferrari (2018) apontam que a privacidade é elástica e admite vários conceitos dependendo de onde é aplicada, a quem é aplicada e sob qual objetivo é aplicada. Desse modo, vale trazer a contribuição de Maia (2011) para o tema, eis que encontra identidade da definição de privacidade na Teoria dos Círculos Concêntricos de Hubman na obra *Das Persönlichkeitsrecht*, em que classificou o direito geral de personalidade em três círculos ou

esferas concêntricas, quais sejam: a primeira da Intimidade (*Intimsphäre*) a qual se tem proteção absoluta, a segunda do Segredo (Geheimnisphäre) que tem proteção mais ampla que a primeira, e a última esfera que é da Privacidade (*Privatsphäre*). Nessa esfera, localizam-se as proibições de divulgação de fatos cujo conhecimento pertence a um determinado círculo de pessoas que não participam obrigatoriamente da vida do indivíduo e que conheçam os seus segredos. Enquanto na esfera secreta os familiares e outras pessoas ligadas ao indivíduo participam de seus segredos, sendo que nessa última esfera, mais pessoas conhecem da privacidade do indivíduo, ficando apenas de fora a coletividade, que nada tem a haver com a vida dessa pessoa (MAIA, 2011).

Cunha e Simão Filho (2017), também sob o ponto de vista da Teoria dos Círculos Concêntricos, explicam que a privacidade estabelecida na circunferência de maior amplitude e externamente, abrange uma maior parte de relações interpessoais cujas informações são de interesse público, visto sua importância para a vida em sociedade, tais como a rotina do indivíduo ou dados sobre seu patrimônio.

Figura 1 - Teoria dos Círculos Concêntricos



Fonte: Cunha e Simão Filho (2017, p. 11).

No círculo do meio está localizada a intimidade, cuja proteção é reforçada em relação à anteriormente citada, como os sigilos bancários, telefônicos, profissionais, familiares, conversações e eventos íntimos que são informações que somente são divididas com quem a pessoa deposite confiança, explicam Cunha e Simão Filho (2017). E bem ao centro da proteção está o segredo, que como lecionam os autores está no patamar mais profundo dos interesses da pessoa humana e de difícil visualização por terceiros. É onde os cidadãos não têm interesse de divulgar a outrem, nem esses podem exigir que aqueles lhes deem publicidade, apontam Cunha e Simão Filho (2017). Bauman e Lyon (2014) também

posicionam o segredo como sendo parte do conhecimento proibido para com terceiros, ao abordar a vigilância como fenômeno característico e central da modernidade, veja-se *in verbis*:

> Um segredo, tal como outras categorias de propriedades pessoais, é por definição a parte do conhecimento cujo compartilhamento com outros é recusada, proibida e/ou estritamente controlada. O sigilo traça e assinala, por assim dizer, a fronteira da privacidade; esta é o espaço daquilo que é do domínio da própria pessoa, o território de sua soberania total, no qual se tem o poder abrangente e indivisível de decidir "o que e quem eu sou", e do qual se pode lançar e relançar a campanha para ter e manter suas decisões reconhecidas e respeitadas (BAUMAN; LYON, 2014, p. 431).

Nesse sentido, na delimitação do tema privacidade veja-se que este deve estar circunscrito e guardar relação com assuntos referentes às relações interpessoais do indivíduo, seu patrimônio, sua saúde ou rotina, não se confundindo com intimidade e segredo. Para as hipóteses de intimidade e segredo pode-se apontar para os dados sensíveis, que possuem uma camada a mais de proteção pela Lei nº 13.709/2020.

Em recente decisão de 06 de maio de 2020, julgando a ADI n. 6387 ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil, o Supremo Tribunal Federal declarou em liminar a inconstitucionalidade de Medida Provisória n. 954/2020 que permitia o IBGE realizar o censo, através de informações coletadas junto às empresas que prestam serviços de telecomunicações. O objetivo da Medida Provisória n. 954/2020 era manter a atividade de recenseamento mesmo durante a pandemia do Covid-19. Na decisão, o STF elevou o direito à privacidade ao patamar constitucional considerando que a Constituição não protege tão somente a intimidade e o sigilo do art. 5º, XII (correspondência, comunicações telegráficas, telefônicas), mas tutela todo dado que tenha a atribuição de corresponder à personalidade humana, dados pessoais. Ou seja, mudou-se um paradigma constitucional ampliando a proteção que antes estava centrada na intimidade e no sigilo das correspondências e das comunicações, para proteger informações referentes a dados pessoais ligados à personalidade.

Nesse sentido, a LGPD define no art. 5º, inciso I um conceito amplo de dado pessoal que é "informação relacionada a pessoa natural identificada ou identificável"(BRASIL, 2018, p. 04), que na verdade repisa o que já vinha previsto na Lei de Acesso à Informação n. 12.527/2011 no art. 4º, IV em que define "informação é aquela relacionada a pessoa natural identificada ou identificável" (BRASIL, 2011, p. 01). Dessarte, o objetivo deste estudo é delimitar as boas práticas das Políticas de Privacidade dos *websites* de no âmbito da LGPD pelas empresas distribuidoras de gás canalizado, respeitando os limites do referencial teórico acima apontado. Entendendo-se por Política de Privacidade um documento presente no

contexto do *website*, em que ali estão consignados os padrões de procedimento relativo ao uso, manuseio, tratamento das informações, que atualmente devem estar de acordo com a Lei Geral de Proteção de Dados.

3 MÉTODO

Vencida a exposição e delimitação quanto ao referencial teórico, tem-se que esta pesquisa se propõe quanto ao procedimento metodológico realizar análise quantitativa e qualitativa, sob o ponto de vista de abordagem do problema. Ou seja, pode-se classificar a pesquisa sob três aspectos: quanto à abordagem do problema; quanto aos seus objetivos; e quanto aos procedimentos técnicos utilizados. No que tange à abordagem do problema, esta pesquisa se classifica em quantitativa e qualitativa, pois traduz em números o nível de adequação às boas práticas da normatização da Lei Geral de Proteção de Dados - LGPD pelas distribuidoras de gás canalizado, através de publicações nas suas páginas na internet, com o que se pretende conhecer as suas abordagens quanto ao novo regramento em suas próprias Políticas de Privacidade. Segundo Raupp e Beuren (2013, p. 92), "a abordagem quantitativa caracteriza-se pelo emprego de instrumentos estatísticos, tanto na coleta quanto no tratamento dos dados". Segundo Oliveira (2011, p.82) "as pesquisas que possuem abordagem qualitativa podem apresentar a complexidade de certo problema, avaliar como suas variáveis interagem entre si e com o todo" trazendo pertinência e validade ao objeto de estudo.

Pode-se considerar que a pesquisa é descritiva, na medida que se considera os seus objetivos, pois pretende descrever a abordagem do conteúdo que as empresas pesquisadas introduzem nas suas Políticas de Privacidade. Gil (2008, p. 28) afirma que as pesquisas deste tipo têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou estabelecimento de relações entre variáveis.

Com base nos procedimentos técnicos utilizados, o estudo pode ser classificado como pesquisa documental. Gil (2008, p. 157) define esse tipo de pesquisa como aquela em que a fonte de coleta de dados está restrita a documentos, escrita ou não, constituindo o que se denomina de fontes primárias. Para realização do estudo, foram utilizadas as Políticas de Privacidade disponibilizadas pelas empresas em seus *websites*, caracterizados, portanto, como fontes primárias. A população definida nesta pesquisa é referente a 12 (doze) distribuidoras de gás natural canalizado do segmento petróleo e gás. A amostra utilizada corresponde às empresas, dentro da população da pesquisa, que divulgaram em seus *web sites* suas Políticas de Privacidade (posição anterior a 10 de julho de 2021). Sendo assim, fazem parte da amostra 12 empresas, que já haviam publicado suas Políticas de Privacidade às vésperas da eficácia da legislação que passou a produzir seus efeitos em 01 de agosto de 2021.

O trabalho de coleta foi realizado em duas etapas, sendo a coleta dos dados referente às Políticas de Privacidade disponibilizadas nos *web sites* e a conferência dos dados de coleta.

Os dados coletados em julho/2021 foram tabulados em excell e classificados partindo-se do entendimento de que as distribuidoras de gás canalizado são consideradas Agentes de Tratamento de dados pessoais no âmbito da implementação de suas Políticas de Privacidade e no acesso ao website. Desse modo, com base no art. 50 da Lei Geral de Proteção de Dados, é que se definiram os itens de boas práticas conforme a previsão legal considerando-se também a referência aos demais dispositivos do corpo legal previsto no Capítulo das Boas Práticas, em vista de que estes dispositivos são complementares e esclarecedores das aplicações do art. 50 da Lei Geral de Proteção de Dados.

Assim, o art. 50 da LGPD fixa uma estrutura que deve estar contida nas Políticas de Privacidade, visto que a regra dispõe que "em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular" devem estar presentes, bem como "na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados" formando assim um padrão de boas práticas a ser seguido (BRASIL, 2018, p. 04).

Desta forma, em razão dos princípios do art. 6º dos incisos VI e VII estarem expressamente elencados no art. 50 como boas práticas é que se entende devem ser abordados, igualmente, de forma expressa. Portanto, para que haja boa prática o Agente de Tratamento deverá ter presente na sua Política de Privacidade questões que atendam expressa e minimamente os princípios da Transparência (inciso VI) e da Segurança (inciso VII). Para averiguar a presença de tais princípios é que se verificou nas políticas a existência de itens que informam a previsão destes princípios, também a possibilidade de atualização constante em vista de que este último item pode ser considerado como extensão a tais princípios. Entendeu-se que a aplicação expressa dos princípios previstos no art. 6º, incisos VI e VII nas Políticas de Privacidade respaldam uma preocupação geral com a adequação da segurança e prevenção de vazamento no cuidado da privacidade dos dados pessoais, razão pela qual se julgou importante esse requisito estar presente nas amostras de boas práticas.

Outros conjuntos de informações relevantes que se entendeu devem estar presentes nas políticas são aqueles que abordam questões sobre dados, tais como: definição dos dados coletados e finalidade da coleta, a definição do tratamento dos dados coletados, informação de compartilhamento com terceiros, informação de compartilhamento internacional, informação a respeito de *cookies,* consentimento do titular se estarão em observância com esse requisito de boa prática. Em relação às ferramentas de controle das boas práticas entendeu-se que

deveriam estar presentes os princípios, a figura do DPO, cujo objetivo é de estabelecer uma relação de confiança com o titular por meio de atuação transparente e que assegure mecanismos de participação efetiva, quanto a propriedade dos dados do titular em que a interface é feita através de um DPO. Um glossário de termos trará certeza e precisão quanto aos institutos utilizados entre as partes e a previsão do descarte de dados.

A fim de avaliar se há cumprimento, quanto estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade se entende que deve conter nas Políticas de Privacidade analisadas itens que prevejam hipóteses de previsão de eliminação/descarte de dados, bem comoa transparência está na informação do uso de *cookies* e como eles são operacionalizados. A letra "f" do art. 50 guarda relação também com a existência do DPO. Assim que, as políticas que relacionam a utilização deste framework acima apontado, como formas de proteção aos dados pessoais em consonância à LGPD se considerou como atuação em boas práticas. Ademais, o Agente de Tratamento estará agindo em boas práticas quando pretender tratar os dados pessoais do Titular, caso observe as hipóteses de consentimento de tratamento dos dados delimitados pelo art. 7º da Lei 13.709/2018. Prevê o dispositivo em comento que para tratar os dados, o Agente de Tratamento precisará do consentimento do Titular (inciso I, assim, se deverá considerar um programa de boa prática quando os dados obtidos de qualquer forma pelo Agente de Tratamento para queobedeçam às regras do art. 7º, I que trazem as hipóteses de possibilidade de tratamentos dos dados pessoais, através do consentimento do Titular.

Vale informar que, na alínea "a", inciso I, §2º do art. 50 aponta como boa prática do Agente de Tratamento estar comprometido com a aplicação da lei de forma abrangente, desse modo pode-se considerar que a eventual observância dos demais princípios elencados pela LGPD agrega valor às boas práticas das CDL investigadas nesse estudo. Portanto, entendeu-se que as políticas que relacionam a utilização dos princípios norteadores da proteção de dados transparecem como resultados de melhores práticas, visto que os princípios são vetores essenciais deste tema.

Agrupou-se a análise em 02 (dois) grupos temáticos onde primeiro se analisou em conjunto de informações quanto as questões abordadas a respeito de tratamento de dados pessoais nas políticas tais como: a coleta de dados, o tratamento e finalidade de dados, compartilhamento com terceiros, compartilhamento internacional, cookies e o consentimento. No segundo grupo a ser analisado agrupou-se o tema quanto as ferramentas que são utilizadas para manejar as boas práticas assim como ocorre com a presença de princípios, a existência de um glossário, em que conceitos bem definidos trazem clareza e certeza no tratamento dos

institutos utilizados, se os princípios definem a governança da Política de Privacidade, se há regra clara para solicitação de eliminação de dados e a existência dedesignação de Encarregado. Assim, a análise de boas práticas das Políticas de Privacidade seguirá como referência os dados coletados, através do fio condutor destes temas acima mencionados que refletem as boas práticas. Abaixo a descrição da coleta realizada com base na definição das letras do inciso I, do art. 50 da LGPD e demais dispositivos que se relacionam, bem como os temas que devam estar presentes nas Políticas de Privacidade abordadas, conforme abaixo:

Quadro 3- Legislação aplicável

TEMA	DEFINIÇÃO	FONTE
PRINCÍPIOS	1. Finalidade2. Adequação 3. Necessidade 4. Livre Acesso 5. Qualidade dos Dados 6. Transparência 7. Segurança 8. Prevenção 9. Não Discriminação 10. Responsabilização 11. Prestação de Contas	**Letra "a" e** Art. 6º
INDICA DPO Encarregado	Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.	Hipótese da Letra "a" eArt. 41
Glossário de Explicações sobre definições legais	I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);IX - agentes de tratamento: o controlador e o operador;X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas	Definições do Art. 5º e Letra "a"

	competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração públicadireta ou indireta ou pessoa jurídica de direito privado sem finslucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivosocial ou estatutário a pesquisa básica ou aplicada de caráterhistórico, científico, tecnológico ou estatístico; eVigência XIX - autoridade nacional: órgão daadministração pública responsável por zelar, implementar e fiscalizar ocumprimento desta Lei em todo o território nacional.	
Definição do Tratamento de Dados	Escrito, verbal, aponta a finalidade do consentimento, informação sobre revogação do consentimento. Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros; ~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~ VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;(Redação dada pela Lei nº 13.853, de 2019)Vigência IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.	Hipótese do Art. 7º
Tratamento de Dados pessoais ou NÃO	1. Mediante consentimento 2 Cumprimento de obrigação legal ou regulatória 3 pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres	Hipóteses do Art. 7º
Acesso do titular aos Dados	I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. Informações sobre a alteração do tratamento dos dados, com possibilidade de revogação.	Art. 9º
Tratamento de Dados Sensíveis	I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:a) cumprimento de obrigação legal ou	Art. 11

	regulatória pelo controlador;b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado porprofissionais de saúde, serviços de saúde ou autoridade sanitária; ou(Redação dada pelaLei nº 13.853, de 2019)Vigência g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II docaputdeste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I docaputdo art. 23 desta Lei. § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.	

Fonte: elaborado a partir dos dados da pesquisa (2021).

A técnica de análise dos dados que foi utilizada é a análise documental, que segundo Teixeira (2003, p.194) “a maioria das técnicas de análise [...] tem o propósito de contar a frequência de um fenômeno e procurar identificar relações entre os fenômenos, com a interpretação dos dados recorrendo a modelos conceituais definidos a *priori*”. Portanto, foi feita análise de essência das Políticas de Privacidade, buscando além de encontrar a menção ou não dos assuntos no conteúdo do seu texto, bem como a forma de abordagem em comparação dentre as distribuidoras de gás natural referente aos mesmos itens e como são tratados.

No que tange a análise da estrutura de apresentação de todos os documentos, foi realizada uma tabulação em Excel da estrutura de cada um dos códigos analisados de forma a permitir identificar os padrões que compõem suas Políticas de Privacidade. Para essa análise, utilizou-se como base categórica dos tópicos os assuntos recomendados no art. 50 da LGPD como elementos necessários para constar nas políticas, a fim de representar boas práticas.

4 ANÁLISE DOS DADOS

Através da análise dos dados é que se pretende avaliar se as Políticas de Privacidade atendem os requisitos de boas práticas de governança. Para tal fim, importante que se tenha presente, neste exercício, o conceito de boas práticas de governança corporativa. Portanto, é sobre esse critério que se entende as boas práticas de Governança Corporativa que deve ser compreendida à luz do quanto consta no *caput* do art. 50 da LGPD, ao mencionar que são os controladores e operadores, que no âmbito de suas competências detém a obrigação de formular regras de boas práticas e de governança para observar os direitos dos titulares, quanto aos seus dados pessoais.

Deste modo, também calha mencionar a conceituação da governança corporativa a partir de estrutura de poder dada pelo Cadbury Committee no qual "A governança corporativa é o sistema e a estrutura de poder que regem os mecanismos através dos quais as companhias são dirigidas e controladas" (CADBURY COMMITTEE, 1992, p. 01). Portanto, a análise das boas práticas é quanto a visão da governança dos dados pessoais havendo um comprometimento de toda a compleição da empresa, partindo do mais alto escalão até os demais colaboradores, que deverão agir em uma visão somente na proteção dos dados pessoais dos Titulares.

4.1 A POLÍTICA DE PRIVACIDADE SOB O PONTO DE VISTA DAS BOAS PRÁTICAS QUANTO A ORGANIZAÇÃO, FUNCIONAMENTO E PROCEDIMENTOS

O objetivo deste item é apresentar sob o ponto de vista da organização, funcionamento e procedimento das boas práticas como os dados pessoais dos titulares são tratados pela gestão na amostragem das distribuidoras de gás natural, quanto a adoção das recomendações pela LGPD, art. 50. Para isso, foi elaborada a Tabela 1, onde estão selecionados itens como informação sobre compartilhamento com terceiros, definição sobre dados coletados e finalidade de tratamento, informação sobre compartilhamento internacional, informa sobre cookies e o consentimento tais itens formam um conjunto que espelha nas Políticas de Privacidade a organização, o funcionamento e procedimentos exigidos no caput do art. 50 para que se tenha boas práticas no uso dos dados pessoais.

Tabela 1 - Dados

	Informa sobre compartilhamento com 3º, art. 9 LGPD	Definedados coletados e finalidade de tratamento	Informa possibilidade de compartilhamento Internacional C	Informa Cookies Na Política de Privacidade	Informa Consentimento Para dados pessoais	TOTAL
1.NATURGY	1	1	1	0	1	80 %
2. GASMIG	0	1	0	1	Zero	40%
3. COMGAS	1	1	0	1	1	80%
4. MITSUI	1	1	0	1	1	80%
5.MSGAS	1	1	0	0	1	60%
6. GASPETRO	0	0	0	0	Zero	ZERO
7. COPERGAS	0	0	0	0	1	ZERO
8. SCGAS	1	1	1	0	1	80%
9. ESGAS	1	1	0	1	1	80%
10. GASBRASILIANO	1	1	0	1	1	80%4
11. COMPAGAS	1	1	0	0	1	80%
12. SULGAS	1	1	1	1	1	100%
TOTAL	9	10	3	6	10	
% CUMPRIMENTO	75%	83,33%	18,75%	50%	83,33	

Fonte: elaborado a partir dos dados da pesquisa (2021).

Veja-se que pela tabela incluímos pontuação 01, quanto ao cumprimento dos parâmetros selecionados relativos a dados como representativos da organização, funcionamento e procedimentos e incluímos zero de pontuação, quando está ausente o parâmetro selecionado, conforme a metodologia deste trabalho. O cruzamento destes dados tem como objetivo verificar se os itens referentes a dados em geral presentes nas Políticas de Privacidade refletem boas práticas nas questões sobre dados pessoais, conforme orienta a LGPD. Assim, entendeu-se que dentre as hipóteses de tratamento de dados o compartilhamento com terceiros é o que gera maior potencial de risco, portanto ingressa no rol de itens de análise quanto às boas práticas por ser relevante a transparência quanto a esse item, tendo-se o §1º do art. 50 da LGPD como elemento orientador,

> 1º - Ao estabelecerregras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular(BRASIL, 2018, p. 15).

Nesse sentido, primeiro item da análise, o compartilhamento com terceiros se relaciona com a gravidade de riscos na forma do §1º do art. 50 da lei, sendo item relevante a se considerar no rol das boas práticas. Nassif Taleb, na obra A Lógica do Cisne Negro (TALEB,2010 p. 78), pontua que toda a relação com dados e internet por estarem sujeitos a uma aleatoriedade extrema, é que se considera um grande risco de responsabilização sobre dados pessoais obtidos pela internet, por força de sua aleatoriedade característica.

Assim que, a 1ª Tabela é formada pelo compartilhamento com terceiros, incluiu-se como item a definição dos dados coletados e a sua finalidade, a transferência internacional de dados, a existência de política de *cookies* sobre os dados e a informação do consentimento como dados que devem estar presentes nas Políticas de Privacidade analisadas. Como resultado pretende-se que as amostras selecionadas demonstrem estar de acordo com o percentual de cumprimento dos parâmetros selecionados, considerando-se como aponta a LGPD que detém controle quanto a organização, o funcionamento e o procedimentos sobre os dados que tem acesso ou coletam no website, que ao final denotam as boas práticas na LGPD, requeridos no caput do art. 50.

Sobre informação de compartilhamento de dados com terceiros 75% da amostra deixa claro como esse assunto é tratado através de sua política de privacidade com a informação de que há ou não há compartilhamento de dados com terceiros, bem como esclarecendo quais razões do compartilhamento. O esclarecimento desta informação pelas empresas que

informam que compartilham dados com terceiros por diferentes razões elencadas, mas em sua maioria informam que compartilham para manter o serviço adequado e proíbem o uso de dados por terceiros para outro fim, de uma certa forma afastando eventuais possibilidades de colocar em risco os dados pessoais do titular, visto que o compartilhamento com terceiros é somente o necessário. Nessa situação temos: Naturgy, Sulgas, Compagas, Gasbrasiliano, Esgas, SCgas, Mitsui, Comgas, Gasmig. Dentre as empresas que trazem informações sobre compartilhamento com terceiros a MSgas é a única que declara não fazer esse compartilhamento, enquanto a SCgas traz um detalhamento técnico em TI que se diferencia das demais.

Veja-se que as questões sobre compartilhamento de dados com terceiros são pontos relevantes para a nova Lei de Proteção de Dados Pessoais, visto que através da troca de dados com terceiros é que os eventos de maior importância do mundo hiperconectado ocorrem com o que se permite o acesso livre a uma série de valiosas informações prontas a se transformarem em mercadoria ou até mesmo predizerem comportamentos de vendas no mercado, como aponta Zuboff (2019). No caso da amostra, a informação de que se faz apenas o compartilhamento com terceiros de forma suficiente para poder acessar os serviços, afasta as hipóteses trazidas pela autora acima.

Outro fator que interessante que decorre do pouco compartilhamento de dados com terceiros da amostra, é que há menor exposição ao risco de incidentes de segurança com os dados pessoais. Nesse sentido, o Centro de Estudos, Respostas e Treinamento de Incidentes de Segurança no Brasil (CERT) aponta algumas razões pelas quais as motivações dos atacantes na ação de acesso aos dados como sendo das mais variadas e, muitas vezes, difíceis de serem determinadas. Apesar de o volume de negócios do mercado de gás canalizado, estar no arcabouço de razões que o CERT levanta para que ocorram ataques aos dados na internet, a escassez de compartilhamento de dados com terceiros reduz as possibilidades de meios de ataques. Veja-se como o CERT classifica o interesse pelos ataques aos dados que estão sob a custódia de Controladores e Operadores, *verbis*:

> a) Ganho econômico ou financeiro: são ataques direcionados principalmente a empresas e realizados, por exemplo, para causar prejuízos a concorrentes (concorrência desleal), tentar extorquir dinheiro e como forma de demonstrar "poder de fogo" a possíveis clientes e alvos;
> b) Represália ou vingança: são ataques realizados como resposta a fatos que os atacantes julgam ser injustos ou que, de alguma forma, os deixaram descontentes;
> c) Crença ideológica ou política: são ataques realizados por desavenças políticas e diferenças religiosas. Costumam estar associados à prática do hacktivismo;
> d) Distração para outros ataques: são ataques realizados com o objetivo de distrair as equipes de rede e segurança das empresas atacadas pois, enquanto estão ocupados

> tentando mitigar o ataque DDoS (Denay Service -negação a serviço), os atacantes aproveitam para efetuar outras atividades maliciosas como, por exemplo, furtar dados e invadir sistemas;
> e) Desafio intelectual: na sua maioria, os atacantes desta categoria são iniciantes e realizam os ataques para experimentar e aprender como realizar diversos ataques DDoS;
> f) Outros: motivações individuais e genéricas, como tentativa de adiamento de prazos para a entrega de documentos e trabalhos(CERT, 2021, p. 2).

Desse modo, a preocupação da LGPD com os compartilhamentos de dados com terceiros se assenta na seara da proteção legal ao Titular, tratando-se de requisito essencial às boas práticas considerando-se o atual *approach* do mercado de gás natural canalizado, em relação aos dados pessoais dos titulares e a legislação aplicável. Nesse sentido, a amostra analisada nesse estudo, ao verificar que 75% informam sobre compartilhamento de dados com terceiros depreende-se que a preocupação em observar a LGPD vem sendo preservada por este segmento de mercado.

A informação quanto a definição dos dados coletados e a finalidade destes dados estão presente em 83,33% da amostra. Portanto, bem mais da metade da amostra apresenta nas Políticas da Privacidade as informações a respeito de quais dados interessam na navegação e o porquê do interesse. Em geral, a informação sobre quais dados são capturados são as seguintes: os dados do navegador de acesso ao site, o modelo de dispositivo móvel, o sistema operacional utilizado, o provedor de conexão, o endereço IP e *logs*. As únicas distribuidoras da amostra que não trazem essa informação disponível nas publicações sobre privacidade dos titulares no site são a Gaspetro e a Copergas.

As informações prestadas aos titulares têm a função de que estes possam expressar corretamente o seu consentimento, que é "a linha mestra para tratamento dos dados" (PINHEIRO, 2021, p.44), portanto definir a informação em relação ao titular informando quais dados são coletados e a finalidade pelo Agente de Tratamento guarda obediência ao art. 6º, inciso VI que traz o princípio da transparência e da finalidade como essenciais ao consentimento e consectário tratamento de dados em que:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> [...]
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (BRASIL, 2018, p.04).

Outro aspecto que se revela é de que parte da amostra como a Mitsui e Sulgas informam que podem coletar dados analíticos para produzir análises estatísticas dos dados

pessoais. Entretanto, não há informações mais precisas a este respeito quanto a quais análises estatísticas as distribuidoras constroem através de dados analíticos, ou seja, a "receita da vigilância" (ZUBOFF, 2019, p.253) pode estar presente na amostra. Dado curioso, é que a única distribuidora que informa coletar dados quanto ao gênero do titular é a Comgas, que declara no item sobre tratamento de dados que coleta a informação quanto ao gênero do Titular. Veja-se que em princípio a simples indicação de gênero não é considerada dado sensível, conforme Redecker et al. (2021, p.1851), visto que se faz necessária a existência de afetação à personalidade, em que no caso da Comgas, trata-se de mera indicação de gênero que simplesmente não possui essa conotação.

Outro dado que analisamos é o compartilhamento internacional. Da amostra duas distribuidoras informam que realizam ou podem realizar compartilhamento internacional, mas não especificam a finalidade Naturgy, SCGas. Nesse sentido, é de se considerar que o ambiente digital é naturalmente internacional (PINHEIRO, 2020, p. 120), entretanto a legislação deixa claro que ainda assim as soberanias dos países devem ser observadas. Dessa forma, quando a distribuidora declara o compartilhamento internacional deverá manifestar a finalidade para tal, como forma de se resguardar quanto a competência em eventual debate sobre incidente de dados, evitando-se a esfera internacional. Entende-se salutar, sobre essa questão, a informação da SCGAs de que o acesso ao site fora do Brasil remeterá, ainda assim, o visitante ao registro dos dados em ambiente brasileiro e terá suas informações armazenadas, sob a orientação da legislação brasileira visto que, desta forma, resguarda para o âmbito brasileiro eventuais debates a respeito de incidente de segurança que possam vir a ocorrer eventualmente no acesso internacional. Outra distribuidora que aborda o tema de compartilhamento internacional é a Sulgas, que expressamente informa que não compartilha dados em ambiente internacional. Vale apontar que a Sulgas informa também no mesmo dispositivo, que obedece aos princípios da LGPD, mormente da finalidade, o que vem ao encontro da informação de que não realiza transferência de dados internacionais, pois não há finalidade para que se faça esta transferência de dados pessoais de forma internacional.

Mais um item que está na análise são os *cookies*. Na Política de Privacidade, a SCGás e a ESGás deixam claro que se utilizam de *cookies* para capturar informações e também especificam quanto a espécie de *cookies* que são utilizados e como eles funcionam, já a Sulgas informa *cookies* de forma mais breve. Da amostra analisada, metade (50%) informa aos titulares na Política de Privacidade, sobre a utilização de *cookies*. De acordo com esta boa prática de informar *cookies* na Política de Privacidade estão: Gasmig, Scgas, Comgas, Mitsui, Esgas, Sulgas, Gasbrasiliano, trazendo a informação completa, mesmo que a maioria dos

titulares ainda não tenham condições de entender a informação na sua totalidade, em razão da tecnicidade. As outras 07 (sete) empresas da amostra não informam na Política de Privacidade como os *cookies* operam diante da privacidade de dados dos titulares. A SCGAS, por exemplo, informa utilizar *cookies* essenciais, funcionais e de desempenho, mas também usa *web beacons* (*web bugs*) que são *cookies* de rastreamento, conforme explica o site G1 na publicação "Saiba como os *cookies* e os *web beacons* rastreiam você" (ROHR, 2017, p. 01). Os web beacons obtém informações a respeito do histórico de navegação acessando o próprio web site e em outros web sites que usam a mesma ferramenta, realizando um rastreio da navegação do usuário.

Continuando em nossa amostra a Gasmig também informa a utilização de *cookies*, a finalidade do uso e os tipos de *cookies* usados sendo eles: *cookies* essenciais, *cookies* de preferência, *cookies* analíticos e de marketing e informa, também, a possibilidade de desativar *cookies* advertindo de as complicações ao usuário optar por não utilizar a ferramenta. A Comgas informa na política de privacidade que registra *cookies*, sem maiores informações a respeito, sem a finalidade para o registro e as espécies de *cookies* aplicados. A Mitsui, por sua vez, informa que registra *cookies* bem como explica quais espécies de *cookies* irá registrar no computador do visitante usuário, apresenta a finalidade e faz o registro de que utiliza somente *cookies* de sessão e persistentes. A distribuidora ESGAS também informa que registra os *cookies*, a sua finalidade, bem como informa as espécies de *cookies* que são *cookies* necessário, de desempenho e funcionalidade, também o orienta a desabilitação segmentada e geral, revelando boa prática no manejo dos *cookies*. A SULGAS informa os *cookies* e os define, informa as finalidades para que utiliza, sem definir a classificação. A GASBRASILIANO informa que faz uso de *cookies*, mas não gera informação detalhada a respeito.

Em conclusão sobre *cookies*, no universo da amostra, depreende-se que o fato de não constarem em todas as Políticas de Privacidade analisadas, demonstra que ainda não alcançaram um nível de atenção e importância, que poderia ser exigido para estas ferramentas. Também, aquelas distribuidoras que trazem no bojo da política informações que utilizam *cookies* nem sempre é feito na forma das boas práticas da LGPD, que exige para o exercício do consentimento a transparência e a finalidade, principalmente quando há tratamento por *cookies* de analítica. Aponte-se, nesse sentido, para as grandes empresas de tecnologia que os *cookies* são ferramentas que despertam bastante atenção, e na amostra esta preocupação não ficou compatível com a importância do tema no mercado. Nesse sentido, há uma mudança de paradigmas em termos de soluções diante dos regulamentos sobre privacidade, tendo-se a

anunciada adoção da ferramenta *PrivacySandBox* pelo Google como forma de solução, afastando a utilização de *cookies* de terceiros.

> […]
> Para as equipes de anúncios do Google, as tecnologias Privacy Sandbox representam o futuro de como nossos anúncios e produtos de medição funcionarão na web. Encorajamos outros a se juntarem a nós na definição dessa nova abordagem que criará melhores experiências para os consumidores, ao mesmo tempo em que fornece soluções mais duráveis para a indústria de anúncios. À medida que avançamos em 2021, você pode esperar ouvir mais sobre os progressos que estão sendo feitos no Privacy Sandbox, incluindo mais oportunidades para você começar a testar essas novas tecnologias em suas campanhas. Portanto, mantenha-se engajado nas discussões públicas sobre as propostas do Privacy Sandbox em fóruns como o Grupo de Negócios de Publicidade Web Aprimorada do W3C, ou trabalhe com seus parceiros de tecnologia para avaliar e experimentar as propostas que já estão em testes de origem. Juntos, podemos remodelar a web para que funcione melhor para todos (TEMKIM, 2021, p. 01).

Destarte, não encontramos evidências na amostra de utilização de *cookies* nos mesmos parâmetros de relevância, quanto a segurança e transparência que devem pautar as boas práticas podendo ser um item a ser revisado pelas distribuidoras. O último dado analisado tratou-se do consentimento, que para a Lei Geral de Proteção de Dados é o núcleo do sistema, tendo-se todos os demais itens importantes gravitando em torno do consentimento, tais como a transparência, a segurança, a finalidade, etc. O consentimento para tratamento de dados pessoais do titular, mesmo sendo prestado pode ser revogável a qualquer tempo, é o que dispõe a LGPD.

A amostra pesquisada revelou ter verdadeira preocupação com o consentimento do titular sobre o tratamento de dados pessoais, visto que 80% das empresas, cujos *websites* foram analisados estão atentos ao consentimento pelo titular do tratamento de dados pessoais, acertadamente. Nesse passo, entende-se um reconhecimento das distribuidoras de gás de que existe uma autodeterminação informacional pelo titular dos dados prestada conforme o comportamento do mercado. Assim, as distribuidoras reconhecem que o titular detém originariamente o direito geral da personalidade, em que os dados do indivíduo são somente deles, cabendo tão somente a eles a determinação do seu destino. Entretanto, caso o titular não consinta em fornecer seus dados pessoais as páginas não possuem uma alternativa a não ser reduzir a experiência. Na medida em que, o titular é informado de que o não consentimento poderá reduzir a sua experiência na página, não se pode afirmar que a escolha do titular nesse momento seja autodeterminada, que se esteja diante de um consentimento livre.

Nesse sentido, as distribuidoras de gás agem conforme a regulamentação preconiza, ainda que de forma institucional os titulares de dados tenham autodeterminação pouco fiel ao

seu real consentimento, quanto ao tratamento de seus dados pessoais, na medida em que possuem poucas condições para fazê-lo de forma legítima às suas convicções, também as distribuidoras não detêm capacitaçãocomo o Google para criar novos modelos. Ainda que a legislação não tenha evoluído a esse patamar de certeza, o mercado de gás poderá dar esse passo à frente assim como Google afastou os cookies de terceiros, adotando o *Privacy Sand Box*. Como informa Doneda (2020), o consentimento caso limitado de alguma forma em uma estrutura negocial, perderia sua razão de ser. Como o contexto da LGPD é recente, estas questões deverão ser tratadas no curso da aplicação da legislação, devendo os atores deste mercado estar atentos para acompanhar eventuais mudanças.

4.2 ANÁLISE DAS FERRAMENTAS PARA CONTROLE DO PROGRAMA DAS BOAS PRÁTICAS DE PRIVACIDADE

A segunda tabela que se apresenta é aquela que entendemos representa as ferramentas que se tem disponível para controle do programa de boas práticas. Assim, conforme o art. 50 em especial da LGPD e demais dispositivos é que se analisou a presença dos itens referentes a princípios, indicação de DPO, glossário de termos, eliminação de dados e atualização constante. Confira-se a seguir:

Tabela 2 - Ferramentas princípios, dpo, glossário, atualização constante

Coluna1	Coluna2	Coluna3	Coluna 4	Coluna 6	Coluna 8	TOTAL Específico
	Princípios Expressos Art. 6º, art. 50, I, a	Indica DPO pessoa físicaart. 41 e 50, I, a, g	Glossário de Termos Art. 5º art. 50, I, a	Prevê Eliminação/descarte art. 50, I, d	Atualização Constante art. 50 "h"	TOTAL
NATURGY	0	0	1	0	1	40%
GASMIG	1	0	1	0	1	60%
COMGAS	0	0	1	1	1	60%
MITSUI	0	0	1	0	1	40%
MSGAS	0	1	1	0	1	60%
GASPETRO	0	0	0	0	0	0
COPERGAS	0	1	0	0	0	20%
SCGAS	0	0	0	0	1	20%
ESGAS	0	0	0	0	1	20%
GASBRASILIANO	1	0	1	0	0	20%
COMPAGAS	0	1	1	1	1	80%
SULGAS	0	1	1	0	1	60%
TOTAL GERAL	16,6%	33,33%	66,66%	8,33%	75%	

Fonte: elaborado a partir dos dados da pesquisa (2021).

O art. 50 da LGPD aponta itens que identificamos como ferramentas às boas práticas, a fim de evitar que situações como as apontadas pelo CERT - Centro de Estudos de Respostas e Tratamento de Incidentes no Brasil ocorram ou se ocorrerem produzam menores impactos, na medida em que se tem a presença de ferramentas no controle da manutenção da privacidade. Deste modo, a presença de princípios relativos à privacidade na estrutura do *privacy by design*, dão sentido aos dados coletados imprimindo uma direção e um senso de organização, sendo no mínimo exigidos o princípio da segurança e o princípio da transparência, ferramentas que vão formando o contorno do escopo de proteção aos dados até se chegar nas questões práticas propriamente ditas.

No mesmo sentido, é que incluímos informações referentes à existência de um glossário, visto que ao se fixar parâmetros sobre quais os temas estão sendo abordados na política, também se proporciona o senso de organização de como a privacidade está sendo tratada naquela política, fixando clareza quanto aos novos termos trazidos pela LGPD, não deixando qualquer dúvida sobre os conceitos tratados a respeito de privacidade. Sobre esses dois pontos tem-se que os princípios expressos nas Políticas de Privacidade analisadas demonstram serem pontos de menor importância para a amostra, por não estarem tão presentes em boa parte dos documentos investigados, ainda que se entenda, que tais princípios são verdadeiras bússolas que podem dar a correta direção interpretativa para as informações as quais a empresa pretende clarificar tanto internamente, quanto ao cliente ou visitante do *website*; ainda assim, não foram considerados como itens relevantes para constar nos documentos encontrados sobre privacidade, pois nem sempre as encontramos na pesquisa.

Sob o ponto de vista de atendimento dos princípios no bojo das Políticas de Privacidade, somente 16,6% da amostra apresentou preocupação em deixar estes itens presentes de forma expressa em suas políticas. O art. 50 da LGPD dispõe que ao mínimo os princípios da transparência e segurança devem estar presentes para que se tenha uma boa prática de governança em Privacidade de dados pessoais, ainda que o art. 6º aponte para um elenco bem maior que compõe: finalidade, adequação, necessidade, livre acesso, transparência, segurança, prestação de contas e responsabilização. Os princípios são o orientador do perfil de como as decisões a respeito de dados pessoais devem se proceder, razão pela qual a ausência destes condutores é inestimável.

Parte da amostra que cumpre o requisito do art. 50 quanto esclarece de que forma expressa os critérios principiológicos da política de privacidade são a Gasmig, e a Gasbrasiliano. Nesse diapasão, tem-se que os princípios declarados são garantias de que os dados pessoais serão pautados com a observância legal de serem direitos dos titulares, visto

que criam um framework informativo sob qual prisma os dados pessoais eventualmente capturados serão tratados, conferindo segurança ao titular de dados.

Dentre as amostras colhidas, tem-se a Gasmig única distribuidora de gás natural analisada, que trouxe na sua política praticamente todo o elenco de princípios apontados pela legislação (não constou apenas qualidade dos dados e incluiu boa-fé) informando ao titular como cada um deles é aplicado pela empresa, na hipótese em que estiver como Controladora dos dados do titular. Já a Gasbrasiliano, que também incluiu os princípios na sua Política de Privacidade não faz de forma tão detalhada, mas deixa claro que aplica de maneira apropriada e que acolhe todos os princípios da LGPD na sua política de privacidade, nas hipóteses em que fizer tratamento de dados pessoais, declarando respeito a autodeterminação informativa. Portanto, a inserção dos princípios é assunto que poderá ser mais bem trabalhado na amostra, pois se trata de declaração da governança da proteção de dados pessoais.

Nesse cenário, a Política de Privacidade do site faz parte da estrutura de todos os documentos de proteção de dados, ou seja, é um dos instrumentos de implementação do *privacy by design,* razão pela qual incluir os princípios traz transparência quanto aos métodos utilizados pela empresa. Entende-se por *Privacy* by *Design* o conjunto de documentos que dispõe sobre o tratamento de dados pelo Controlador, sob o ponto de vista de todo o ciclo de vida do negócio.

Outro requisito analisado na amostra é a correta indicação de um Encarregado ou *DPO*. A existência da indicação pelo Controlador ou Operador de dados de um Encarregado ou *DPO* é outro dado de relevância nas Políticas de Privacidade analisadas da amostra, visto que é esta figura quem faz a interface entre o titular de dados e a empresa, também entre a empresa e a Autoridade Nacional de Proteção de Dados Pessoais-ANDP. Desse modo, a tarefa do Encarregado ou *DPO* é de informação ao Titular de Dados em todas as situações solicitadas, principalmente em relação a alteração do consentimento ou quando ocorrer caso de incidente ou informar à ANDP quando cabível. No caso da amostra, ao não haver a indicação de figura certa para responder às questões de privacidade, ao se enfrentar uma situação de incidente de informação não haverá a interface correta com o titular de dados ou com a ANDP. Em especial, em relação à ANDP, deverá o Controlador de Dados estar apto para cumprir exigências já previstas pela regulamentação a respeito de possíveis requerimentos feitos pela ANDP, como a remessas do Relatório de Impacto à Proteção de Dados, para análise da Autoridade. Ao não haver a definição desta figura pelas distribuidoras fica prejudicada a relação com o órgão fiscalizador, podendo por essa razão ser imposta multa. Desse modo, é o Encarregado de Dados que deve estar responsabilizado no âmbito do

organograma do Controlador a responder para a ANDP, exatamente como prescreve a LGPD, sendo que a atenção a esse item das boas práticas é essencial.

A situação de fragilidade de indicação da figura do Encarregado de Dados ou DPO apresentada no cenário da amostra pode decorrer em razão de que se trata de novidade, no cenário brasileiro. A LGPD reproduz a figura criada com a edição do Regulamento Geral de Dados Pessoais da União Europeia, que passa a existir com a tarefa de fazer o controle dos dados pessoais que trafegam no ambiente corporativo e governamental, bem como faz a interface com os órgãos oficiais responsáveis pelo controle. Observa-se que não houve na amostra hipóteses de Encarregado Geral ou *Data Protection Supervisor*. Em alguns desenhos empresariais corporativos ou de governo tem-se também essa figura de um *Data Protection Supervisor*, a fim de controlar os demais *officers* quando o ambiente for muito volumoso para que somente um titular consiga responder por todas as situações. No caso da nossa amostra, não houve essa situação em nenhum caso.

Apesar de a legislação deixar claro quanto a forma de indicação do Encarregado, não se verificou na amostra a repercussão destes requisitos. Desse modo, 33,33% da amostra indicam o DPO ou Encarregado na forma como descrita na legislação, através da indicação de pessoa física. Em análise de situações correlatas no ambiente em que vigora o GDPR, houve também a mesma situação de não aplicação do modelo legal como seu observa no capítulo 2. Entretanto, situações que não seguiram o modelo legal no ordenamento paradigma sofreram sanções pela aplicação do GDPR, e pela tabela que verificamos no site *Enforcement Tracker* (2021) colacionado no item 2.3, a tendência é de aumento de multas no decurso do tempo.

De certa forma, a estatística que colacionamos no referencial teórico referente à casos similares na União Europeia, bem ilustra o resultado obtido em nossa amostra, visto que em boa parte dos achados as distribuidoras brasileiras ainda não apontam o DPO na forma que a Lei Geral de Proteção de Dados impõe, utilizando outras fórmulas que poderão ser interpretadas pela Autoridade brasileira como violadoras, conforme vem ocorrendo na precursora GDPR. A estatística Europeia guarda uma referência com os resultados que averiguamos, em vista de que somente 03 distribuidoras da amostra apresentam adequação ao regulamento de dados, na forma como preconizado pela lei. Portanto, o paradigma traça um fiel entendimento de como a lei vem sendo interpretada quanto a exigência desta figura do Encarregado ou DPO, que muitas das vezes é negada sua existência pelos Agentes de Tratamento, em razão de instituírem diferentes modelos de responsáveis pela interface entre estes e outros meios, de forma diferente do quanto orienta a legislação.

Em sendo a LGPD um regramento inspirado na lei Europeia, pode ocorrer o mesmo

movimento aqui em relação ao volume de aplicação de multas, inclusive porque há previsão legal de aplicação de multas até R$50 milhões por infração ou em 2% do faturamento, que já podem ser fixadas em virtude que o regulamento da ANPD foi publicado em 28 de outubro último. Ainda que não seja da nossa cultura a aplicação de multas pesadas por descumprimento de obrigações, a LGPD ao fixar o patamar de valores indica a intenção do legislador quanto à multa, sendo que o Encarregado por exercer o papel de interface com a autoridade fiscalizadora desempenha um papel importante devendo ser observado. Ao exemplo do apontado, algumas distribuidoras da amostra utilizam o canal da LAI como contato da privacidade ou disponibilizam qualquer outra forma de contato como ouvidoria do canal de denúncias ou um e-mail corporativo geral para tratar dos temas de privacidade, não segregando a atividade de Privacidade das demais atividades com interface ao público em geral, e não definindo um DPO enquanto pessoa física ou jurídica.

Também é ponto relevante para as boas práticas, a definição de glossário de termos em vista de que a LGPD se utiliza de uma terminologia própria, tendo-se na legislação a definição de diversos termos novos. Nesse contexto, tem-se que metade da amostra estudada inclui em suas políticas a definição dos termos utilizados pela LGPD, através de glossário de termos. Entende-se que tal item está presente no item organização apontado pelo art. 50 da lei no sentido de sistematização, de haver um método ou padrão para se ter boas práticas. Na medida em que a LGPD trouxe em seu arcabouço novos termos, novas terminologias e aplicações diferentes para termos já conhecidos (dados pessoais e dados sensíveis, e.g) é que se percebe a importância da presença do item de definição de termos conferindo uma lógica própria para que se configure uma boa prática em privacidade, pois ao conferir clareza e transparência ao tema tratado está sistematizando e organizando.

Dentre os glossários encontrados, alguns são extremamente simples quando se faz um contraponto com o quanto a própria LGPD traz em seu texto, visto que a lei apresenta dezenove expressões novas a merecer definição específica na legislação. Sob esse ponto de vista, a norma reconhece a importância de se estabelecer com clareza parâmetros de significado, quando esclarece sobre o que se tratam os dezenove itens que elucidou.

Seguindo-se a análise do quanto as CDL's incluem sobre definição de termos nas suas Políticas de Privacidade é que se inicia com a Gasmig que incluiu doze termos, a Naturgy traz oito definições, a Comgas seis definições, a Mitsui apenas duas definições (dados pessoais e processamento), MSGas com três definições, Gasbrasiliano também com seis definições, Compagas traz nove definições e Sulgas são dez definições. Dentre os termos essenciais se entende inafastável constar as seguintes definições, por se tratar de verdadeiros institutos com

significados próprios no contexto da privacidade quais sejam: (i) dados pessoais, (ii) dados sensíveis, (iii) dado anonimizado, (iv) tratamento, (v) titular, (vi) Controlador, (vii) Operador, (viii) Agentes de Tratamento, (ix) Consentimento, (x) Anonimização, (xi) Eliminação, (xii) Compartilhamento, (xiii) transferência internacional de dados. Entende-se que dos dezenove itens presentes na legislação pelo menos doze deles deveriam estar bem definidos no escopo das políticas, para que o titular de dados pudesse ter a exata fotografia da situação dos seus dados junto àquele distribuidor de gás natural, visto que estes minimamente caracterizam o ciclo de vida dos dados pessoais junto a empresa.

Do ponto de vista, da eliminação de dados a análise aqui busca identificar no *website* não somente a informação do direito a eliminação, mas a possibilidade da efetiva execução do pedido de descarte pelo titular. A amostra analisada não apresentou na Política de Privacidade a informação necessária de como o titular dos dados deverá proceder para requerer a eliminação. A maioria das distribuidoras aponta que é um direito do titular, mas não orienta como o titular poderá exercer este direito, o que dificulta a execução do direito para o titular.

Nesse sentido, a única distribuidora que informa as regras para solicitação do descarte de dados é a Compagas do Paraná, as demais informam que é um direito do titular sem considerar orientações de como o titular faz o exercício. Valendo lembrar que o direito de eliminação deve ser exercido de forma expressa, ou seja, é necessário que o titular requeira/peticione para o Agente de Tratamento que deseja a eliminação dos seus dados. Não havendo a informação do procedimento junto ao Agente de Tratamento deverá o titular, antes de tudo, requerer informações quanto ao procedimento do seu pedido; enquanto de regra essa informação já deveria estar disponível na Política de Privacidade.

A informação sobre atualização constante é importante na medida em que a tecnologia da informação está sempre em modificação, o novo de ontem rapidamente passa a velho hoje, portanto é essencial que os Agentes de Tratamento mantenham a atualização das informações e das Políticas de Privacidade em dia. Alguns documentos previstos na LGPD revelam a necessidade de se estar com a informação atualizada, dentre eles o Relatório de Impacto de Proteção a Dados Pessoais – RIPD ou DPIA, do art. 5º, XVII que pode ser requerido a qualquer momento pela Autoridade brasileira, uma vez que o Regulamento que prevê fiscalização já está vigente desde 28/10/2021, devendo os Controladores preocupar-se em manter suas informações sempre atualizadas, para os casos de fiscalização do art. 15 do regulamento em comento.

Nesse diapasão, informar no *website* quando houve a última atualização da Política de Privacidade é boa prática conforme o art. 50 da LGPD dispõe. A amostra investigada

demonstra boa preocupação em externar aos titulares, que as regras previstas no site são atualizadas a partir de uma data certa, a fim de esclarecer que a Política está atualizada. Nesse panorama, 75% da amostra apresenta no *website* a informação suficiente para que o titular tenha ciência de que as regras as quais está aderindo são atuais, com a data da última atualização. Portanto, o reconhecimento de que essa informação é importante ao titular retrata a maturidade das distribuidoras, nesse ponto do tema, apesar do pouco tempo de vigência da legislação.

5 CONCLUSÃO

O objetivo deste estudo é investigar quanto as boas práticas das Políticas de Privacidade disponibilizadas nos *websites* das distribuidoras de gás natural, o que foi cumprido com as análises que foram feitas na parte 4, em que se verificou a presença de itens essenciais destacados do art. 50 da LGPD nos documentos "Política de Privacidade" publicados pela amostra investigada.

Em especial sobre o investigado, foi possível observar que as distribuidoras de gás natural canalizado estão, na sua maioria, atentas aos critérios de boas práticas na proteção de dados pessoais dos titulares, mas por ser ainda assunto novo há espaço para melhorias. Nesse sentido, destaca-se que na Tabela I a respeito de variáveis sobre dados (define dados coletados e informa finalidade, compartilhamento com terceiros, *cookies*, compartilhamento internacional, e outros) em que pode se observar que 66% da amostra cumpriram com 80% dos requisitos necessários para boas práticas.

Nesse cenário, destaca-se o item consentimento que é considerado positivo quando o titular simplesmente acessa o site do Agente de Tratamento, que neste primeiro momento de vigência da legislação se considera suficiente. Entretanto, deve-se ficar atento a este item, visto que provavelmente pelo exercício da modulação dos dados pessoais pelo titular essa forma de consentimento deverá ser revista exigindo-se condições mais favoráveis com uma convicção de ciência expressa pelo titular mais assertiva, que o simples acesso ao site que última *ratio* é uma adesão aos termos oferecidos pelo Agente de Tratamento de dados.

Destaca-se também, o item que está expresso nas políticas quanto aos dados coletados e a finalidade desta coleta, visto que 75% da amostra cumprem esse requisito demonstrando última análise transparência ao titular, a respeito de como está fazendo o tratamento dos dados pessoais, externando boa prática. Outro item a ser destacado é em relação aos *cookies*, em que metade da amostra 50% confere relevância ao item prestando informações aos titulares, muitas vezes até com detalhamento técnico que não seria necessário, visto que a maioria dos titulares não tem condições de compreensão desta tecnicidade.

Por outro lado, é necessário que as distribuidoras deem maior atenção à forma de indicação de um Encarregado ou DPO que nem sempre se observou na amostra coletada que tenha seguido, conforme previsto em lei. Nesse sentido, a LGPD é clara que o Encarregado deve ser pessoa física ou jurídica, mas certa e individualizada, não devendo se confundir com a simples indicação de endereço de e-mail, grupo ou comitê. Também se observou que de regra há uma confusão na indicação do canal da privacidade com outros canais de informação,

tais como o canal de denúncias ou aquele dedicado ao cumprimento da Lei de Acesso à Informação – LAI. Entende-se que esta prática deve ser evitada buscando deixar claro na Política de Privacidade quanto ao canal individualizado da privacidade, podendo-se incluir um hiperlink levando o titular direto para o ambiente do canal da privacidade. Outra questão que se pontua, é que seria salutar incluir os princípios da lei expressamente na política como forma de manifestação que se está de acordo com novo arcabouço principiológico da lei, unificando o conceito de que a empresa segue a legislação.

O ponto sobre descarte de dados, também é item a ser mais bem trabalhado nas Políticas de Privacidade analisadas. O esclarecimento de forma induvidosa sobre o exercício de descarte de dados como possibilidade existente ao titular é essencial que se faça presente na Política de Privacidade. Nesse sentido, deve estar discriminado o passo a passo, para que o titular tenha condições de realizar o exercício do descarte de dados se assim quiser. Essa situação não ficou evidente na amostra, que muitas das vezes somente deixou expresso na Política de Privacidade que o descarte de dados é um direito do titular, tão somente. É preciso evoluir nesta informação possibilitando reais oportunidades para o exercício deste direito, com a ressalva de uma distribuidora de gás canalizado que conferiu essa possibilidade ao titular.

Destaca-se pela análise realizada, que as distribuidoras de gás canalizado ainda não se utilizam de informações coletadas para oferecer serviços em mercados adjacentes, como o de casas inteligentes, por exemplo. Nesse caso, trata-se de oportunidade no mercado que se bem utilizada poderia trazer benefícios aos consumidores com a promoção de acesso a uma tecnologia integrada com outros serviços e também, oportunizar, o próprio crescimento no setor. Depreende-se tal conclusão, visto que não há qualquer regulamentação dessa possibilidade nas Políticas de Privacidade ou oferta de serviços de mercados adjacentes nos *websites*. Assim, que há espaço para que esse mercado evolua nesse sentido, e, nessa hipótese, tais situações deverão compor posteriormente a regulamentação atual evitando-se eventuais abusos como a predição de comportamentos.

Algumas dificuldades no decorrer do processo desta pesquisa foram vivenciadas. A maior dificuldade que se enfrentou foi a pouca referência de estudos específicos sobre o tema na área abordada de gás natural canalizado, visto que a amostra pesquisada não é beneficiada com estudos científicos a respeito desta temática. Nesse sentido, também limitou a pesquisa a pouca divulgação de situações ocorridas até aqui de incidentes de segurança com dados pessoais relativos a titulares da amostra. Embora a legislação seja recente a tecnologia não é, provavelmente algum fato já tenha ocorrido até aqui, mas não houve a atenção para o registro,

modo a se permitir o estudo das situações específicas ligadas ao mercado. A falta de situações diretamente ligadas à amostra, não permite que se tenha um desdobramento direto, razão pela qual se buscou situações ocorridas em outros mercados, como referência, ao exemplo de casos decididos pelas autoridades na União Europeia, como paradigmas no referencial teórico para o nosso estudo.

Destarte, por ser assunto longo, novo e de complexidade razoável é que o presente estudo não foi exaustivo podendo ser beneficiado com futuras pesquisas, mormente referente a segurança dos dados pessoais. O presente estudo poderia ser favorecido com uma pesquisa complementar posterior analisando itens de segurança da informação deste mercado de gás canalizado aplicado à proteção de dados pessoais tais como: uso de criptografia para proteger a confidencialidade dos dados, utilização de mecanismos de proteção contra perda de dados, registro de dados e geração de evidências, utilização de ferramentas de garantia de que as operações ocorram de forma segura, segurança contra *malware*, *randsomware* e outros. Também, a gestão de eventuais incidentes de segurança da informação quanto aos dados pessoais deveriam ser um desdobramento deste item de segurança da informação, a fim de se verificar o quanto a amostra está preparada para estes eventos, cada vez mais comuns entre as empresas ou órgãos públicos nos dias de hoje. Essa pesquisa futura poderia concluir este ciclo do estudo sobre as boas práticas pelas distribuidoras de gás na área da proteção de dados pessoais.

REFERÊNCIAS

ACQUISTI, A.; TAYLOR, Curtis; WAGMAN, Liad. The economics of privacy. **Journal of Economic Literature**, v. 52, n. 2, 2016. Disponível em: https://ssrn.com/abstract=2580411. Acesso em: 26 set. 2021.

AGÊNCIA ESPAÑOLA DE PROTECCIÓN DE DADOS – AEPD. **Procedimiento Nº: OS/00231/2021**. Resolución de procedimiento sancionador. Madrid, 2021. Disponível em: https://www.aepd.es/es/documento/ps-00231-2021.pdf. Acesso em: 7 nov. 2021.

BAHRI, B.; CARMINATI, B.; FERRARI, E. Decentralized privacy preserving services for online social networks.**Online Social Networks and Media**, Stockholm, Sweden, v. 6, p. 18-25, June 2018. Disponível em: https://reader.elsevier.com/reader/sd/pii/S2468696417301040?token=F5577AE638C6520F2D3B1580238776546A7207277729E7B8D50D028AD0D30D89EB514DB45CDBBF37B2D922B56C675497&originRegion=us-east-1&originCreation=20210828133819. Acesso em: 15 ago. 2021.

BAUMAN, Z.; LYON, D. **Vigilância líquida.** Rio de Janeiro: Zahar, 2014.

BIONI, B. **Proteção de dados pessoais a função e os limites do consentimento.** 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União, Brasília, out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 22 ago. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. **Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019.**Diário Oficial da União, Brasília, ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm.Acesso em: 22 ago. 2021.

CADBURY COMMITTEE. **The report of the committee on financial aspects of corporate governance**. Londres: Cadbury Committee, Dec. 1992.

CALDAS, E. O que aprendemos após as revelações de Snowden?**Revista Galileu**, Cidade, 6 jun. 2014. Disponível em: https://revistagalileu.globo.com/Sociedade/Politica/noticia/2014/06/o-que-aprendemos-um-ano-apos-revelacoes-de-snowden.html. Acesso em 14 nov. 2021.

CENTRO DE ESTUDOS, RESPOSTA E TREINAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT. **Cartilha de vazamento de dados.** maio 2021. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso em: 6 nov. 2021.

CHINA APROVA LEI de proteção de dados pessoais. **Opice Blum,** 29 set. 2021. Disponível em: https://opiceblum.com.br/china-aprova-lei-de-protecao-de-dados-pessoais-semelhante-a-lgpd-e-ao-gdpr/ Acesso em: 10 dez. 2021.

CUNHA, T.;SIMÃO Filho, A. A teoria dos círculos concêntricos e a preservação da

privacidade humana no registro civil das pessoas naturais. 2018. *In:* CONGRESSO BRASILEIRO DE PROCESSO COLETIVO E CIDADANIA. 5., 2018. **Anais ...** [S.l.: s.n.], 2018. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/971. Acesso em: 3 out. 2021.

DATA DILIGENCE. **Guia de boas práticas implementando a LGPD**. Rio de Janeiro: Data Diligence Consultoria e Assessoria Empresarial Ltda., 2020.

DATA PROTECTION COMISSION. Draft decision for the purpose of article 60 GDPR. Dublin, Oct. 6th, 2021. Disponível em: https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf. Acesso em: 10 dez. 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law - EJJL**, [S. l.], v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 28 ago. 2021.

DONEDA, D. **Da privacidade a proteção de dados pessoais:** elementos da formação da lei geral de proteção de dados. 2. ed. São Paulo: Revista dos Tribunais; Thomson Reuters; Brasil Conteúdo e Tecnologia Ltda, 2020.

ENFORCEMENT TRACKER.**GDPR Enforcement Tracker**. 2021. Disponível em: https://www.enforcementtracker.com/. Acesso em: 13 nov. 2021.

EUROPEAN DATA PROTECTION OFFICER - EDPO. **Spanish DPA imposes a 25.000 EUR fine for not appointing a DPO and not notifying the DPA on time**. June, 2020. Disponível em: https://edpo.com/news/spanish-dpa-imposes-a-25-000-eur-fine-for-not-appointing-a-dpo-and-not-notifying-the-dpa-on-time/. Acesso em: 6 dez. 2021.

FORNASIER, M.; BECK, C. Cambridge analítica:escândalo, legado e possíveis futuros para a democracia.**Revista Direito em Debate**, n. 53, p. 182-195, jan./jun. 2020. Disponível em: https://www.academia.edu/53317571/Cambridge_Analytica_Esc%C3%A2ndalo_Legado_e_Poss%C3%ADveis_Futuros_Para_a_Democracia. (14/11/2021)

FURLANETTO, M.; CARMO, J.; SCARMANHÃ, B. Cookies: vulnerabilidade do direito à privacidade nos meios digitais no âmbito da legislação brasileira.**Revista Jurídica Luso - Brasileira - RJLB**, n. 4, p. 1491-1517, 2018. Disponível em: https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1491_1517.pdf. Acesso em: 27 out. 2021.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento correttivo e sanzionatorio nei confronti di Eni Gas e luce S.p.A. Roma, Itállia. 11 Dic. 2019. Disponível em: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9244365. Acesso em: 10 dez. 2021.

GIL, A. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GLOBAL SMART HOMES. **Global smart homes market** - segmented by product type (sistemas de segurança e vigilância, sistemas de iluminação, controles HVAC e R) e regional-growth, tendências e previsões (2018-2023). Dallas: Pesquisa Orbis, 2021.

GOMRLEY, K. **One hundred years of privacy.**University of Winscosin, 1992. Disponível em: https://cyber.harvard.edu/privacy/Gormley--100%20Years%20of%20Privacy.htm.

Acesso em: 28 ago. 2021.

GRUPO BINÁRIO. **Quais são os riscos dos cookies?** 6 jan. 2021. Disponível em: https://www.binarionet.com.br/quais-sao-os-riscos-dos-cookies/ Acesso em: 10 dez. 2021.

HUSSEINI, T. As energy companies race to cash in on data, should we be worried? **Power Technology,** Sept. 23. 2019. Disponível em: https://www.power-technology.com/features/energy-companies-sharing-data/. Acesso em 04/10/2021)

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA – IBGC. **Código das melhores práticas de governança corporativa.** 5. ed. São Paulo: IBGC, 2015. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138. Acesso em: 10 ago. 2021.

ISHITANI, L. **Uma arquitetura para controle de privacidade na web**. 2003. Tese (Doutorado em Ciências da Computação) - Universidade Federal de Minas Gerais – UFMG, Belo Horizonte, 2003. Disponível em: http://hdl.handle.net/1843/SLBS-5WAJQ3. Acesso em: 20 nov. 2021.

LAUBE, K. Entendendo os cookies e sessões. **Klaiuslaube,** abr. 2012. Disponível em: https://klauslaube.com.br/2012/04/05/entendendo-os-cookies-e-sessoes.html Acesso em: 10 dez. 2021.

LEE, A. **What is China's social credit system and why is controversial?** South China Morning Post, Economy, 9 ago. 2020. Disponível em:https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial. Acesso em: 27 set. 2021.

LEGIFRANCE. **Délibération de la formation restreinte n SAN-2020-008 du 18 novembre 2020 concernant la société Carrefour France**. 26 nov. 2020 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756

LIMA, A.; ALVES, D. **Encarregados:** data protection officer. São Paulo: Haikai, 2021.

MACHADO, J. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados.**Revista da AJURIS**, Piauí, v. 41, n. 134, 2014.

MAIA, L. **A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais**. 2011. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf Acesso em: 28 ago. 2021.

MARKETERS MIDIA. **The Global Smart Homes.**Dallas. Feb. 2018. Disponível em: https://marketersmedia.com/global-smart-homes-market-2018-by-evolving-technology-projections-estimations-business-competitors-cost-structure-key-companies-and-forecast-to-2023/302165. Acesso em: 10 dez. 2021.

MENDES, L.;DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor,** Brasília, v. 120, p. 555-587, nov./dez. 2018.

MOORE, S. A proactive approach to privacy and data protection helps organizations increase trust.**Gartner**, Jan. 2020. Disponível em:https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020. Acesso em: 27 out. 2021.

OLIVEIRA, A. B. S. **Métodos da Pesquisa Contábil**. São Paulo: Atlas, 2011.

PINHEIRO, P. **Proteção de dados pessoais:** comentários à Lei nº 13.709/2018.3. ed. São Paulo: Saraiva. 2020.

PUBLYA. O quase fim dos cookies de terceiros e o que se tem até agora. **Publya,** jun. 2021. Disponível em: https://www.publya.com/blog/fim-dos-cookies-de-terceiros Acesso em: 10 dez. 2021.

RAUPP, F.; BEUREN, I. Metodologia da pesquisa aplicável às ciências sociais. *In*: BEUREN, I. (Org.).**Como elaborar trabalhos monográficos em contabilidade**: teoria e prática. 3. ed. São Paulo: Atlas, 2013, p. 76-97.

REDECKER, A. et al. **Proteção de Dados: Temas Controvertidos**. Editora Foco. Indaiatuba. São Paulo, 2021.

REIS, B. A Cultura de *Compliance* em matéria de proteção de dados e sua adoção no âmbito laboral.**Revista de Direito do Trabalho,** São Paulo, v. 214, p. 323-340; nov./dez. 2020.

ROHR, A. Saiba como os cookies ou web beacons rastreiam você. **G1, Segurança Digital,** jan. 2017. https://g1.globo.com/tecnologia/blog/seguranca-digital/post/saiba-como-os-cookies-ou-web-beacons-rastreiam-voce.html. Acesso em: 27 out. 2021.

SESSION OF DAVOS Agenda 2021 online forum. **The Kremlin,** Moscow. Jan. 27, 2021. Disponível em: http://en.kremlin.ru/events/president/news/64938. Acesso em: 27 set. 2021.

SNOWDEN, E. **Who is Edward Snowden?**2013. Disponível em: https://edwardsnowden.com/. Acesso em: 10 nov. 2021.

TALEB, N. **A Lógica do Cisne Negro, o impacto do altamente improvável**. 2. ed. Cidade: Objetiva, 2010.

TEIXEIRA, E. Análise de Dados na Pesquisa Científica: Importância e Desafios em Estudos Organizacionais. **Revista Desenvolvimento em Questão**, Ijuí, v. 1, n. 2, p. 177-201, 2003.

TEMKIN, D. **Charting a course towards a more privacy-first web**. Blog. 3 Mar. 2021. Disponível em: https://blog.google/products/ads-commerce/a-more-privacy-first-web/ Acesso em: 03/11/2021.

THE WHITE HOUSE. **Procurement Information System for Management** – PRISM. Washington DC, 2008. Disponível em: https://georgewbush-whitehouse.archives.gov/oa/functions/prism.html. Acesso em: 10 dez. 2021.

TRANSFERÊNCIA INTERNACIONAL de dados pessoais: o que é e quando está permitida pela LGPD. **Get Privacy,** 2020. Disponível em: https://getprivacy.com.br/transferencia-internacional-de-dados/. Acesso em: 10 dez. 2021.

UNIÃO EUROPEIA - UE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0807. Acesso em: 30 de julho de 2021.

UNIÃO EUROPEIA - UE. **History of General Data Protection Regulation**. Disponível em: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en Acesso em: 02 de agosto de 2021.

UNIÃO EUROPEIA - UE. **The history of the general data protection regulation.**Disponível em: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 30 de julho de 2021.

VIEIRA, V. **Lei Geral de Proteção de Dados:** uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f.Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2019.

WAKKA, F.Facebook é condenado a pagar cinco bilhões de dólares por caso Cambridge Analytica.**Canaltech,** 2019. Disponível em: https://canaltech.com.br/redes-sociais/facebook-e-condenado-a-pagar-us-5-bilhoes-por-caso-cambridge-analytica-144841/ Acesso em: 12 de agosto de 2021.

WEINBERGER, M. Companies stand to make a lot of money selling data from smart devices, says Microsoft. **Business Insider,** Dec. 2015. Disponível em: https://www.businessinsider.in/companies-stand-to-make-a-lot-of-money-selling-data-from-smart-devices-says-microsoft/articleshow/50068955.cms Acesso em: 10 dez, 2021.

Who is Edward Snowden? Disponível em: https://edwardsnowden.com/ Acesso em: 08 de agosto de 2021.

ZENG, J.; DUMMIT, K.; GRAVES, J.; LISKER, P.; SWEENEY, L. Who knows what about me? A survey of behind-the-scenes personal data sharing to third parties by mobile apps.**Techscience,** 2015. Disponível em: https://techscience.org/a/2015103001/. Acesso em: 27 set. 2021.

ZUBOFF, S. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. New York: Public Affairs, 2019.