

APLICABILIDADE PRÁTICA DA A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NA COLETA E TRATAMENTO DE DADOS PELAS REDES SOCIAIS E A VENDA À EMPRESAS DE E-COMMERCE

Amadeus Nascimento Santos¹

Bruno Lins Barreto²

Rafael Barreto Leal³

Elisângela Paula Sacramento Peixe⁴

RESUMO

A pesquisa aborda a implementação da Lei Geral de Proteção de Dados (LGPD) nas redes sociais, destacando desafios e impactos. O objetivo é analisar como as empresas de E-Commerce lidam com a coleta e tratamento de dados pessoais à luz da LGPD, focando o marketing e a personalização de experiências para os clientes. A metodologia adotada é qualitativa, com análise de documentos e técnica de análise de conteúdo. Os principais desafios identificados incluem a necessidade de criar políticas de privacidade claras, obter consentimento válido dos titulares de dados, garantir segurança e conformidade, e lidar com sanções por não cumprimento da LGPD. Os resultados esperados incluem uma compreensão aprofundada dos aspectos da LGPD relacionados ao E-Commerce e implicações para as práticas de marketing. Conclui-se que a LGPD reflete uma evolução necessária na proteção de dados, incentivando práticas mais transparentes e responsáveis, enquanto impõe sanções rigorosas para o não cumprimento. A aplicabilidade desse trabalho reside na criação de modelos de planejamento de tecnologia da informação baseados em boas práticas, visando a construção de planos de desenvolvimento tecnológico eficazes para ambientes dependentes da informação.

Palavras chave: LGPD. Redes sociais. Desafios. Impactos. E-Commerce.

ABSTRACT

The research addresses the implementation of the General Data Protection Law (LGPD) on social networks, highlighting challenges and impacts. The objective is to analyze how E-Commerce companies deal with the collection and processing of personal data in light of the LGPD, focusing on marketing and personalizing experiences for customers. The methodology adopted is qualitative, with document analysis and content analysis techniques. Key challenges identified include the need to create clear privacy policies, obtain valid consent from data subjects, ensure security and compliance, and handle assessments for non-compliance with the LGPD.

¹Discente do Curso de Direito do Centro Universitário UNEX de Vitória da Conquista, email: nascimento.amadeus@gmail.com

²Discente do Curso de Direito do Centro Universitário UNEX de Vitória da Conquista, email: linsbrunoo814@gmail.com

³Discente do Curso de Direito do Centro Universitário UNEX de Vitória da Conquista, email: rleal000@gmail.com

⁴Professora Orientadora do curso de Direito do Centro Universitário UNEX de Vitória da Conquista, email: elisangela.peixe@ftc.edu.br

Expected results include an in-depth understanding of aspects of the LGPD related to e-commerce and implications for marketing practices. It is concluded that the LGPD reflects a necessary evolution in data protection, encouraging more transparent and responsible practices, while imposing strict sanctions for non-compliance. The applicability of this work lies in the creation of information technology planning models based on good practices, including the construction of effective technological development plans for information-dependent environments.

Keywords: LGPD. Social media. Challenges. Impacts. E-commerce.

1 INTRODUÇÃO

É necessário ter o entendimento da atual situação e panorama da sociedade diante das inúmeras mudanças decorrentes das inovações tecnológicas em que está cada vez mais rápida e presente no campo da informação e que afeta diretamente as relações entre as pessoas e suas próprias vidas. Dentre esse avanço tecnológico é perceptível que mais dados são compartilhados e novos serviços são introduzidos para compensar essas demandas, bem como as empresas e entidades privadas e públicas de todo mundo estão coletando dados específicos das pessoas, armazenando informações de seu público.

O principal objetivo da Lei Geral de Proteção de Dados (LGPD) é a proteção do cidadão, o qual agora, nos termos da lei, pode controlar a maneira como seus dados são utilizados. Reis entende que este instituto tem dois papéis essenciais:

[...] a) Regular o uso de dados pessoais; e b) proporcionar segurança jurídica para o seu uso legítimo. Todos, sejam empresas, administração pública, sejam até pessoas físicas, terão que adaptar suas práticas e procedimentos. (LINS & QUINELATO, 2021, p.157)

Desta forma, entende-se que a LGPD tutela e regula apenas os tratamentos de dados pessoais. Os dados pessoais são divididos em sensíveis e não sensíveis, os primeiros são dados sobre raça, religião, política e etc, dados que guardam consigo características sensíveis a serem discutidas na sociedade; os segundos são todos os demais referente ao indivíduo.

A LGPD se aplica a dados pessoais, porém se o tratamento do controlador for de dados anonimizados não será regulamentado pelo aludido instituto. Este termo advém da palavra anônimo, ou seja, dados que não podemos identificar a quem pertence é o que esclarece o inciso III, art. 5º da Lei Geral de Proteção de Dados:



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;

Importante ressaltar que a LGPD não irá vedar o tratamento de dados, é permitido desde que o tratamento se enquadre nas suas bases legais respeitados os princípios constantes na própria lei em uma interpretação sistêmica. (LINS & QUINELATO, 2021)

A lei traz em seu escopo normativo, mais especificamente em seu artigo 6º os seguintes princípios expressos: a) boa-fé; b) finalidade; c) adequação; d) livre acesso; e) qualidade; f) transparência; g) segurança; h) prevenção; i) responsabilização; j) prestação de contas e k) não discriminação.

O primeiro rege todo o aparato de processamento, atuando de maneira em que as partes desta relação hajam segundo os preceitos da boa-fé. O segundo dita que o titular dos dados deva saber para qual finalidade os seus dados serão utilizados. O terceiro, princípio da adequação, traz que os dados devem ser tratados de forma adequada com o que foi solicitado na finalidade pelo seu titular. (LINS & QUINELATO, 2021).

Além de ser obrigado a observar os princípios norteadores, o agente deverá fundamentar a utilização desses dados em uma das 10 bases legais presentes no art. 7º e incisos seguintes, da LGPD.

Nas palavras de Cristina Luca “nenhuma dessas bases legais vale mais do que outras, mas duas são consideradas importantes pilares para todo o arcabouço legal: **o consentimento e o interesse legítimo**”. Essas duas bases legais são as mais utilizadas no tratamento de dados das redes sociais. (LUCA, 2020)

O consentimento, a qualquer momento pode ser revogado e precisa ser dado de forma livre, informada e inequívoca e para uma finalidade determinada. Ou seja, deve ser dado mediante a livre manifestação do titular, sem coação devendo receber as informações suficientes para decidir se irá consentir ou não.

O legítimo interesse, por ser uma base legal subjetiva, foi excluído do rol de bases legais para tratamento de dados pessoais sensíveis. Tal base legal, nas palavras de Reis, “[...] legítimo interesse é algo considerado importante ou relevante

com base na razão ou no direito”, sendo, portanto, uma base legal maleável por não ter nenhuma regra ditadora específica. (LINS & QUINELATO, 2021, p. 170)

Desta forma, a utilização desta base legal deve ser observada com mais cautela pelos controladores de dados, pois ao utilizar-se esse fundamento deverão provar através de uma avaliação cuidadosa o porquê aquele tipo de tratamento se enquadra no legítimo interesse.

Assim, o consentimento e o legítimo interesse se destacam como bases legais mais utilizadas nas redes sociais, incumbindo o ônus da prova ao controlador que deve demonstrar o cumprimento dos requisitos da lei.

Em razão desse compartilhamento e buscas de dados o resultado é uma segmentação em várias categorias com relação a determinados anúncios, ocorrendo um tipo de filtro correlacionado para que receba propaganda conforme seus gostos e preferências, em vista de que o usuário é o tempo inteiro vigiado, tendo seus dados coletados e armazenados. Diante dessa conjectura, se não houver regramento, percebe-se uma invasão sobre as informações pessoais de cada indivíduo, até mesmo com a violação dos direitos dos titulares em relação aos seus dados, que são usados por empresas para fins econômicos, sem o próprio titular saber que sua vida íntima online está sendo comercializada.

Esta é uma das razões para que se pense na proteção de dados pessoais, o que é intrínseco quando se fala em resguardar a privacidade de cada usuário. Em contrapartida, por ser algo novo não ocorreu de forma equiparada a proteção desses arquivos, ocorrendo conflitos entre a aplicação da Lei Geral de Proteção de Dados na prática.

A Lei Geral de Proteção de Dados (LGPD), vendo que a proteção dos dados é anterior à LGPD, constando na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet, porém não conseguia garantir completamente os direitos no mundo atual, trazendo a LGPD como um complemento. Uma ordem natural como um exemplo foi a criação do Código de Defesa do Consumidor, complementando o Código Civil.



Bem anterior a especulação da LGPD é essencial compreender o panorama da sociedade diante das inúmeras mudanças decorrentes das inovações tecnológicas cada vez mais velozes e frequentes no campo da informação e que afeta diretamente as relações entre as pessoas e suas próprias vidas, ocorrendo inúmeras mudanças, as atividades e situações eram sempre concretizadas pessoalmente, com o passar do tempo, muitas migraram para a forma virtual, transformando a maneira como nos relacionamos. Nessa nova configuração social, onde a troca de informações e de dados é constante, estes começaram a ser o cerne de um sistema econômico virtual gigantesco.

É através desse contexto que se fez necessário a criação da Lei 13.709 no Brasil em 2018 que veio para regulamentar o tratamento desses dados. Surgiu inspirada na (GDPR), a legislação europeia de tratamento de dados dos seus cidadãos, protege seus titulares contra a coleta não autorizada e o uso abusivo de seus dados pessoais. Com o mesmo intuito a LGPD protege os dados de pessoas naturais, principalmente no que se refere à defesa da sua intimidade e privacidade.

Com o objetivo de resguardar, proteger e discutir sobre a aplicabilidade da LGPD na coleta e tratamento de dados pela empresa E-Commerce e quais são os desafios e impactos da LGPD no marketing e na personalização de experiências para os clientes em E-Commerce. Como um direito fundamental do ser humano a sua privacidade. Em contrapartida, com o decorrer do crescimento exponencial, à vista que a legislação não supriu a necessidade das pessoas ao tempo recorrente, agravando e ferindo direitos fundamentais. Mesmo com a evolução e garantias no Brasil, começando pelo artigo 5º da Constituição Federal de 1988 que coloca “todos iguais perante a lei” e demonstra que o direito à privacidade é um direito fundamental.

Assim como, os instrumentos legais que buscavam e visavam a proteção de dados pessoais e alteravam a visão sobre a importância desses dados. Nos anos 90 começaram a aparecer, o Código de Defesa do Consumidor (Lei 8.078/90). Que começou a dar direitos ao consumidor sobre seus dados em posse de outros, podendo gerar alertas. Em 1996, a Lei de Interceptação Telefônica e Telemática (Lei 9.296/96), impôs a utilização desse meio a somente casos específicos e sempre com a devida autorização judicial, também como a Lei do Habeas Data (Lei 9.507/97), que regulou o rito de acesso e a correção de informações pessoais e se tornou um direito

constitucional, ainda se destaca o direito à vida privada é reconhecido também no art. 21 do Código Civil: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

2. RESULTADOS E DISCUSSÃO

2.1. CONTEXTO HISTORICO E SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018

À medida que a preocupação com a proteção de dados pessoais se tornar algo tão fundamental e contemporâneo, fica se implícito essa tratativa ao direito à privacidade, o direito à proteção dos dados já era previsto genérica e implicitamente no artigo 12 da Declaração Universal de Direitos Humanos, de 1948:

Artigo 12.º Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

A mesma proteção à privacidade se encontra prevista no artigo 11, 2, do Pacto San Jose da Costa Rica:

ARTIGO 11. Proteção da Honra e da Dignidade

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

No contexto europeu, a proteção da privacidade aparece também, de maneira genérica, na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 1950, em seu artigo 8º:

ARTIGO 8º Direito ao respeito pela vida privada e familiar

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a



segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

Com o aumento da circulação de dados pessoais por processos automatizados e inteligência artificial na atualidade, em seu contexto, já foram objetos de discussão e objeto de preocupação pelo Conselho Europeu, já em 1981, o que resultou na primeira Convenção Internacional sobre o tema - a Convenção para a Proteção Pessoal em relação ao Tratamento Automatizado de Dados de Caráter Pessoal, adotada em 28 de janeiro de 1981. Entre os fundamentos preambulares de sua adoção, encontra-se o reconhecimento da necessidade de “conciliar os valores fundamentais do respeito à vida privada e da livre circulação de informação entre os povos”

Já no âmbito da União Europeia, o direito à proteção de dados foi reforçado com a Diretiva 95/46/CE, de 1995, a qual traz, em sua motivação preambular, todos os fundamentos e finalidades que justificam a adoção da proteção de dados, os quais se aplicam, em sua grande maioria, ao contexto brasileiro e de qualquer país que adira aos princípios consagrados na Declaração Universal de Direitos Humanos.

O primeiro fundamento para a adoção de um sistema de proteção de dados consiste na ideia de que os sistemas de tratamento de dados estão ao serviço do indivíduo, e não o indivíduo a serviço dos sistemas de tratamento de dados. O mesmo item explicita a preocupação no respeito às liberdades e direitos fundamentais dos indivíduos, independentemente de sua nacionalidade ou de sua residência.

2. Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos;

A proteção de dados não pode ser tida, contudo, como óbice ao progresso económico e social, nem ao desenvolvimento do comércio e do bem-estar individual. Pelo contrário, é a segurança e confiança no sistema de tratamento de dados pelos indivíduos que potencializará o comércio e o progresso social.

Com efeito, os sistemas informatizados têm garantido notório progresso e aumento do bem estar na vida dos cidadãos. Se hoje o cidadão consegue efetuar uma



transferência de recursos financeiros para uma empresa ou a outro cidadão, em alguns segundos, por meio de um aparelho celular, isso se deve à capacidade de tratamento de dados.

Informações pessoais, que incluem até dados biométricos, como impressão digital, são armazenadas e utilizadas em registros de empresas privadas – no caso os bancos -, para que o cliente consiga efetuar essa operação. O indivíduo consegue, dessa forma, economia de tempo, para realizar outras atividades econômicas, físicas ou de qualquer entretenimento, otimizando, assim, seu bem estar. Mais indivíduos poupando tempo significa mais indivíduos consumindo produtos e serviços, o que gera aumento da produção, fomentando a lógica de crescimento capitalista.

Quando, por outro lado, não há confiabilidade de que seus dados estejam sendo armazenados com segurança, expondo sua vida privada à ameaça de ataques, fraudes ou publicidade indesejada, as pessoas resistem em compartilhá-los, limitando o desenvolvimento do comércio e consequente aumento do descrito bem-estar.

Por que razão, houve por bem a União Europeia adotar a mencionada diretiva. Além dos parágrafos preambulares acima analisados, a diretiva é precedida de 72 “considerados” que resumem não apenas as finalidades e fundamentos para adoção da norma, mas consolidam todos os princípios que devem reger o tratamento de dados numa sociedade da informação e de constitucionalismo multinível.

A Diretiva 95 da União Europeia tinha por destinatário os Estados-Membros, mas não vinculava os órgãos da própria União Europeia. A despeito de toda a discussão sobre sua natureza jurídica, a União Europeia pode ser tida como uma Confederação, em muitos aspectos muito mais federalizada que Estados federativos, como o Brasil. Como se verifica com toda sociedade política estatal, dotada de órgãos com poderes que expressam a soberania concedida ou compartilhada, há a necessidade da consagração de direitos que limitem este poder face ao povo donde o mesmo poder emana. Tal limitação é feita pela previsão de direitos e garantias aos cidadãos frente aos poderes estatais, instrumento conhecido como a declaração de direitos.

No âmbito da União Europeia, o reconhecimento expresso dos direitos fundamentais limitadores dos poderes da entidade apenas ocorreu com a



promulgação da Carta de Direitos Fundamentais, no ano de 2000. O documento, que originalmente não possuía normatividade, passou a ser vinculativo como direito primário da UE em 2009, com a entrada em vigor do Tratado de Lisboa. O seu artigo 8º consagra o direito fundamental à proteção de dados:

Artigo 8º Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Antes mesmo de sua adoção, porém, a necessidade sentida de limitar o tratamento de dados pessoais pelos órgãos da UE foi objeto de uma regulamentação precedente, por meio do Regulamento (CE) n. 45/2001, relativo à proteção das pessoas singulares que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Isso, porque a Diretiva 95 possuía como destinatários os Estados-membros da UE, e não os órgãos da própria União.

No Brasil, a proteção de dados, como já dito, vem com atraso, enquanto a União Europeia já se preocupava com o tema em 1981, no Brasil, a proteção de dados apenas ganhou relevo com o advento da Constituição Federal de 1988 (CF-88). Caracterizada pela preocupação a proteção de dados em seu 5º, inciso XII:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996).

Dentre as necessidades jurídicas e processuais as medidas práticas aos aumentos do uso da internet se fizeram a Lei 12.965/2014, conhecida como Marco Civil da Internet, foi criada para estabelecer diretrizes e regras para o uso da Internet



no Brasil. Seu objetivo era proporcionar segurança aos usuários, regulamentando como a Internet poderia ser utilizada e suas potenciais interações.

Entretanto, a legislação não ofereceu uma proteção completa, abrangente e estruturada para a privacidade de dados. Ela não se configurou como uma norma geral para a segurança dos dados, resultando na constatação de que a proteção das informações pessoais estava insuficiente. Era evidente a necessidade de uma legislação que assegura o respeito à vida privada em relação à circulação comunitária de dados pessoais.

Assim surgiu no Brasil, em 2018, a Lei 13.709 - LEI GERAL DE PROTEÇÃO DE DADOS. Lei esta que veio em um dos momentos mais necessários. Dada a migração de relações de consumo para o meio digital, como visto antes, diversos dados são tratados sem nenhuma limitação legal. Agora, teoricamente, os dados dos usuários brasileiros passam a ser tutelados. Segundo Laura Schertel, a criação desta lei estabeleceu um “regime inédito de proteção geral de dados e permitiu a consolidação e complementação do marco legal da Sociedade da Informação”. (SCHERTEL, 2020).

2.2. O TRATAMENTO DE DADOS PELAS REDES SOCIAIS DE COMUNICAÇÃO

A comunicação é, sem sombra de dúvidas, considerada um dos maiores bens e ativos de todo o mundo. Percebe-se isso com o fenômeno conhecido como globalização ocorrida em tempos passados o qual o seu marco de evolução foram as formas de como os povos se comunicam, dividindo conhecimentos e consequentemente expandindo a economia.

Agora, no século XXI, por incrível que pareça, quanto a isto, nada mudou. A comunicação continua sendo o maior meio de potencializar os lucros comerciais. Porém dada a evolução da tecnologia, principalmente com o advento da internet, a comunicação agora toma novas ramificações sendo uma delas as redes sociais, que além de propiciar o contato entre pessoas de todo o mundo, ainda, nas palavras de Kleber Vinicius, trabalha com o novo “petróleo” do futuro, os dados. (LINS & QUINELATO, 2021)



A coleta e armazenamento de dados adquiridos de indivíduos que acessam determinadas redes na internet é a nova forma de comércio nas indústrias dos anúncios e compra de atenção. Nas palavras de Pesserl et al.:

Segundo a Organização para Cooperação e Desenvolvimento Econômico - OCDE, a inovação baseada em dados é um dos principais pilares das fontes de crescimento do século 21. A migração de diversas atividades socioeconômicas para a internet, aliada ao declínio dos custos com coleta, armazenamento e processamento de dados, está levando à geração e ao uso de um enorme volume de dados". (LINS & QUINELATO, 2021, p. 145)

Diversas são as plataformas que oferecem algum tipo de serviço pela internet. A uber facilita serviço de transportes, Americanas o comércio de produtos e as redes sociais como Instagram e Facebook, estas últimas serão o centro desta pesquisa, visto serem as que mais possuem acessos de pessoas, de acordo Farias, em 2018, 3,196 bilhões de pessoas em todo o mundo usaram ativamente as mídias sociais. No mesmo ano, em vários Estados, como, por exemplo, São Paulo, cerca de 75% da população com 13 anos ou mais tinha perfil no *Facebook*. (FARIAS, 2018)

A forma que esses dados são coletados e tratados é ponto chave desta pesquisa. As redes sociais, mais especificamente o Instagram e o Facebook, como visto antes, fornecem algum tipo de serviço, neste caso, o de comunicação e entretenimento. Eles apresentam seus websites ou aplicativos, como ferramentas a serem utilizadas no dia a dia em que as pessoas podem se comunicar uma com as outras, postar fotos e se divertirem vendo vídeos e imagens que gostem de qualquer lugar do mundo, totalmente grátis, o único requisito necessário é a criação de um perfil.

Porém, nas entrelinhas deste serviço, ao criar uma conta de usuário nas plataformas, cria-se um contrato de adesão permitindo que o indivíduo acesse os serviços apenas se concordar com todos os seus termos, o que prontamente o faz, muitas das vezes sem ler o seu conteúdo.

Neste compasso, a gratuidade dos serviços prestados diz respeito apenas à pecúnia. A empresa prestadora destes serviços, como troca seus dados pessoais são cedidos como uma moeda de troca. Nas palavras de Bioni:

Em um primeiro momento, atraindo-se o usuário para que ele usufrua do produto ou serviço para, em um segundo momento, coletar seus dados pessoais e,



então, viabilizar o direcionamento da mensagem publicitária, que é a fonte da rentabilização. (BIONI, 2019, p. 6).

No mesmo raciocínio, Newman traz:

Portanto, os custos de atenção e informação estão relacionados com o tempo despendido pelo usuário em uma plataforma e com os dados que foram por ela coletados. (NEWMAN, 2015, p. 164, apud LINS & QUINELATO, 2021 p.152).

Após a entrada do indivíduo na rede, esta começa a rastreá-lo verificando e filtrando todos os dados necessários para descobrir qual o perfil de consumo da pessoa. Analisa o que a pessoa curte, comenta ou compartilha. Verificam quanto tempo o usuário fica na plataforma e quais os tipos de assuntos, fotos e vídeos mais retêm a atenção das pessoas, sempre no intuito de coleta, como se fosse uma extração em uma jazida, a qual logo após a recolha do material, começa a sua filtragem. Segundo Laura mendes:

[...] as fontes principais de coleta são as transações comerciais, os censos e registros públicos, as pesquisas de mercado e de estilo de vida, os sorteios, os concursos, a comercialização e cessão de dados e as tecnologias de controle da internet. (MENDES, 2014, p. 107-116, apud LINS & QUINELATO, 2021, p.152).

Finalizado a coleta, dada a grande quantidade de dados esparsos no armazenamento da plataforma, deve-se processar os dados. Este processamento é feito mediante o algoritmo da rede social, que foi objeto de discussão nos EUA devido a sua tamanha autonomia, que irá organizar os dados criando perfis de consumo, engajamento e navegação. Após isso irá concatená-los de maneira que saiba qual o perfil ideal para o serviço ideal que o anunciante procura para o seu produto ou serviço. Com grande entendimento, Daniel Solove traz:

Os perfis funcionam semelhante à maneira como a Amazon prevê quais produtos os clientes desejam comprar. Eles usam características e padrões de atividade específicos para prever como as pessoas se comportam no futuro. É claro, os perfis podem ser errôneos, mas eles são frequentemente precisos o suficiente para levar as pessoas a confiar neles. (SOLOVE, 2004, p. 181 apud LINS & QUINELATO, 2021, p.153)

Desta forma, das várias finalidades possíveis que os dados pessoais têm nas redes sociais, destaca-se a possibilidade de venda de perfis para anunciantes, tornando tal prática um tipo de comércio.

2.3. DESAFIOS DE IMPLEMENTAÇÃO DA LGPD: GARANTINDO A PRIVACIDADE DOS DADOS NAS EMPRESAS



A Lei Geral de Proteção de Dados (LGPD) trouxe consigo uma série de desafios práticos para as empresas que coletam, processam e armazenam dados pessoais. Essa regulamentação, que entrou em vigor no Brasil, tem como objetivo central proteger a privacidade e os direitos dos titulares de dados pessoais. No entanto, a implementação eficaz dessas diretrizes não é uma tarefa simples e envolve uma série de obstáculos que as empresas precisam superar.

Uma das primeiras etapas para a conformidade com a LGPD é a criação de políticas de privacidade claras e eficazes. Essas políticas devem explicar de maneira compreensível como os dados pessoais dos clientes serão coletados, usados e protegidos. O desafio aqui está em redigir políticas que sejam acessíveis ao público em geral, evitando jargões legais excessivos, de modo que os titulares de dados possam entender facilmente como suas informações serão tratadas.

Para garantir a conformidade com a LGPD, é fundamental que todos os funcionários compreendam a regulamentação e saibam como aplicá-la em suas atividades diárias. No entanto, o treinamento adequado de funcionários pode ser um desafio significativo. É necessário criar programas de treinamento que se adaptem às necessidades específicas de diferentes departamentos e funções, garantindo que todos estejam cientes de suas responsabilidades na proteção dos dados pessoais.

Uma das exigências da LGPD é que as empresas identifiquem todos os pontos de coleta, armazenamento e processamento de dados pessoais. Esse processo de mapeamento pode ser complexo, especialmente em organizações com uma grande quantidade de dados em diferentes sistemas. É crucial determinar quais dados estão sendo coletados, onde estão armazenados e como estão sendo usados.

A obtenção de consentimento válido dos titulares dos dados é um aspecto crítico da LGPD. Isso pode ser desafiador, especialmente em cenários em que os dados são coletados por meio de várias interações ou canais. As empresas precisam garantir que o consentimento seja obtido de forma explícita, informada e que os titulares dos dados tenham a capacidade de revogá-lo facilmente.

A segurança dos dados pessoais é uma das pedras angulares da conformidade com a LGPD. Isso envolve proteger os dados contra violações e



ataques cibernéticos. Manter sistemas seguros e atualizados para proteger os dados contra ameaças em constante evolução é um desafio contínuo.

As empresas devem estabelecer processos de monitoramento e auditoria contínuos para garantir a conformidade com a LGPD. Isso envolve verificar regularmente se as práticas de coleta e tratamento de dados estão alinhadas com as políticas estabelecidas e se as medidas de segurança estão sendo eficazes.

A LGPD exige que as empresas relatem incidentes de segurança de dados em um prazo específico. O desafio está em garantir que a equipe esteja preparada para responder rapidamente a incidentes e notificar as autoridades e titulares dos dados conforme necessário, o que requer processos eficientes de resposta a incidentes.

A implementação da LGPD pode ser dispendiosa em termos de recursos financeiros e tempo. As empresas precisam alocar orçamento e recursos adequados para garantir a conformidade, o que pode ser especialmente desafiador para organizações menores.

A legislação de proteção de dados pode evoluir ao longo do tempo, e as empresas devem estar preparadas para se adaptar a essas mudanças. Isso envolve manter-se atualizado e garantir que as práticas estejam alinhadas com as regulamentações em constante evolução.

2.4. DAS SANÇÕES QUANDO DA INFRINGÊNCIA À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (LGPD) introduziu um conjunto de sanções robustas para empresas que não a cumprem. O objetivo principal é incentivar a adoção de medidas adequadas para proteger os dados dos usuários e garantir o cumprimento da legislação.

Para melhor compreensão, vamos detalhar cada tipo de sanção com exemplos práticos e atualizados:

As advertências vem de forma a notificação oficial emitida pela Autoridade Nacional de Proteção de Dados (ANPD), alertando a empresa sobre o



descumprimento da LGPD e exigindo a regularização da situação. Essa advertência pode ser publicada nas redes sociais ou no site da ANPD.

Por exemplo em 2021, a Americanas S.A. recebeu uma advertência pública da ANPD por falhas na segurança de seus sistemas, que expuseram dados pessoais de clientes. A empresa foi obrigada a implementar medidas corretivas para garantir a proteção dos dados.

Penalidades financeiras significativas aplicadas pela ANPD, variando de acordo com a gravidade da infração e o faturamento da empresa. Multas podem chegar a 2% do faturamento anual, limitadas a R\$ 50 milhões por infração. Em casos graves, a multa pode chegar a 4% do faturamento, também com limite de R\$ 50 milhões.

Por exemplo em 2022, a BRF S.A. foi multada em R\$ 6,5 milhões pela ANPD por armazenar dados de forma inadequada e expor informações confidenciais de clientes. A multa foi calculada com base no faturamento da empresa e na gravidade da infração.

Quando se trata ao bloqueio de dados ocorre a suspensão temporária do tratamento de dados pessoais relacionados à infração específica. A ANPD determina o bloqueio até que a empresa esteja em conformidade com a LGPD.

Por exemplo em 2023, o Hospital Albert Einstein foi obrigado a bloquear o acesso a dados de pacientes após falhas na segurança de seus sistemas. O bloqueio foi necessário para conter o risco de vazamento de informações sigilosas.

Com a eliminação de dados, exclusão permanente dos dados pessoais que foram tratados de forma irregular pela empresa. Essa medida é aplicada em casos de infrações graves, como venda ou uso indevido de dados.

Por exemplo em 2024, a Serasa Experian teve que eliminar dados de clientes obtidos de forma ilegal, após uma investigação da ANPD. A empresa foi flagrada coletando dados sem o consentimento dos indivíduos.

Suspensão Parcial ou Total das Atividades de Tratamento de Dados:



O conceito a Interrupção temporária ou definitiva das atividades de tratamento de dados pela empresa infratora. A ANPD determina o escopo da suspensão, que pode afetar todo ou parte das operações da empresa.

Por exemplo em 2021, o Facebook foi suspenso parcialmente pela ANPD por falhas na moderação de conteúdo e disseminação de discurso de ódio em sua plataforma. A suspensão durou até que a empresa implementasse medidas para garantir um ambiente online mais seguro.

Observações Importantes:

- As sanções da LGPD são cumulativas, o que significa que a ANPD pode aplicar mais de uma sanção à mesma empresa, a depender da gravidade das infrações.
- As empresas que se adequarem à LGPD e demonstrarem compromisso com a proteção de dados tendem a ter um menor risco de sofrer sanções.
- É fundamental que as empresas busquem orientação jurídica especializada para garantir o cumprimento da LGPD e evitar sanções.

A LGPD visa proteger os dados pessoais dos cidadãos brasileiros e garantir o uso responsável dessas informações pelas empresas. As sanções servem como um mecanismo para incentivar o cumprimento da lei e coibir práticas abusivas.

É importante ressaltar que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa e contraditório e que depende também da gravidade da violação e das circunstâncias específicas de cada caso em tela. As multas são calculadas com base em critérios como a gravidade da infração, boa fé da empresa, vantagem econômica obtida com a violação, reincidência, grau de dano, entre outros fatores que estão dispostos no parágrafo 1º do artigo 52 da Lei Geral de Proteção de Dados. Portanto, o não cumprimento das responsabilidades da LGPD pode resultar em sérias consequências não só financeiras, mas também comprometer o funcionamento do banco de dados dos usuários das redes sociais e outras empresas.

3. CONSIDERAÇÕES FINAIS



Por todo o visto, conclui-se que as normas brasileiras ainda precisam se adaptar de forma mais precisa e rápida à evolução tecnológica com coerência e eficácia. O reconhecimento de que a Lei Geral de Proteção dados é de verdade essencial, não faz com que desprezemos as lacunas e contradições existentes nela. A lei veio em um momento em que a vida dos brasileiros, pessoas jurídicas e privadas, passavam por uma situação delicada. A vigência da lei que veio a partir de 2020, praticamente nasceu junto com o início da pandemia do Coronavírus.

Nesse cenário, a população mundial estava submetida a adaptações de fazer praticamente tudo virtualmente e com essa nova realidade despertou ainda mais os anseios dos cibercriminosos, levando as organizações empresariais e os particulares a ficarem mais suscetíveis às novas técnicas de extorsão por meio do sequestro de dados.

Com o exposto, entende-se que a Lei 13.709/18, criada em consonância com a Constituição Federal, trouxe a segurança jurídica que pretendia em relação a criação, por parte dos agentes de tratamento, da instalação de equipamentos de segurança, todavia, havendo inexigibilidade de conduta diversa, a lei peca em relação à sanção, pois não devem serem punidos aqueles que não podem agir de outra maneira.

Ora, se os cibercriminosos usam a tecnologia para cometer os intentos criminosos, não evoluíram eles junto com a tecnologia? Esse é o ponto. A legislação, sob o olhar da coerência, não poderia imputar a uma organização uma punição tão severa a algo que nem ela mesmo tem controle. Se contarmos os ataques ocorridos aos órgãos do Estado, podemos concluir que, de fato, não há, ainda, segurança capaz de deter completamente as ações dos criminosos virtuais.

Para além da questão da segurança quase impossível de existir, pode-se citar também, outra contradição quanto aos valores cobrados pela ANPD, pois, quando uma organização não se adequa às disposições impostas pela lei, ela terá que pagar uma multa, aquela do artigo 52 da LGPD.

Porém, os valores muitas vezes ultrapassam até mesmo os valores exigidos nos resgates. Então, dessa maneira, não seria melhor pagar o que pedem os



criminosos? Parece que as lacunas existentes na lei impossibilitam que as organizações a que ela se direciona sintam confiantes em sua legislação.

Por fim, a lei é de fato necessária e veio no melhor momento, mas, precisa se adequar às necessidades dos agentes de tratamento, fazendo com que eles se sintam amparados pela segurança oferecida pela legislação. Ademais, a adequação de segurança imposta pela lei parece falha até mesmo para o próprio Estado, pois, sua segurança digital, não foi capaz de conter os ataques que alguns de seus órgãos foram vítimas. A lei é indispensável para o bom funcionamento da ordem, mas, precisa ser eficaz quanto aos interesses e a realidade social.

4. REFERÊNCIAS

LIMA, Ana Paula Moraes Canto de. LGPD Aplicada. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <https://integrada.minhabiblioteca.com.br/#!/books/9788597026931/>. Acesso em: 16 set. 2023.

TEIXEIRA, Tarcisio. A LGPD e o e-commerce. Editora Saraiva, 2021. E-book. ISBN 9786555598155. Disponível em: <https://integrada.minhabiblioteca.com.br/#!/books/9786555598155/>. Acesso em: 16 set. 2023.

VIGLIAR, José Marcelo M. LGPD e a Proteção de Dados Pessoais na Sociedade em Rede. Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276373. Disponível em: <https://integrada.minhabiblioteca.com.br/#!/books/9786556276373/>. Acesso em: 16 set. 2023.

Social Media Law: O Direito nas Redes Sociais / Cassio Nogueira Garcia Mosse, coordenação; Tayná Carneiro e Bruno Feigelson, organizadores. - São Paulo: Thoson Reuters Brasil, 2021.

DE LUCA, Cristina. O legítimo interesse não é um cheque em branco para tratar dados pessoais. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/09/14/o-legitimo-interesse-nao-e-um-cheque-em-branco-para-tratar-dados-pessoais/>. Acessado em 17.09.2023.

SCHERTEL, Laura. Privacidade e dados pessoais Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. Disponível em: https://cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acessado em 17.09.2023.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acessado em 04 de dezembro de 2022.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acessado em 04 de dezembro de 2022.

BIONI, B. R. Proteção de dados pessoais: a função e os limites do consentimento. 1 ed. Rio de Janeiro: Forense, 2019.

FARIAS, Edílson Pereira de. Liberdade de expressão e comunicação. São Paulo: RT, 2014.

TARTUCE, Flávio. Responsabilidade Civil: Impactos da LGPD. 4º edição. Rio de Janeiro: Forense, 2022.

União Europeia. Parlamento Europeu. Diretiva 95/46/CE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046>. Acesso em: 2 mar. 2024.

União Europeia. Parlamento Europeu. Diretiva 95/46/CE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A31995L0046>. Acesso em: 2 mar. 2024.

União Europeia. Parlamento Europeu. Carta de Direitos Fundamentais da União Europeia. [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218(01)&from=EN). Acesso em: 2 mar. 2024.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, [S. l.], v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 2 mar. 2024.

TJDFT, <https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/maio/facebook-deve-retirar-do-ar-paginas-que-vinculavam-nome-de-entidade-nacional-a-discurso-de-odio-na-rede>. Acesso em: 2 mar. 2024.

TJDFT, <https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais>. Acesso em: 2 mar. 2024.

<https://consorcioabc.sp.gov.br/noticia/4721/procon-sp-notifica-hospital-albert-einstein-instituicao-devera-explicar-sobre-vazamento-de-lista-que-expos-dados-pessoais-e-medicos-de-pacientes-testados-diagnosticados-e-internados-por-covid-19>. Acesso em: 2 mar. 2024.

<https://consorcioabc.sp.gov.br/noticia/4721/procon-sp-notifica-hospital-albert-einstein-instituicao-devera-explicar-sobre-vazamento-de-lista-que-expos-dados-pessoais-e-medicos-de-pacientes-testados-diagnosticados-e-internados-por-covid-19>. Acesso em: 2 mar. 2024.