O USO DAS REDES SOCIAIS E A LEI GERAL DE PROTEÇÃO DE DADOS

THE USE OF SOCIAL MEDIA AND THE GENERAL DATA PROTECTION LAW

Ana Clara Ramos de Carvalho[1]

RESUMO

Em um contexto onde a informação é frequentemente utilizada para fins comerciais, o presente estudo aborda como a Lei Geral de Proteção de Dados (LGPD), implementada no Brasil em 2020, busca proteger os direitos de privacidade dos usuários ao impor diretrizes e responsabilidades para empresas que lidam com dados pessoais. Para tanto, foi realizada uma pesquisa de revisão bibliográfica a respeito do tema proposto, visando levantar dados para responder a seguinte pergunta: Qual é a relação entre o uso das redes sociais e a LGPD? Analisando casos de exposição de dados sem consentimento, o estudo examina os principais desafios que a LGPD enfrenta para assegurar a conformidade das redes sociais, incluindo questões de consentimento, segurança de dados, e o direito dos usuários de acessar, corrigir ou excluir suas informações. Assim, conclui-se que é importante conscientizar tanto usuários quanto empresas sobre o uso ético de dados e a necessidade de incorporar práticas de proteção à privacidade desde a concepção das plataformas digitais. Ao promover o cumprimento da LGPD, o estudo contribui para a criação de um ambiente digital mais seguro, em que os direitos dos indivíduos são respeitados.

Palavra-chave: LGPD; Redes Sociais; Internet e proteção de dados.

ABSTRACT

In a context where information is frequently used for commercial purposes, this study addresses how the General Data Protection Law (LGPD), implemented in Brazil in 2020, seeks to protect users' privacy rights by imposing guidelines and responsibilities for companies that handle personal data. To this end, a literature review was conducted on the proposed topic, aiming to collect data to answer the following question: What is the relationship between the use of social networks and the LGPD? By analyzing cases of data exposure without consent, the study examines the main challenges that the LGPD faces in ensuring compliance by social networks, including issues of consent, data security, and the right of users to access, correct, or delete their information. Thus, it is concluded that it is important to raise awareness among both users and companies about the ethical use of data and the need to incorporate privacy protection practices from the design of digital platforms. By promoting compliance with the LGPD, the study contributes to the creation of a safer digital environment, in which the rights of individuals are respected.

Keyword: LGPD; Social Networks; Internet and data protection.

[1] Bacharelanda em Direito – Doctum JF/MG

1 INTRODUÇÃO

"O recurso mais valioso do mundo não é mais o petróleo, são dados" [THE ECONOMIST, 2017], Esta afirmação destaca a importância dos dados na economia moderna, comparando-os a um recurso essencial que move o mundo contemporâneo. Redes sociais, como o Instagram, ilustram perfeitamente esse fenômeno, pois coletam, armazenam e utilizam um vasto conjunto de informações pessoais para direcionar conteúdo, impulsionar engajamento e atémesmo traçar o perfil de seus usuários.

No entanto, essa coleta massiva de dados apresenta riscos significativos à privacidade, gerando preocupações globais sobre a proteção das informações pessoais. No Brasil, a Lei Geral de Proteção de Dados (LGPD), em vigor desde2020, busca regulamentar o tratamento de dados pessoais, estabelecendo direitos para os cidadãos e obrigações para as empresas e indivíduos que manipulam essas informações.

Nesse contexto, surgem também preocupações com a privacidade e a proteção dos dados dos usuários, especialmente diante do uso crescente desses dados por plataformas digitais e perfis de entretenimento e fofoca. Zuboff (2019) descreve essa prática como "capitalismo de vigilância", onde dados pessoais sãoexplorados economicamente, muitas vezes sem o devido consentimento dos indivíduos. Essa nova realidade exige regulamentações para proteger o direito àprivacidade dos cidadãos, principalmente quando figuras públicas são expostassem autorização.

A Lei Geral de Proteção de Dados (LGPD), sancionada no Brasil em 2018, tem como objetivo regulamentar o tratamento de dados pessoais e sensíveis, estabelecendo diretrizes e responsabilidades para empresas, plataformas digitais e indivíduos (BRASIL, 2018). Segundo Santos e Silva (2020), a LGPD representa um avanço para o país, pois "estabelece uma série de princípios de segurança e transparência, garantindo aos titulares de dados um maior controlesobre suas informações pessoais".

Neste contexto, o presente trabalho tem como objetivo investigar a relação entre o uso de dados pessoais por perfis de fofoca no Instagram e a aplicação

da LGPD, buscando compreender as consequências legais e éticas da exposição de dados sem consentimento. Para ilustrar essa análise, será abordado o caso da atriz Klara Castanho, cuja vida pessoal foi exposta de forma abusiva, gerando grande repercussão pública e trazendo à tona o debate sobreos direitos de privacidade e a responsabilidade da mídia digital.

Assim, esta pesquisa propõe-se a discutir os limites da exposição midiática e os mecanismos de proteção de dados previstos pela LGPD, analisando até queponto a legislação brasileira é capaz de proteger o direito à privacidade no ambiente digital. Espera-se, com isso, contribuir para o entendimento das responsabilidades legais nas redes sociais e para a conscientização sobre a importância de um uso ético e seguro dos dados pessoais.

2. TRATAMENTO DE DADOS NAS REDES SOCIAIS E A LGPD

As redes sociais são provavelmente a maior novidade da última década para os meios de comunicação, visto que lhes proporcionam uma interatividade insuspeitada até muito recentemente. Tradicionalmente, o rádio era o meio que podia abrir regularmente seus microfones em tempo real para os ouvintes. No entanto, isso dependia da disponibilidade de tempo na grelha e da natureza do programa. Hoje, qualquer mídia que se preze desembarcou em uma rede social, seja como uma corporação, seja por meio da utilização de abrir seus programas mais significativos para a interação com o usuário (CASTELLS, 2013).

Por esse procedimento, as possibilidades de dar destaque ao seguidor se multiplicam e vão desde a conversa em tempo real até a provocação. A interação na rede social permite assim que o utilizador se integre na dinâmica do programa, esteja em contato com o a opinião em tempo real e, dada a capilaridade destes meios, multiplique o impacto de cada emissão. Ao fenômeno das redes sociais deve-se somar o impacto da chamada blogosfera, que, de fato, foi anterior no tempo. Nasceu um jornalismo de opinião do cidadão - nem sempre rigoroso - e os meios de comunicação tradicionais se apressaram em incorporar em seus espaços na internet um espaço de blog, seja conduzido por seus profissionais, seja aberto ao cidadão (GOMES, 2017).

Uma compreensão clara do contexto é essencial para a aplicação das regras de proteção de dados pessoais. Como Castells, apontou em sua época, a evolução da rede favorece a geração de comunidades, tanto por meio da transferência de grupos sociais pré-existentes para o mundo virtual, quanto por meio da criação de grupos de interesse globais. Além disso, grande parte dos serviços a ela vinculados são voltados para o lazer e para a promoção de aspectos diretamente relacionados à vida pessoal ou privada, como compartilhar fotos, ouvir música ou compartilhar vídeos, ou expressar uma opinião por meio de pílulas curtas de 140 caracteres (LIMBERGER, 2016).

Para isso, deve-se reunir um conjunto de elementos técnicos, cuja influência futura é imprevisível hoje. Em primeiro lugar, a onipresença é uma das características mais proeminentes dos serviços de Internet. O telefone móvel torna-se um gestor e organizador completo com funções que vão desde a agenda pessoal à gestão na chamada “internet das coisas” através da tomada de decisões baseada em serviços de valor acrescentado, como a geolocalização (MAYER-SCHONBERGER e CUKIER, 2013).

O telefone é agora um espaço de lazer e jogos partilhados, uma ferramenta de acesso às redes sociais ou um fornecedor de acesso a serviços de televisão digital interativa. Por outro lado, também do ponto de vista tecnológico, o universo web deixou de ser um lugar passivo para se tornar um espaço social muito dinâmico. O usuário pode expressar sua opinião, obter opiniões de terceiros, se mostrar. É um ambiente complexo no qual os aplicativos nem sempre são do provedor principal e os usuários podem ser testadores beta e desenvolvedores (BORELLI, 2019).

Se desse ponto de vista de seu funcionamento básico e "tradicional", a internet apresentava um desafio para a proteção da vida privada, ela é mais complexa nas redes sociais, onde perfis genéricos de um usuário ou identidades fictícias não são mais suficientes. Para ser eficaz em uma rede social, para atingir seus objetivos, o indivíduo se identifica. E, neste contexto, a identidade tem um valor extraordinário, porque graças a ela as informações, a mensagem ou a publicidade são personalizadas. Eles terão a capacidade de estabelecer ou identificar círculos de confiança e, graças a isso, a viralidade das mensagens multiplica a eficiência e eficácia dos tratamentos (PIÑAR MANÃS, 2017).

Em nenhum caso a contribuição das redes sociais para o debate público deve ser questionada; exemplos recentes de democratização nos países do norte da África são uma prova clara. Isso não significa que as ações dos próprios provedores e usuários não estejam sujeitas a regras. Portanto, a primeira pergunta que devemos nos fazer é se existem princípios aplicáveis à Internet e, em particular, às redes sociais. E a resposta só pode ser afirmativa. Portanto, a questão em seus aspectos centrais não reside tanto em determinar se existem ou não princípios básicos aplicáveis, que obviamente existem, mas se eles são realmente levados em conta desde o design inicial das aplicações (BIONI, 2019).

Atualmente, os dados pessoais e as informações em geral são considerados bens econômicos fundamentais, o que representa um desafio para o poder legislativo que deve garantir o cumprimento do direito à privacidade e, ao mesmo tempo, garantir que a utilização que diferentes entidades ou organizações dão à informação dos cidadãos. é apropriado e é feito com o consentimento dos proprietários das informações (BIONI, 2019).

No entanto, o conceito de propriedade de dados pessoais tem algumas reservas a nível internacional, pois tem implicações importantes para o futuro da economia digital e do comércio de dados; é por isso que o conceito de propriedade de dados surgiu recentemente como um direito legal no nível da União Europeia. Janeček afirma que uma discussão pode ocorrer e que os dados são um alvo móvel; o que significa que o que agora é considerado pessoal pode se tornar não pessoal graças aos grandes avanços tecnológicos e analíticos nos quais a sociedade está imersa todos os dias (LIMBERGER, 2016).

Esta situação suscita um interessante debate sobre quais dados específicos a legislação em vigor deve aplicar; e sobre como o dinamismo da classificação dos dados pode modificar as leis atuais ou levar à publicação de novas. Hoje em dia é muito comum encontrarmos que os buscadores armazenem as consultas feitas pelos usuários, o que possibilita rastrear o computador de onde essas consultas estão sendo feitas, lembrando o interesse de cada pessoa. Os motores de busca são geralmente gratuitos e a utilização destes serviços implica a renúncia ao direito à privacidade ou a redução do âmbito da mesma (LÉVY, 2011).

O mesmo ocorre com outros serviços de internet, como redes sociais, e-mail e serviços de armazenamento em nuvem. Essas atividades permitem que as informações de interesse dos usuários sejam vendidas para campanhas publicitárias, meios de comunicação, dentre outros. Porém, o problema ocorre quando essas mesmas informações são utilizadas para fins indesejáveis às pessoas, como roubo de contas bancárias por meio de phishing, entre outros (FARIA, 2019).

Atualmente, a computação é considerada a quinta utilidade mais importante depois da água, eletricidade, gás e telefonia que, graças aos importantes avanços tecnológicos do dia-a-dia, tem despertado o interesse no desenvolvimento de serviços de computação em nuvem. Quatro modelos de implantação de nuvem estão atualmente definidos: nuvem privada, nuvem comunitária, nuvem pública e nuvem híbrida.

A nuvem privada é destinada apenas a uma organização, enquanto a nuvem pública é para o público em geral. A nuvem comunitária é composta por um conjunto de organizações com interesses comuns; e o híbrido é uma composição dos modelos de nuvem já descritos (CASTELLS, 2013).

O crescimento dos serviços de hospedagem em nuvem soma-se aos desafios descritos anteriormente em termos de proteção de dados e informações, uma vez que como a nuvem é um meio armazenado na internet, todos os riscos de segurança da internet são transferidos para ela. Além disso, há outras implicações, como, por exemplo, que as informações sejam armazenadas e processadas em diferentes localizações geográficas ao redor do mundo com regulamentações distintas, o que pode implicar em problemas de jurisdição e conformidade legal; que a infraestrutura física seja compartilhada entre os usuários; e que os provedores de serviços de computação em nuvem tenham acesso às informações do usuário, entre outros (CHENG e LAI, 2012).

Nesse sentido, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) definiu o termo de responsabilidade comprovada, para fornecer uma solução para proteção de dados que inclui cinco elementos fundamentais:

> Compromisso das organizações com a responsabilidade e adoção de políticas internas de acordo com o contexto externo. Mecanismos para implementar políticas de privacidade, incluindo ferramentas de treinamento e educação. Sistemas de revisões internas, com supervisão contínua e garantia de verificação externa. Transparência e mecanismos de participação individual. Meios de remediação e conformidade externa (Barros, 20, p.43).

O princípio da responsabilidade demonstrada é muito relevante, uma vez que a sua implementação inclui benefícios não só para os titulares dos dados pessoais, mas também para as organizações; permitindo maximizar o uso inteligente da informação, aumentar seu nível de competitividade e consolidar sua reputação empresarial (GOMES, 2017).

O guia para a implementação do princípio da responsabilidade demonstrada nas transferências internacionais de dados tem por objetivo apresentar algumas recomendações para o envio de dados pessoais a outros países, respeitando os direitos dos titulares das informações. Este guia está orientado para que sua implementação seja realizada em países latino-americanos. As recomendações a seguir são descritas em detalhes para implementar o princípio de responsabilidade na transferência de dados pessoais (LÉVY, 2011).

Além da transferência de informação, existe também a transmissão da mesma e é muito importante levar em consideração a diferença entre esses dois conceitos, sendo a transferência entendida como a ação de entregar a informação a um terceiro para que o receptor irá tratá-lo de forma independente do responsável ou gerente. Durante a transmissão, o receptor tratará as informações de acordo com as regras impostas pelo remetente (ZANATTA, 2019).

Além disso, uma estrutura institucional para segurança digital consistente com uma abordagem de gerenciamento de risco, que deve levar em consideração os seguintes itens:

> Criar as condições para que várias partes interessadas gerenciem o risco de segurança digital em suas atividades socioeconômicas e criar confiança no uso do ambiente digital; Fortalecer a segurança dos indivíduos e do Estado no ambiente

> digital, e a nível nacional e transnacional, com um abordagem de gestão de risco; Fortalecer a defesa nacional e a soberania no ambiente digital com uma abordagem de gestão de risco; Gerar mecanismos permanentes e estratégicos para promover a cooperação, colaboração e assistência em segurança digital, nacional e internacionalmente (Borelli et al., 2019, p.34).

É sabido por muitas pessoas que o século 21 trouxe consigo muitas mudanças, tanto na indústria, transporte, comércio, relações internacionais, em suma. Mas a era da internet pode ser sem dúvida a maior mudança que ocorreu à humanidade nos últimos tempos, desde que comparamos o modo como as atividades quotidianas que realizamos hoje são realizadas com a forma como o fazemos por pelo menos trinta anos percebemos a olho nu o impacto que a internet gerou na vida e no desenvolvimento do ser humano. Nas comunicações, por exemplo, há três décadas era necessário enviar uma mensagem através dos sistemas de correspondência da época, dependendo totalmente dos horários do prestador do serviço para que fosse efetuada a entrega do documento ou comunicação (MAYER-SCHONBERGER e CUKIER, 2013).

Todos os dias é muito comum ver como são oferecidos serviços “gratuitos” na internet como buscadores, e-mail, acesso a redes sociais, música, filmes, serviços de entretenimento, entre outros, agora, como esses serviços são financiados se o usuário final não paga pelo seu uso? Vale destacar uma frase que se ouve muito nos dias de hoje "a era da informação", e é bastante assertiva se a aplicarmos ao uso de serviços de Internet sem pagar por eles, em por outras palavras, a remuneração que está a ser paga pela utilização dos referidos serviços é provavelmente a informação do próprio utilizador (MAYER-SCHONBERGER e CUKIER, 2013).

Os serviços do Google se destacam por estarem presentes no sistema operacional de uma grande quantidade de smartphones como o Android, isso pode ser uma faca de dois gumes para o gigante da internet, já que nos últimos dias foi multado em pouco mais de R $ 4,3 bilhões por abuso de posição dominante no sistema operacional Android ("Multa histórica da UE para o Google para Android: 4,34 bilhões de euros por abuso de posição dominante", 2018), como gigante da Internet, o Google se apoia em sua necessidade de oferecer um serviço onipresente serviço, sem a necessidade de estar solicitando ao

usuário dados que possam ser captados de forma transparente por sensores telefônicos, localização, contatos frequentes, rotinas de transporte, ou seja, o que proporciona é uma experiência na utilização de seus serviços ao custo da entrega do quantidade de dados (BIONI, 2019).

3 USO DE DADOS E O DIREITO DA PERSONALIDADE

Para compreender a importância do direito digital na proteção de dados pessoais, devemos mencionar o mais importante precedente internacional desse direito. Isso surge após a Segunda Guerra Mundial, uma vez que diversos instrumentos jurídicos internacionais, invocando a dignidade humana, reconhecem o direito à não ingerência na vida privada das pessoas, como um direito humano. a vida familiar como direito inerente à pessoa, bem como o respeito e a não ingerência no domicílio e na correspondência (BARROS, 2020).

Os artigos dos instrumentos internacionais referidos são: artigo 12 da Declaração Universal dos Direitos Humanos, de 10 de dezembro de 1948; Artigo 11 da Convenção Americana sobre Direitos Humanos (Pacto de San José, Costa Rica) de 1966; Artigo 17 do Pacto Internacional de Direitos Civis e Políticos de 19 de dezembro do mesmo ano de 1966; Artigo 8 da Convenção Européia de Direitos Humanos de 4 de novembro de 1950; da mesma forma, a Carta dos Direitos Fundamentais da União Européia assinada em Nice em 7 de dezembro de 2000 (DONENA, 2010).

Embora não encontremos um reconhecimento expresso do direito à proteção de dados pessoais nos instrumentos internacionais acima mencionados, podemos afirmar que, no desenvolvimento dos direitos humanos, essa figura encontra seu antecedente mais importante. Além do exposto, deve-se dizer que cada país optou por configurar o direito à não ingerência na vida privada das pessoas, através de diferentes figuras jurídicas. No caso do Brasil, consiste em um reconhecimento constitucional do direito à proteção de dados pessoais, desenvolvido no marco dos postulados da doutrina europeia e dos esquemas de autorregulação e setorização do sistema anglo-saxão (FORTES, 2016).

Dito isto, a recepção e reconhecimento do direito à proteção de dados pessoais no Brasil teve que esperar até 2002, com a Lei Federal de Acesso à

Informação Pública do Governo, que foi o primeiro sistema legal a reconhecer o direito à proteção de dados pessoais. para o domínio público. Mas isso foi apenas uma limitação ao exercício do direito de acesso à informação. Mais tarde, em 2009, as reformas constitucionais dos artigos 16º e 73º conferiram pleno reconhecimento à proteção de dados pessoais como direito fundamental e autónomo. Da mesma forma, essas reformas deram ao Congresso poderes para legislar sobre o assunto (FORTES, 2016).

No entanto, dois grandes problemas foram observados: a legislação sobre proteção de dados pessoais no setor público não garantia todos os direitos de acesso, retificação, cancelamento e oposição, e o segundo problema estava relacionado à falta de regulamentação que se aplicasse a proteção de dados pessoais no setor privado (FORTES, 2016).

Nesse sentido, foi em 2010 que pela primeira vez houve disposições expressas que as empresas observariam para o tratamento de dados pessoais no setor privado, por meio da Lei Federal de Proteção de Dados Pessoais de Titularidade Privada. Finalmente, em 2018, foi emitida a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 133.709, com a qual se harmonizaram as normas sobre o assunto no Brasil (BRASIL, 2018).

Para compreender a relevância do direito à proteção de dados pessoais na sociedade da informação e do conhecimento, é necessário analisar as componentes do conceito, bem como a classificação dos dados pessoais, de acordo com o tipo de informação que refletem. Nesse sentido, o titular dos dados pessoais é o indivíduo e sua proteção é um direito recentemente reconhecido no Brasil. Os dados de um indivíduo são pessoais e ele tem o direito de reserva e confidencialidade ou à maior cobertura da liberdade de privacidade (GLOBALGCS, 2020).

Os dados pessoais referem-se à informação do indivíduo, que permite identificá-lo através da sua descrição, origem, local de residência, histórico académico e laboral, entre outros. Os dados pessoais também podem ser sensíveis, descrevendo aspectos do indivíduo, como seu modo de pensar, estado de saúde, características físicas, ideologia, vida sexual, entre outros (GONÇALVES, 2017).

Vários instrumentos proporcionaram uma definição de dados pessoais, entre os quais se destacam a Convenção 108 do Conselho da Europa para a proteção das pessoas no que diz respeito ao tratamento automatizado dos seus dados pessoais, bem como as diretrizes da Organização para a Cooperação e Desenvolvimento sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais, e a Diretiva 95/46/EC do Parlamento Europeu e do Conselho da Europa sobre a proteção de dados pessoais emitida em 1995. Esta última define dados pessoais como "todas as informações sobre uma pessoa física identificada ou identificável" (JÚNIOR, 2019).

No caso do Brasil, a LGPD define dados pessoais como qualquer informação relativa a uma pessoa física identificada ou identificável. Prevê uma definição de dados pessoais sensíveis, aqueles que se referem a dados pessoais que afetam a esfera mais íntima do seu titular ou cuja utilização indevida pode dar origem a discriminação ou implicar um risco grave para o mesmo (ZANATTA, 2019).

São muitas as características dos dados pessoais, cuja importância e significado dependem do uso da informação que constituem. Uma vez definidos os conceitos de dados pessoais e dados pessoais sensíveis, o leitor poderá perceber que a informação utilizada pelo serviço no Brasil inclui essas duas categorias de dados, razão pela qual o cumprimento da lei é fundamental (ZANATTA, 2019).

Uma vez analisado o conceito de direito à proteção de dados pessoais, é necessário falar sobre os princípios nesta matéria. Para tanto, é pertinente definir o que se entende por princípio no campo jurídico. Os princípios são mandatos de otimização; ou seja, são normas que ordenam a realização de algo na medida das possibilidades jurídicas e reais. Tais princípios caracterizam-se pelo fato de poderem ser cumpridos em diferentes graus, uma vez que seu cumprimento depende não apenas das possibilidades reais, mas também das legais. Este, por sua vez, é determinado por regras e, sobretudo, por princípios que atuam na direção oposta. Portanto, sua ponderação é necessária (BARROS, 2020).

O direito à não ingerência na vida privada das pessoas é um direito humano reconhecido desde a Declaração Universal dos Direitos Humanos de

1948. No entanto, no caso do Brasil, foi feito o reconhecimento expresso do regime de proteção de dados pessoais em poder das empresas até 2010, o que levou a uma defasagem na regulamentação sobre o assunto, em contraste com outros países (FARIA, 2019).

4 O USO DAS REDES SOCIAIS E A LEI GERAL DE PROTEÇÃO DE DADOS

Como observado nas informações levantadas, a ascensão das redes sociais transformou a maneira como os indivíduos compartilham informações e se relacionam no ambiente digital. Essas plataformas acumulam uma quantidade imensa de dados pessoais, criando um cenário desafiador para a privacidade dos usuários. Neste contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada no Brasil em 2018 e em vigor desde 2020, estabelece diretrizes para o tratamento de dados e busca assegurar os direitos dos usuários em relação às suas informações pessoais. Este artigo explora a relação entre o uso das redes sociais e a LGPD, analisando os principais desafios e implicações para a proteção dos dados dos usuários.

As redes sociais operam com um modelo de negócios que valoriza o uso extensivo de dados pessoais, como preferências de consumo, localização, e hábitos de navegação, para personalizar conteúdos e oferecer publicidade direcionada. A coleta e o processamento desses dados ocorrem muitas vezes de forma opaca, com pouca transparência para o usuário. Segundo a LGPD, as redes sociais devem obter consentimento explícito e garantir que os dados coletados sejam usados apenas para os fins informados e autorizados pelo usuário.

Contudo, observa-se que o cumprimento dessas diretrizes nem sempre é fácil para as plataformas de redes sociais, especialmente aquelas internacionais, como Facebook e Instagram, que têm suas próprias políticas de privacidade e práticas de coleta de dados. Além disso, a complexidade da infraestrutura tecnológica dessas plataformas torna difícil para os usuários acompanharem como seus dados são utilizados, criando uma lacuna entre as práticas reais das empresas e os requisitos de transparência e segurança previstos pela LGPD.

A LGPD impõe uma série de obrigações que buscam dar maior controle aos usuários sobre seus dados pessoais. Entre os principais direitos garantidos pela LGPD estão o direito de acesso, o direito à retificação e o direito de exclusão de dados. No contexto das redes sociais, esses direitos obrigam as plataformas a desenvolverem mecanismos que permitam que o usuário possa visualizar, corrigir ou excluir seus dados com facilidade.

Por outro lado, o processo de adequação à LGPD pode representar um custo elevado para as empresas de redes sociais, especialmente no que tange à implementação de mecanismos de segurança e à necessidade de nomeação de um encarregado de proteção de dados. A conformidade com a LGPD exige mudanças significativas nas práticas de coleta e tratamento de dados, o que pode gerar um impacto nos modelos de monetização dessas empresas.

Conforme destacado por Castells (2013), a integração de plataformas como Facebook, Instagram e Twitter em nossa rotina transformou a forma como acessamos e produzimos informações, democratizando a comunicação e multiplicando o impacto das mensagens. No entanto, esse ambiente dinâmico e de fácil acesso levanta questões críticas sobre a privacidade e a proteção de dados pessoais, especialmente em um contexto onde a informação digital é frequentemente vista como um ativo econômico valioso.

A Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, similar à GDPR na Europa, foi implementada como resposta aos crescentes desafios de proteção dos dados pessoais no cenário digital. A lei estipula que as empresas obtenham o consentimento explícito dos usuários para coleta e uso de dados e que tratem as informações pessoais com transparência e segurança. No contexto das redes sociais, essa exigência traz implicações complexas, uma vez que os modelos de negócio dessas plataformas frequentemente dependem de técnicas avançadas de personalização e direcionamento de anúncios, que envolvem a coleta massiva de dados, muitas vezes de forma opaca para o usuário. Além disso, conforme apontado por Bioni (2019), a LGPD exige que o tratamento de dados pessoais seja conduzido de forma ética e responsável, alinhando-se a um princípio de responsabilidade comprovada para minimizar abusos no uso das informações.

Um dos principais desafios discutidos por Limberger (2016) e Borelli (2019) reside na complexidade do ambiente digital atual, onde o celular e outras tecnologias móveis facilitam a coleta constante e omnipresente de dados pessoais. Os smartphones, por exemplo, com funcionalidades como geolocalização e acesso a redes sociais, capturam detalhes diários sobre hábitos e preferências do usuário, muitas vezes sem uma compreensão clara dos mesmos sobre o uso final desses dados. Essa prática, que visa aprimorar a experiência do usuário por meio de conteúdos personalizados, levanta preocupações sobre a autonomia do usuário e a possível invasão de sua privacidade. Além disso, a análise de Mayer-Schönberger e Cukier (2013) enfatiza como o armazenamento em nuvem e a transmissão de dados entre fronteiras geográficas diferentes criam desafios legais e de conformidade, principalmente pela variação das regulamentações de privacidade e segurança entre países.

Outro ponto relevante abordado por Gomes (2017) é o impacto da chamada "blogosfera" e do jornalismo de opinião digital na gestão de dados pessoais. Com a proliferação de blogs e plataformas que permitem a expressão de opiniões sem o rigor tradicional do jornalismo, o controle e a proteção de dados tornam-se tarefas ainda mais complexas. Ao permitir que cidadãos comuns assumam um papel de relevância na produção de conteúdo, as redes sociais e blogs ampliam o número de fontes de dados e aumentam o risco de compartilhamento irresponsável de informações. Essa questão está diretamente ligada ao princípio da responsabilidade comprovada (ou accountability), que exige das organizações uma postura proativa e transparente no tratamento dos dados pessoais, conforme destacado pela OCDE e citado por Barros (2019).

Por fim, embora as redes sociais sejam reconhecidas como um importante meio para fortalecer o debate público e democratizar o acesso à informação, a LGPD e outras regulamentações internacionais vêm reforçar que essa liberdade de comunicação deve ser acompanhada por uma sólida estrutura de proteção de dados. A legislação busca equilibrar a necessidade de inovação e monetização das plataformas com a segurança dos direitos individuais. Para que essa proteção seja efetiva, é essencial que os desenvolvedores e gestores de

redes sociais integrem princípios de privacidade desde a concepção de suas plataformas, adotando práticas como a pseudonimização e a minimização de dados para reduzir o potencial de invasão de privacidade dos usuários.

Em resumo, o uso massivo e interativo das redes sociais impõe desafios significativos à privacidade e à proteção de dados. A LGPD surge como uma ferramenta essencial para proteger os direitos dos usuários em um ambiente digital cada vez mais intrusivo, onde a informação pessoal é um recurso valioso, mas também vulnerável. Portanto, a implementação de regulamentações mais rígidas e a promoção de uma cultura de respeito aos dados pessoais são passos fundamentais para assegurar que o impacto positivo das redes sociais no debate público e na interação social não seja comprometido por violações de privacidade.

5 Conclusão

Os dados pessoais têm um alto valor econômico e social. Em sua proteção está uma oportunidade de construir confiança entre clientes e usuários do serviço, a fim de consolidar modelos de negócios. Embora o impulso da regulamentação sobre a proteção de dados pessoais no Brasil atenda à garantia de um direito humano, também encontra sua origem em aspectos econômicos em nível internacional. Alcançar padrões de níveis adequados de proteção da informação tem sido condição para que o país se declare seguro nas trocas comerciais.

Apesar de o marco legal em matéria de proteção de dados pessoais no Brasil incluir padrões internacionais e oferecer garantias para a proteção efetiva desse direito, o cumprimento das disposições enfrenta grandes desafios. Exemplo disso é o desconhecimento das implicações jurídicas do tratamento da informação, a falta de ética no referido tratamento, a dessensibilização quanto às repercussões do mau uso da informação e o desconhecimento dos mecanismos legais para exigir esse direito.

Do exposto, podemos deduzir que as informações pessoais processadas na Internet podem identificar ou tornar identificável uma determinada pessoa, uma vez que incluem informações de tipo identificativo como nome, morada,

número de telefone, fotografias; entre outros, daí a importância de proteger essas informações em áreas intangíveis como a internet ou como o ciberespaço é conhecido hoje.

REFERÊNCIAS

BARROS, Julião Napoleão de. **Big data, proteção de dados e transparência: Desfios para a consolidação da confiança e garantia dos direitos do cidadão.** Vol. 07, N.07, Maio/Ago. 2020. Disponível em: https://periodicos.uff.br/culturasjuridicas/article/view/45329/26012. Acesso em: 06 de setembro de 2024.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BORELLI, Alessandra et al. LGPD: Lei Geral de Proteção de Dados comentada. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

BRASIL. **Lei Geral de Proteção de Dados. 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 06 de setembro de 2024.

CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2013.

DONEDA, Danilo**. A proteção dos dados pessoais nas relações de consumo:** para além da informação creditícia. Brasília: SDE/DPDC, v.2, p.122, 2010.

FARIA, Luisa Campos. **Impactos do Big Data e das Legislações de Proteções de Dados nas Análies Antitruste**. Brasília, 2019. Disponível em: https://bdm.unb.br/bitstream/10483/23556/1/2019_LuisaCamposFaria_tcc.pdf. Acesso em 06 de setembro de 2024.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

GLOBALGCS. **5 benefícios de ter lgpd para empresas.** Disponível em: https://globalgcs.com.br/5-beneficios-de-ter-lgpd-para-empresas/. Acesso em: 06 de setembro de 2024.

GOMES, Rodrigo Dias de Pinho. **Big data: desafios à tutela da pessoa humana na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2017.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado.** São Paulo: Atlas, 2017.

JUNIOR, Sérgio Ricardo de Sá. **A regulação jurídica de dados pessoais no Brasil.** Rio de Janeiro. 2019. Disponível em: https://www.maxwell.vrac.puc-rio.br/37295/37295.PDF. Acesso em: 06 de setembro de 2024.

LÉVY, Pierre. Cibercultura. 3.ed. São Paulo: Ed.34, 2011.

LIMBERGER, Têmis. **Cibertransparência: informação pública em rede: a virtualidade e suas repercussões na realidade.** Porto Alegre: Livraria do Advogado, 2016.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big data: a Revolution that will transform how we live, work, and think**. New York: Houghton Mifflin Harcourt, 2013.

PIÑAR MAÑAS, José Luis. **Sociedad, innovación y privacidad. Información Comercial Española**, ICE: Revista de economía, Madrid, n. 897, p.70, jul./ago, 2017.

SANTOS, L. F.; SILVA, M. R. A proteção de dados no Brasil: Impactos e desafios da LGPD. **Revista Brasileira de Direito Digital**, v. 2, n. 1, p. 45-62, 2020.

ZANATTA, Rafael A. F. **A proteção de dados pessoais entre leis, códigos e programação:** os limites do marco civil na internet. 2019. Disponível em: file:///C:/Users/Pedro/Downloads/A_Protecao_de_Dados_Pessoas_entre_Leis_C.pdf Acesso em 06 de setembro de 2024.

ZUBOFF, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. NewY ork: **PublicAffairs**, 2019.