REDE DE ENSINO DOCTUM – CAMPUS GUARAPARI/ES

ANNELISE NASCIMENTO DA MATA CORREA
DONIZETE DA SILVA RIBEIRO
PAULO CESAR DE OLIVEIRA MEIRELES

COMPLIANCE DIGITAL: A RESPONSABILIDADE DAS EMPRESAS NO VAZAMENTO DE DADOS PESSOAIS DOS CLIENTES SOB A LUZ DA LEI Nº 13.709/2018

GUARAPARI/ES
2024

ANNELISE NASCIMENTO DA MATA CORREA
DONIZETE DA SILVA RIBEIRO
PAULO CESAR DE OLIVEIRA MEIRELES

COMPLIANCE DIGITAL: A RESPONSABILIDADE DAS EMPRESAS NO VAZAMENTO DE DADOS PESSOAIS DOS CLIENTES SOB A LUZ DA LEI Nº 13.709/2018

Trabalho de Conclusão de Curso apresentado à Rede de Ensino Doctum – Campus Guarapari/ES, como requisito parcial para a obtenção do título de bacharel graduado em Direito.

Orientador: Leonardo Fontes

GUARAPARI/ES
2024

ANNELISE NASCIMENTO DA MATA CORREA
DONIZETE DA SILVA RIBEIRO
PAULO CESAR DE OLIVEIRA MEIRELES

COMPLIANCE DIGITAL: A RESPONSABILIDADE DAS EMPRESAS NO VAZAMENTO DE DADOS PESSOAIS DOS CLIENTES SOB A LUZ DA LEI Nº 13.709/2018

Trabalho de Conclusão de Curso apresentado à Rede de Ensino Doctum – Campus Guarapari/ES, como requisito parcial para a obtenção do título de bacharel graduado em Direito.

BANCA EXAMINADORA

_____

Prof(a). Titulação Nome do Professor(a)

_____

Prof(a). Titulação Nome do Professor(a)

_____

Prof(a). Titulação Nome do Professor(a)

Guarapari/ES, 03 de julho de 2024.

RESUMO

É uníssono que práticas de proteção de dados se tornam cada vez mais necessárias conforme a expansão do acesso à internet. Partindo disso origina-se a Lei Geral de Proteção de Dados (LGPD), versando como tais informações devem ser colhidas, tratadas, armazenadas, as responsabilidades por parte daqueles que obtém esses dados pessoais, sensíveis e tão importantes, além das penalizações pelo mau uso destes. Como é de se esperar, nem tudo que é coletado passa pela devida proteção, causando precedentes, onde a Agência Nacional de Proteção de Dados (ANPD) trabalha para mitigar situações danosas aqueles que tem suas informações expostas. Tal autarquia governamental visa fiscalizar e proteger e também fazer valer a norma, restabelecendo o controle e normalidade nas situações de exposição. Por isso, torna-se imprescindível políticas de boas práticas como a aplicação do compliance digital, uma vez que o emprego de tais práticas, o traçado de procedimentos para que a norma seja aplicada em sua totalidade mitigue quaisquer danos advindos dessa exposição de dados ou vazamentos, seja por falha humana ou por falta de aplicação de protocolos de segurança adequados. As empresas são obrigadas a implementar medidas de segurança adequadas para proteger os dados pessoais e notificar imediatamente a ANPD e os titulares dos dados em caso de vazamento que possa comprometer a privacidade ou segurança das informações. Infelizmente no Brasil tais políticas ainda se encontram em estágio inicial de desenvolvimento e acaba encontrando como fator dificultador a imperícia das empresas em políticas de compliance, tornando difícil a tarefa, porém atualmente mais fácil, considerando as diretrizes e atualizações trazidas pela LGPD ao ordenamento jurídico brasileiro. A pesquisa é encarada com o propósito de aproximar o leitor do tema, explorando as nuances positivas e negativas, que foram refletidas nas hipóteses já descritas. A concretização da pesquisa bibliográfica não é rígida, pelo contrário será flexível, o que trará liberdade para o teste das hipóteses. Na perseguição do objetivo geral, esta possibilidade menos engessada, permitirá que as etapas possam se ajustar ao aprofundar das descobertas. Para desenvolvimento desta pesquisa empírica, o procedimento adotado é o da Pesquisa Bibliográfica, haja vista que as fontes secundárias abundantes no ordenamento jurídico, por se manifestarem por meio de livros, artigos científicos, dicionários, legislação e periódicos, permitem ao pesquisador ampla visão técnica. Para o ramo do direito, não há procedimento de pesquisa melhor adequado. Tem-se a escolha do procedimento, como o mais adequado, verificável é testável para o tema. No primeiro momento, o levantamento das fontes bibliográficas norteará esta fase, permitindo proximidade ao tema. Posteriormente, as fontes serão classificadas, buscando-se a compreensão das posições convergentes e divergentes. Neste momento, começarão os testes das hipóteses. E por fim, concretizando o tratamento das fontes, visando aproximar o pesquisador da clareza e precisão.

Palavras-chave: Compliance Digital; LGPD; Responsabilidade Empresarial; ANPD; Abordagens Práticas.

ABSTRACT

It is unanimous that data protection practices become increasingly necessary as internet access expands. From this, the General Data Protection Law (LGPD) originates, dealing with how such information should be collected, treated, stored, the responsibilities of those who obtain this personal, sensitive and important data, in addition to the penalties for its misuse. As is to be expected, not everything that is collected is properly protected, causing precedents, where the National Data Protection Authority (ANPD) works to mitigate harmful situations for those who have their information exposed. Such governmental autarchy aims to supervise and protect and also enforce the norm, reestablishing control and normality in exposure situations. Therefore, it is essential to have good practice policies such as the application of digital compliance, since the use of such practices, the design of procedures for the standard to be applied in its entirety mitigate any damage arising from this data exposure or leaks, either due to human error or lack of application of appropriate security protocols. Companies are required to implement appropriate security measures to protect personal data and immediately notify the ANPD and data subjects in the event of a leak that could compromise the privacy or security of information. Unfortunately in Brazil, such policies are still in the early stages of development and end up finding as a complicating factor the incompetence of companies in compliance policies, making the task difficult, but currently easier, considering the guidelines and updates brought by the LGPD to the Brazilian legal system. The research is undertaken with the purpose of familiarizing the reader with the topic, exploring the positive and negative nuances that were reflected in the hypotheses already described. The implementation of the bibliographic research is not rigid; on the contrary, it will be flexible, which will provide freedom to test the hypotheses. In pursuit of the general objective, this less rigid possibility will allow the stages to adjust as discoveries deepen. For the development of this empirical research, the adopted procedure is Bibliographic Research, considering that the abundant secondary sources in the legal system, manifested through books, scientific articles, dictionaries, legislation, and periodicals, provide the researcher with a broad technical view. For the field of law, there is no better-suited research procedure. The choice of procedure is considered the most appropriate, verifiable, and testable for the topic. Initially, the collection of bibliographic sources will guide this phase, allowing proximity to the topic. Subsequently, the sources will be categorized, aiming to understand convergent and divergent positions. At this point, hypotheses testing will commence. Finally, through the treatment of sources, efforts will be made to bring the researcher closer to clarity and precision.

***Key-words*:** Digital Compliance; General Data Protection Law; Corporate Responsibility; National Data Protection Authority; Practical Approaches

SUMÁRIO

1. INTRODUÇÃO 7
2. MARCO TEÓRICO 9
2.1 CONCEITO **9**
2.2 EVOLUÇÃO HISTÓRICO **11**
2.3 DISCUSSÃO DOUTRINÁRIA **13**
3. O COMPLIANCE DIGITAL COMO FERRAMENTA PARA MITIGAÇÃO DE INCIDENTES DE VAZAMENTOS DE DADOS 16
4. O ENTENDIMENTO JURISPRUDENCIAL ACERCA DA RESPONSABILIZAÇÃO DAS EMPRESAS NOS VAZAMENTOS DE DADOS 19
5. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO ÓRGÃO REGULADOR E FISCALIZADOR DA LGPD..... 21
6. ABORDAGENS PRÁTICAS PARA GARANTIR UMA APLICAÇÃO ACERTADA À LUZ DA LGPD..... 24
7. CONSIDERAÇÕES FINAIS 26
REFERÊNCIAS 28

1. INTRODUÇÃO

Considerando os avanços da internet no cotidiano mundial, por vezes, indagamos sobre suas extensões e limitações e sobre o que acontece neste amplo campo que possa interferir em nossa vivência. Visando criar parâmetros e diretrizes para proteger os dados pessoais daqueles que a utilizam diariamente para executar diversas transações, seja no campo pessoal quanto no campo profissional, o compliance digital buscar dar respaldo e segurança aos usuários.

O compliance digital surge a partir de diversas doutrinas que vão desde organizar essa coleta de dados até instaurar sanções aqueles que fazem o tratamento de tais dados sensíveis, corrigindo possíveis danos causados. Após anos de discussões e evolução da doutrina jurídica brasileira, temos a criação da Lei Geral de Proteção de Dados (LGPD), norma que visa gerir assuntos relacionado a segurança de dados na rede, normatizando o que pode ser coletado, de qual forma e suas tratativas após este deixarem de ser interessantes para a finalidade a qual foram empregados, e também como as empresas coletoras devem armazená-los.

Pouco é sabido, mas o governo federal possui uma autarquia destinada a essa fiscalização, denominada de Autarquia Nacional de Proteção de Dados, atualmente sob a jurisdição do Ministério da Justiça. A principal discussão a respeito do tema Compliance Digital sempre fora de encontrar um “norte” ao qual se basear para iniciar as tratativas, atualmente indicado de forma unânime, como proteção de dados para a partir disso reduzir de forma drástica, ou até mitigar, as chances de vazamentos, como por exemplo o ocorrido nos Estados Unidos, por intermédio de Edward Snowden, que divulgara à época que a CIA exercia vigilância dentro e fora de sua jurisdição, criando atrito em escala global e levantando suspeitas graves sobre o serviço secreto americano e seu governo.

Conforme fala Snowden “Quando todos nos unirmos contra as injustiças e em defesa da privacidade e dos direitos humanos básicos, poderemos nos defender até dos mais poderosos dos sistemas” (Snowden, *online*) ou ainda, em declaração dada na Web Summit, considerado um dos maiores eventos de tecnologia mundial quando bradou “Dados não são inofensivos ou abstratos quando se trata do ser humano. Não são dados que estão sendo explorados. São pessoas que estão sendo exploradas”. (Snowden, 2019, *online*). Assim, contando com caminhos determinados, a abordagem prática torna-se mais facilitada e assertiva, contribuindo para que demandas baseadas

em vazamento de informações sejam tratadas diretamente na sangria, evitando exposição desnecessárias e ações judiciais demasiadas, colaborando não só para uma solução mais célere como um desafogo no sistema judiciário brasileiro.

2. MARCO TEÓRICO

2.1 CONCEITO

Partindo do princípio de que o Compliance vem do termo em inglês "*to comply*" que, em sua essência, quer dizer conformidade, é possível afirmar que esse é aplicado ao ambiente organizacional através de normas e diretrizes adotadas para agir de acordo com a legislação vigente que rege o seu funcionamento.

Nesse mesmo sentido, encontra-se o Compliance digital, esse que consiste em um mecanismo utilizado para garantir a regulação dos processos e, assim, atender as normas e leis que incidem sobre o meio digital buscando, dessa forma, mitigar riscos, com o foco no âmbito da cibersegurança, haja vista as armadilhas virtuais que crescem vertiginosamente.

Assim assevera Bielgelman (2008, p.107):

> "Muitas empresas não tinham freios efetivos e contrapesos para regular seu comportamento e os consultores jurídicos internos eram incapazes ou não queriam dar conselhos legais claros e pertinentes. A gestão agiu com superproteção e assumiu grandes riscos, assim como preocupações de curto prazo dominaram as tomadas de decisões corporativas. Isso coincidiu com uma maior atenção do público acadêmico sobre atos ilegais e lesivos das corporações, que levaram à regulamentação posterior. "

Nesta esteira, levando em consideração que o Compliance digital diz respeito ao conjunto de medidas que determinada empresa precisa adotar e seguir para que assim assegure a proteção de dados particulares, bem como informações pessoais dos seus clientes, e, isso através da implementação de protocolos de segurança e cumprimento de leis, normas e regras, abarcados, em sua maioria, pela Lei Geral de Proteção de Dados (LGPD), essa que trata acerca da segurança da informação nas redes. Seguindo, dessa forma, uma linha legislativa que preza pela proteção da propriedade virtual.

De acordo com a interpretação de (COLARES, 2014, p.64):

> "Garantir a aderência e cumprimento de leis; desenvolver e fomentar princípios éticos e normas de conduta; implementar normas e regulamentos

> de conduta; criar sistemas de informação; desenvolver planos de contingência; monitorar e eliminar conflitos de interesses; realizar avaliações de risco periódicas; desenvolver treinamentos constantes e estabelecer relacionamento com os órgãos fiscalizadores, auditores internos e externos e associações relacionadas ao setor da companhia."

Sendo assim, vale ressaltar que, tal texto legislativo visa proibir a utilização de informações que, de forma isolada ou em conjunto, possam, de alguma forma, revelar a identidade de clientes por partes de organizações.

Dessa forma, é correto afirmar que a relação entre a Lei Geral de Proteção de Dados (LGPD) e o Compliance digital é direta, haja vista que tal texto legislativo é utilizado pelas empresas para criar seus programas de conformidade, códigos de conduta e normas corporativas, sendo estes essenciais à garantia da construção de um ambiente seguro.

Segundo os autores Sarlet, Marinoni e Mitidiero (2018, p.49):

> "Embora não se trate de direito absoluto, o direito à proteção dos dados, especialmente na medida de sua conexão com a dignidade humana, revela-se como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a intimidade e pode implicar violação da dignidade da pessoa humana."

Por todo o exposto fica claro que a observância da Lei Geral de Proteção de Dados (LGPD) é de suma importância, pois, a aplicação dessa somado ao Compliance Digital faz-se obrigatória para prevenção de riscos, e o seu conhecimento é primordial para a harmonia das relações corporativas.

Importante ressaltar que, como visto anteriormente, a LGPD (Lei Geral de Proteção de Dados Pessoais) dispõe que as empresas têm o dever de garantir a proteção dos dados pessoais de seus clientes e usuários, e, no caso de violação à legislação de proteção de dados pessoais, a Lei n. º 13.709/2018, em seu artigo 42 assevera:

> "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. "

Sendo assim, segundo o artigo supramencionado, fica sob responsabilidade da empresa, a obrigação de reparar os danos, seja ele patrimonial, moral, individual ou coletivo.

2.2 EVOLUÇÃO HISTÓRICA

A Lei Geral da Proteção de Dados (LGPD) se moldou na base da *General Data Protection Regulation* (GDPR), criada pela União Europeia com o Regulamento (UE) 2016/679 sobre o tratamento e a livre circulação dos dados pessoais (COMISSÃO EUROPEIA, 2016, s.p.). Esse modelo foi estruturado em torno de uma Diretiva 95/46/CE conforme aponta Doneda como “uma disciplina ampla e detalhada que é transposta para a legislação interna de cada estado-membro” (DONEDA, 2006, p. 222).

Essa Diretiva foi revogada, mas manteve seus princípios na GDPR de acordo com os princípios do tópico 2 do referido regulamento: (2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares (REGULAMENTO UE, 2016, s.p.).

Uma vez formatado tal modelo serve como base para cada país tomá-lo como inspiração e consequentemente uniformizar sua legislação para que haja harmonização do entendimento quando o assunto for proteção de dados pessoais.

Com a inovação tecnológica houve uma expansão em diversos ramos da sociedade, inclusive do mundo dos negócios, nesse passo é certo que a empresa que pretende integrar a tal transformação precisa se adequar para estimular a tomada de risco, incentivar a inovação e desenvolver um ambiente de trabalho corporativo. Nesse passo, conforme Jimene (2019, p. 47 apud Cavalari, 2020) destaca:

> [...] atualmente os dados corporativos das organizações encontram-se armazenados em diferentes ambientes: servidores da empresa ou em nuvem,

> notebooks, celulares,*tablets*, *smartwatches*, *pendrives* e aplicações de Internet, corporativas ou muitas vezes particulares, de modo que, nos dias atuais, *WhatsApp*, *Facebook* e *LinkedIn,* por exemplo, são ferramentas utilizadas, ao mesmo tempo, para marcar o jantar com a família e fechar grandes negócios.

Assim, diante dos apontamentos acima verifica-se a relevante importância da proteção dos dados no mundo, de modo que é indispensável o desenvolvimento de garantias legais para a proteção da privacidade decorrente da colheita de informações dos administrados.

Considerando a importância da aplicação destes princípios que visam mitigar, entre outros malefícios, os vazamentos de dados pessoais em rede aberta, torna-se cada vez mais necessário a busca por parâmetros e condutas que venham a padronizar os comportamentos das empresas. Conforme expande-se a aplicação da internet nos demais ramos da vida cotidiana, passa-se a considerar o qual protegido/desprotegido o indivíduo se encontra, o que traz, por consequência a preocupação com seus dados e comportamentos perpetrados na rede. A partir disso, Lins (2013, p.21) discorre:

> “Infelizmente, a precaução de respeitar essas regras básicas ficou perdida após o advento da Internet comercial. E estende-se ao uso do smartphone nos dias de hoje. É comum ver pessoas teclando, tirando selfies ou falando ao telefone em público, sem qualquer cuidado com a privacidade. Abrigam-se em uma suposta redoma de cristal vinda do telefone, que as protegeria de qualquer indiscrição. Pura ilusão.”

Neste momento vem à luz a Lei Geral de Proteção de Dados (LGPD) como forma de prevenção, embora desconhecida por grande parte da massa, sem considerarmos que anterior a esta, conforme Pinheiro (2021) cita em sua obra, fora disponibilizada a pelo Ministério da Justiça um anteprojeto de Leis de Proteção de Dados, por volta de 2010, que viria a ser o germinar da LGPD atualmente estabelecida.

Ainda conforme traz a autora, “em 2012, com clara inspiração na consulta pública, foi protocolado o PL nº 4.060 que dispunha sobre o tratamento de dados pessoais e dava outras providências”. Em contrapartida, considerando o contexto histórico em simultâneo, estourava nos EUA, por meio da figura de Edward Snowden,

um escândalo acerca do tratamento de informações e espionagem corporativa em nível mundial, relacionado a Agência Nacional de Segurança daquele país. Conforme traz em sua obra Marcarcini (2016, p.22)

> "Tal fato acelerou o trâmite do projeto de lei, enquanto este ainda se encontrava na Câmara dos Deputados. A Presidência da República solicitou a aplicação de regime de urgência constitucional para apreciação do projeto, motivada pelas revelações trazidas à luz por Edward Snowden. Divulgou-se que a própria Presidência da República de nosso país teria sido foco de espionagens mediante interceptação de suas comunicações telefônicas e eletrônicas, e a indignação que isso causou em nossa então governante resultou na aplicação do regime de urgência ao projeto de lei sobre o Marco Civil."

Assim, após discussões, a aprovação deu-se em agosto de 2018, quando passou pela sanção presidencial, além de breves alterações trazidas pela lei 13.853/19. Enfim, nasceu legislação aplicável à proteção de dados e respaldo jurídico na tratativa destes, onde antes pouco se deliberou.

Isto posto, nota-se que o histórico do Compliance Digital é recente, tendo em vista o pouco tempo da implementação de uma lei específica regendo o tema, como também, por ser uma matéria recente dentro do nosso ordenamento jurídico.

2.3 DISCUSSÃO DOUTRINÁRIA

É uníssona a necessidade de parâmetros e normas éticas que visem regular e eliminar condutas negativas quando consideramos as evoluções tecnológicas e expansão do acesso à internet, principalmente nas últimas décadas, se analisarmos que desde a menor operação financeira até a novidade do metaverso está inserida neste avanço e também suscetível a erros. Partindo disso, Carvalho (2021, p.502) denota que um norte deve ser eleito como alicerce desta nova etapa, discorrendo no seguinte:

> "Poderíamos ter escolhido abordar cada um dos setores do compliance digital (e.g. segurança da informação, teletrabalho, investigações internas e provas eletrônicas, leis específicas a exemplo do Marco Civil da Internet, entre tantos outros). Preferimos, no entanto, dar prioridade àquele que desponta como o mais relevante, e sobre o qual a discussão acerca do papel de programas de

> compliance é, certamente, a mais rica: a privacidade e proteção de dados pessoais. ”

Assim, no ramo empresarial temos a crescente disseminação da compliance, ainda que grande parte das organizações empresarial não possui capacidade, disponibilidade ou diretrizes que sejam facilitadores para aplicação de normas como define o compliance, considerando a penúltima pesquisa realizada pela KPMG (2019, p.05), avaliada com nota 2,82, o que significa nível fraco de maturidade; situação ainda mais precária quando observamos o meio digital, avaliado com média de 2,55, deixando grande margem de evolução. Na pesquisa mais recente, realizada em 2021, essa média continua baixíssima, porém observa-se que a preocupação com tais demandas se torna mais evidenciada com a maior conectividade gerada pela expansão do trabalho *home office* e pela própria pandemia de COVID-19.

Levando em conta o meio social brasileiro, o compliance passa a ter grande visibilidade a partir da Operação Lava Jato, que culminou não só na devolução de exorbitantes valores aos cofres públicos, mas exposição de figuras públicas envolvidas em diversos esquemas de corrupção, sendo considerado o maior na história deste país. Desde então, é notória a necessidade de gerenciar mecanismos que visem combater tanto corrupção e perpetração de atos ilícitos nos diversos setores públicos. Logo, vem à tela a Lei Geral de Proteção de dados (LGPD), onde a adequação a seus parâmetros pelas organizações tornou-se meta a ser batida, surgindo uma nova leva de profissionais, buscando capacitação para atuação na área de proteção de dados, bem como de compliance e divisão dedicada dentro das empresas, por exemplo.

Desde 2019, existe uma autarquia nacional, denominada de Autoridade Nacional de Proteção de Dados (ANPD), vinculada ao Ministério da Justiça e Segurança Pública, responsável pela regulamentação, implantação e fiscalização do cumprimento da LGPD no país. É a esta autarquia que os vazamentos de dados pessoais devem ser comunicados e esta determina quais situações devem ser disponibilizadas ao público bem como informar medidas que visem reverter ou findar os efeitos deste vazamento, quando possível for seu tratamento.

Assim como dispõe Castro (2020, p.72) algumas medidas devem ser consideradas por aquelas organizações, tanto públicas como privadas, que buscam

implantar o compliance de forma a garantir a integridade destes órgãos, tais como padrões de ética e conduta a serem disseminadas na organização; treinamento buscando promover maior informação e conhecimento em todos os setores; a criação e manutenção de canais de denúncias, visando coibir vazamento de dados pessoais por parte de colaboradores e/ou empresas; medidas disciplinares e de controle como dispostas nas legislações citadas anteriormente, assim como sua eficácia no caso concreto e, por fim, tratativas que visem mitigar ou remediar vazamentos e seus desdobramentos, conforme a legislação dispõe.

3. O COMPLIANCE DIGITAL COMO FERRAMENTA PARA MITIGAÇÃO DE INCIDENTES DE VAZAMENTOS DE DADOS

Como o próprio nome aduz, Compliance Digital busca aplicar regras e normas de governança ao meio digital, conforme o tema em tela, visando resguardar dados coletados por empresas, viabilizando seu tratamento e minimizando falhas de segurança que possam permitir que estes sejam direcionados a outras finalidades diversa daquela para qual fora adquirida. Assim como traz a Lei do Marco Civil da Internet, constante em seu artigo 3°, como segue:

> "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; (...)" (Brasil, 2014, *online*).

Visando essa proteção e como estabelecer qual meta a ser trabalhada, Carvalho *et al*. (p.503) discorre:

> "Não seria nenhum exagero afirmar que, se por falta de recursos, houvesse a necessidade da escolha de conformidade, por uma organização, em apenas um tema associado a leis de "fundo digital", o Compliance em proteção de dados pessoais e privacidade seria a escolha a ser feita."

Assim, partindo do princípio exposto anteriormente, o rumo a ser tomado fora eleito, bastando ao ente privado verificar em suas políticas de proteção os gargalos onde possa haver insegurança de dados e trabalhar nestes, tratando aqueles possíveis e substituindo condutas automáticas ou manuais defasadas, criando protocolos a serem seguidos pelos colaboradores responsáveis no trato de tais informações desde sua coleta.

Ademais, é a base do artigo 2º da Lei Geral de Proteção de Dados:

> "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a

> inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.” (Brasil, 2018, *online*)

Com isso, nota-se que o artigo segundo da lei 13.709 (LGPD) trouxe princípios fundamentais para a proteção dos dados, tanto de forma remota quanto de forma digital e on-line. Ocorre que para preservar e aplicar tais normativas são necessárias políticas rígidas e plausíveis, a fim que possam ser aplicadas por grandes empresas, bem como, empresas de médio porte.

Vale ressaltar que o atual contexto de crescimento da digitalização nas empresas deve ser levado em consideração durante essa análise, haja vista que as estratégias que foram criadas para garantir a eficiência dos controles internos das empresas, visando assim, a mitigação de riscos derivados dos ambientes virtuais, são alicerçados por esse momento atual, qual seja, o crescimento vertiginoso da digitalização nos ambientes corporativos.

Posto dessa forma, é de suma importância agir de acordo com as regras aplicáveis ao ambiente digital, adotando procedimentos e técnicas de segurança digital que evitem a exposição a fraudes, vazamentos de dados e outras situações de risco. E, sobre esse assunto o artigo 11, alínea g, da Lei Geral de Proteção de dados, preconiza:

> “Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) 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.” (Brasil, 2018, *online*)

Desta feita, a lei permite em casos específicos, tratamentos dos dados pessoais, evitando assim, possíveis fraudes, bem como, mantém a segurança dos titulares dos respectivos dados. Ocorre que no dia a dia, o usuário permite e fornece os dados para inúmeras empresas na Internet, não tomando as devidas cautelas no

fornecimento dos mesmos, podendo muitas das vezes, fornecer dados para possíveis fraudadores.

Com a aplicação do Compliance Digital, tendo como base a mitigação de vazamentos de informações e com o objetivo geral de mitigar possíveis ações judiciais, alicerçadas no fornecimento ilegal de dados pessoais coletados na rede de internet, o Compliance e as políticas de dados se mostra como a única alternativa viável para uma aplicação harmônica das mais recentes legislações acerca do tema.

4. O ENTENDIMENTO JURISPRUDENCIAL ACERCA DA RESPONSABILIZAÇÃO DAS EMPRESAS NOS VAZAMENTOS DE DADOS

Apesar da Lei Geral de Proteção de Dados ser relativamente nova, o tema de vazamentos de dados já fora apreciado em diversos casos anterior à lei, e por isso, com advento da lei especial, o Superior Tribunal de Justiça já está consolidando a jurisprudência acerca dos vazamentos de dados pelas empresas no ambiente virtual, bem como, no ambiente físico.

No Agravo em Recurso Especial nº 21306.19, os ministros firmaram o seguinte entendimento:

> "(...) I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. **Os dados de natureza comum, pessoais, mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.** (...) **Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.**" (Brasil, 2019, *online*)

Isto posto, percebe-se que nem todo vazamento de dados é passível de indenização, devendo ser provado em juízo o efetivo dano sofrido pelo vazamento. Ademais, a decisão observa que somente dados íntimos e sensíveis ensejam o dever

de indenizar. Vale ressaltar, que a própria Lei Geral de Proteção de Dados dita o que seria dados sensíveis, *in verbis*:

> “Art. 5º Para os fins desta Lei, considera-se: [...] 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.” (Brasil, 2018, *online*)

Portanto, em seu voto, o Ministro Francisco Falcão também afirmou que, no caso dos autos, o dano moral não é presumido, sendo necessário que o titular dos dados demonstre ter havido efetivo dano com o vazamento e o acesso de terceiros.

> "Diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural. No presente caso, trata-se de inconveniente exposição de dados pessoais comuns, desacompanhados de comprovação do dano", concluiu o ministro ao acolher o recurso da Eletropaulo e restabelecer a sentença.”

Tal afirmativa, não poderia estar mais correta, levando em consideração a legislação especial, tendo em vista que o próprio artigo 42 da Lei Geral de Proteção de Dados (BRASIL, 2018, *online*) que preconiza que “*o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo*”.

Dessa forma, o legislador permitiu a indenização ao cliente somente quando o controlador ou o operador, tais como as empresas que recebem os dados pessoais e sensíveis, tão somente quando provado que os dados vazados eram de caráter pessoal, capaz de causar danos a outrem.

5. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO ÓRGÃO REGULADOR E FISCALIZADOR DA LGPD

Criada através da promulgação da Lei Geral de Proteção de Dados (LGPD), Lei Nº 13.709, de 14 de Agosto de 2018, a Autoridade Nacional de Proteção de Dados (ANPD), atua como autoridade reguladora e fiscalizadora, tendo como objetivo principal, tutelar e zelar pela proteção dos dados pessoais, bem como supervisionar o tratamento de tais informações, garantindo, dessa forma, que empresas, órgãos públicos e as demais entidades, tratem os dados pessoais dos titulares de forma adequada, considerando os princípios da LGPD, quais sejam, finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilidade e prestação de contas. (PINHEIROS, 2020).

E, para tanto, tal órgão fiscalizador atua na orientação preventiva, bem como aplicação de penalidades nos casos de descumprimentos. Imperioso destacar que, antes da aplicação de qualquer sanção, haverá a comunicação aos agentes de tratamento, bem como a possibilidade de ampla defesa e apresentação de razões que visem justificar ou mesmo minimizar os eventuais dados causados. Levando em consideração o rápido avanço tecnológico bem como as bruscas mudanças nas formas de coleta e uso de dados, a implementação da LGPD é um desafio contínuo. Por isso, a ANPD está constantemente adaptando suas estratégias para proteger a privacidade dos dados pessoais dos cidadãos.

Conforme mencionado, a ANPD, possui papel fundamental no que tange a supervisão e tratamento dos dados pessoais, e, para o desenvolvimento e garantia dessa tutela, essa autoridade verifica se as organizações estão coletando, armazenando e processando as informações, que são categorizadas como dados pessoais, de acordo com os fundamentos da Lei Geral de Proteção de Dados (LGPD), que em seu artigo 2º preceitua que:

> “Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;

> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.”

Ademais, a ANPD oferece, de igual forma, orientações preventivas, com o objetivo de auxiliar empresas, bem como os clientes na qualidade de cidadãos, a compreenderem seus direitos e deveres no tocante à privacidade.

Na ocorrência de infrações à LGPD, a ANPD atua na aplicação de sanções administrativas, sendo que tais penalidades podem variar entre advertências e multas, de acordo com a gravidade da violação. Importante ressaltar que, tal fiscalização é realizada através de investigações, denúncias e auditorias. Dessa forma, segundo o §1º, do art. 52, da Lei nº 13.709/2018: *“As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto”*

Os critérios utilizados durante a análise, estão pautados na gravidade das infrações e dos direitos pessoais feridos, a boa-fé do infrator e sua cooperação, o objetivo ou vantagem pretendido pelo infrator, as condições econômicas, a reincidência, a extensão do dano ocasionado, a adoção de mecanismos, bem como procedimentos internos que visem proteger os dados coletados, adoção de políticas de boas práticas e governança voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 da Lei supracitada, e, por fim, a adoção de medidas corretivas eficazes e a proporção entre a gravidade da infração e a penalidade a ser imposta.

Por todo o exposto, destaca-se que, a ANPD exerce papel fundamental na fiscalização do cumprimento da LGPD, garantindo, dessa forma, a proteção dos direitos fundamentais da liberdade e privacidade, direitos esses que estão expostos na nossa estimada Constituição Federal, essa que rege nossa República. Por isso, a sua devida observância pelas empresas é de suma importância, pois, aplicando devidamente as medidas de mitigação de riscos no vazamento de dados pessoais, fomenta-se a construção de um ambiente seguro.

Em suma, é possível afirmar que, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel vital no contexto da proteção de dados pessoais no Brasil, pois, enquanto órgão regulador, não garante apenas que as organizações observem e cumpram devidamente o que está expresso na Lei Geral de Proteção de dados

(LGPD), mas atua também como uma ponte essencial entre os cidadãos e as entidades. Tendo em vista que, através de suas diretrizes, atua promovendo uma cultura de transparência e responsabilidade, fundamentos esses que são essenciais para a manutenção da confiança digital e desenvolvimento econômico sustentável.

Por conseguinte, a ANPD transcende a mera conformidade legal, ela é uma guardiã dos direitos digitais dos cidadãos e um pilar essencial para a construção da inovação no cenário global.

6. ABORDAGENS PRÁTICAS PARA GARANTIR UMA APLICAÇÃO ACERTADA À LUZ DA LGPD

Atualmente, a Lei Geral de Proteção de Dados (LGPD) do Brasil está moldando significativamente a forma como as organizações lidam com informações pessoais. Suas principais abordagens práticas visam garantir a proteção dos dados dos cidadãos e promover uma cultura de responsabilidade e transparência nas operações de tratamento de dados. Pode-se considerar abordagens práticas da LGPD como o consentimento onde o titular dos dados deve autorizar a coleta dos dados. As organizações devem obter consentimento explícito e informado dos indivíduos para o uso de seus dados, esclarecendo finalidades específicas e direitos do titular.

Outra forma de guarda são os Princípios de Proteção de Dados, baseados na LGPD, destacando princípios fundamentais que as organizações devem seguir no tratamento de dados pessoais, como finalidade e transparência, adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização e aplicação da norma. Tais condutas visam afunilar e por conclusão, mitigar válvulas de escape por onde esses dados sensíveis ficariam “desprotegidos”.

Como trazido anteriormente, para coleta necessita de consentimento do possuidor desses dados. Assim, os titulares dos dados têm diversos direitos garantidos pela LGPD, incluindo o direito de acessar seus dados pessoais, corrigi-los, eliminar dados desnecessários ou excessivos, portar seus dados para outro fornecedor de serviço, obter informações sobre o compartilhamento de seus dados, etc.

Partindo disso, surge a necessidade de um profissional capacitado para operar tais ferramentas e verificar se a norma tem aplicação. Ademais, a LGPD requer que empresas designem um DPO (Data Protection Officer), responsável por monitorar a conformidade com a lei, servir como ponto de contato para os titulares dos dados e cooperar com a autoridade de proteção de dados. Tal função é designada pela LGPD como Encarregado de Proteção de Dados. Esta é uma posição chave dentro das organizações que lidam com dados pessoais., sendo este responsável pelo monitoramento de conformidade, funcionando como o ponto de contato entre a empresa, os titulares dos dados e a ANPD e ainda esclarecer dúvidas sobre como os

dados estão sendo tratados. Outra função do DPO é conscientizar e promover treinamento dos funcionários a respeito das práticas de proteção de dados conforme exige a LGPD. Essa nomeação de um DPO não é obrigatória para todas as organizações, mas é de grande valia, principalmente nas empresas que tratam dados em larga escala ou aqueles dados sensíveis. O que é obrigatório é a notificação de qualquer incidente relacionado a disponibilização de dados não autorizada ou falha de segurança no tratamento destes, devendo ser reportado a ANPD e aos titulares e discriminar as tratativas empregadas para correção de tal desvio.

Outra preocupação é quanto a Transferência Internacional de Dados. A LGPD estabelece requisitos específicos para a transferência internacional de dados pessoais, garantindo que dados enviados para fora do Brasil sejam protegidos de acordo com os padrões exigidos pela lei. Essa transferência é um aspecto crítico abordado pela LGPD, principalmente por causa das crescentes interações globais entre empresas e indivíduos. A lei estabelece requisitos específicos para garantir que dados pessoais enviados para fora do Brasil recebam proteção adequada, alinhada aos padrões de segurança exigidos pela LGPD, onde a proteção na transferência deve possuir nível de segurança equiparado ao que dispõe a LGPD, utilizando de cláusulas contratuais que, por padrão, possam assegurar a proteção dos dados durante a transferência. Caso necessário, buscando a obtenção de consentimento específico e informado dos titulares dos dados para a transferência internacional, informando sobre os riscos envolvidos, notificando a ANPD quando a legislação estrangeira não suprir os requisitos da normal brasileira para proteção de dados.

Essas abordagens práticas refletem o compromisso da LGPD em proteger a privacidade dos indivíduos, promover a segurança dos dados e estabelecer um ambiente de confiança nas relações comerciais e institucionais que envolvem o tratamento de informações pessoais. A implementação efetiva dessas medidas não apenas ajuda as organizações a cumprir com a legislação como orientam o fazer e coordenam correções, mas também fortalece a proteção dos direitos fundamentais dos cidadãos em um mundo digital cada vez mais complexo.

7. CONSIDERAÇÕES FINAIS

Como advém da atual composição, considerando também o cenário atual da circulação de dados, faz-se cada vez mais necessária a implementação de políticas de proteção. Com o intuito de facilitar a compreensão do tema, a pauta abortada englobou desde o surgimento das primeiras leis até a atual organização de compliance, dando forma ao que hoje é a LGPD, trazendo um rumo a ser tomado, visando mitigar quaisquer hipóteses de vazamento, exposição de dados pessoais ou danos a terceiros.

Por se tratar de um tema relativamente novo, é notório salientar a importância da organização de mais estudos a respeito, buscando sempre complementar e aprimorar legislações atuais, impedindo que possíveis brechas apareçam e possam ser exploradas por criminosos digitais. Boa parte das empresas brasileiras não possuíam condições favoráveis para implementação do compliance digital, seja por dificuldade de capacitação, por impossibilidade de adição do setor dentro de suas operações ou até por conta de legislação especial. Porém, esse cenário outrora caótico, vem melhorando.

Conforme estudos apresentados no decorrer do trabalho, as empresas buscam qualificar-se para que a segurança desses dados seja aplicada de forma eficaz, auxiliadas pela LGPD e fiscalizadas pela Autoridade Nacional de Proteção de Dados (ANPD), funcionando de forma atuante, possuindo até sanções já impostas a transgressores da norma já transitada em julgado. Evidente que com a atuação deste órgão, tornam-se mais assertivas as condutas adotadas, principalmente no que diz respeito as empresas, outrora no escuro, encontrando luz para avançar rumo a um ambiente seguro, físico e virtualmente falando, e quando não o for possível, aplicando correções necessárias e prestando informações e suporte aos que tiverem seus dados expostos, o que transforma a ANPD em guardiã dos direitos dos cidadãos em âmbito digital e imprescindível atuação como intermediárias entre estes e as organização.

Nossa pesquisa apontou que as empresas vêm se adequando quanto o que rege a norma, por mais complicada que pareça, a implementação do DPO surge como grande ferramenta para capacitação e treinamento dos colaborados responsáveis pelo trata dos dados pessoais sensíveis, contribuindo assim para que o erro humano não venha a prejudicar terceiros. Portanto, quando as organizações se encontram

munidas de informação e qualificação, alinhadas com boas práticas estimuladas pela legislação atuante, torna-se menos dificultoso que as políticas de compliance digital sejam aplicadas de forma assertiva, zelando para que as informações prestadas sejam corretamente tratadas, utilizadas e armazenadas.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho cientifico**. 10. ed. São Paulo: Atlas, 2010.

BITTAR, Eduardo C. B. **Metodologia da pesquisa jurídica**. 16. ed. São Paulo: Saraiva, 2019.

BRASIL. **Autoridade Nacional de Proteção de Dados – ANPD.** Disponível em <https://www.gov.br/anpd/pt-br>. Acessado em 02 de novembro de 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Organizado por Cláudio Brandão de Oliveira. Rio de Janeiro: Roma Victor, 2002. 320 p.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**.

BRASIL. **Lei 12.965/14 – Marco Civil da Internet**. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 28 de outubro de 2023.

BRASIL**. Lei 13.709, de 14 agosto de 2018**. Brasília, DF. Disponível em <L13709 (planalto.gov.br)>. Acesso em 10 de Junho de 2024.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 628137 RG/RJ** – Rio de Janeiro. Repercussão geral no Recurso Extraordinário. Administrativo. Incidência dos juros progressivos sobre conta vinculada de Fundo de Garantia por Tempo de Serviço – FGTS. Aplicação dos efeitos da **ausência** de repercussão geral tendo em vista tratar-se de divergência solucionável pela aplicação da legislação federal. Inexistência de repercussão geral. Relatora: Min. Ellen Gracie, 21 de outubro de 2010. Disponível em http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=fgts&base=baseRepercussao. Acesso em 20 de agosto de 2023.

BRASIL. Superior Tribunal de Justiça. **Súmula n° 333**. Cabe mandado de segurança contra ato praticado em licitação promovida por sociedade de economia mista ou empresa pública. Diário da Justiça: seção 1, Brasília, DF, ano 82, n. 32, p. 246, 14 fev. 2007.

BRASÍLIA/DF: Presidência da República, [2016]. Disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm. Acesso em 02 de janeiro de 2024.

CARVALHO, André Castro; Bertoccelli, Rodrigo de Pinho; Alvim, Tiago C.; AL, et. **Manual de Compliance.** Forense, Grupo GEN, 2021. E-book. ISBN 9786559640898. Disponível em https://integrada.minhabiblioteca.com.br/#/books/9786559640898/. Acesso em: 28 de outubro de 2023.

CARVALHO, André C.; BERTOCCELLI, Rodrigo de P.; ALVIN, Tiago C.; AL, et. **Manual de Compliance**. Grupo GEN, 2021. *E-book.* ISBN 9786559640898. Disponível em <https://integrada.minhabiblioteca.com.br/#/books/9786559640898/> Acesso em: 02 de Novembro de 2023.

CASTRO, Filipe. **Compliance: Aspectos da iniciativa privada e da Adm. Pública.** Cefospe, 2020. Disponível em <https://www.scge.pe.gov.br/wp-content/uploads/2020/11/Curso-Aperfeicoamento-GGCI-2020-Compliance.pdf>. Acessado em 02 de novembro de 2023.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GODINHO, Thais. **Vida organizada: como definir prioridades e transformar seus sonhos em objetivos**. São Paulo: Gente, 2014. E-book.

GOV.BR. **Base jurídica – Autoridade Nacional de Proteção de Dados**. Disponível em < https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica> . Acessado em 16 de junho de 2024.

GOV.BR. **Portaria nº 1, de 8 de março de 2021.** Disponível em <https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618> Acessado em 15 de junho de 2024.

HENRIQUES, Antônio; MEDEIROS, João Bosco. **Monografia no curso de direito: trabalho de conclusão de curso**. 3. ed. São Paulo: Atlas, 2014.

JULIO, Rennan A. **Edward Snowden: "Não são dados sendo explorados, são pessoas".** Época Negócios, 2019. Disponível em https://epocanegocios.globo.com/Web-Summit/noticia/2019/11/edward-snowden-nao-sao-dados-sendo-explorados-sao-pessoas.html Acessado em 12 de novembro de 2023.

KPMG. **Pesquisa de Maturidade do Compliance no Brasil**. 4ª ed, 2019. Disponível em <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2019/10/br-pesquisa-de-maturidade.pdf>. Acessado em 02 de novembro de 2023.

KPMG. **Pesquisa de Maturidade do Compliance no Brasil**. 5ª ed, 2021. Disponível em <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2021/07/KPMG-pesquisa-maturidade-compliance-2021.pdf>. Acessado em 02 de novembro de 2023.

LEC. **Compliance no Brasil: tudo o que você precisa saber para se destacar na área**. LEC, 2022. Disponível em <https://lec.com.br/compliance-no-brasil-tudo-o-que-voce-precisa-saber-para-se-destacar-na-area/> Acessado em 02 de novembro de 2023.

ROMEIRO, Dandara Araruna; MASCARENHAS, Igor de Lucena; GODINHO, Adriano Marteleto. **Descumprimento da ética médica em publicidade: impactos na responsabilidade civil**. Revista Bioética [*online*]. 2022, v. 30, n. 1 [Acessado 23 Agosto 2023], pp. 27-35. Disponível em <https://doi.org/10.1590/1983-80422022301503PT https://doi.org/10.1590/1983-80422022301503EN https://doi.org/10.1590/1983-80422022301503ES>. Epub 09 Maio 2022. ISSN 1983-

8034. https://doi.org/10.1590/1983-80422022301503PT. Acessado em 23 de agosto de 2023.

SILVA, Ana Jasmim Barbosa da; CEREWUTA, Pollyanna Marinho Medeiros. **A RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES BANCÁRIAS POR DANOS SOFRIDOS NO GOLPE DO PIX**. **Facit Business and** Technology **Journal**, v. 4, n. 39, 2022.

STJ. RECURSO ESPECIAL: **AREsp 2130619-SP 2022/0152262-2. Relator: Ministro Francisco Falcão. DJ: 07/03/2023**. JusBrasil, 2023. Disponível em < https://www.jusbrasil.com.br/jurisprudencia/stj/1780119718/inteiro-teor-1780119729>. Acesso em: 11 de novembro de 2023.