Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Sistemas de Informação

Ética e Privacidade:
Um Estudo Sobre os Problemas da Coleta de Dados Pessoais nas Redes Sociais

Victor Guerra Horta

JUIZ DE FORA
JULHO, 2023

Ética e Privacidade:
Um Estudo Sobre os Problemas da Coleta de Dados Pessoais nas Redes Sociais

Victor Guerra Horta

Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Bacharelado em Sistemas de Informação

Orientador: Edelberto Franco Silva

JUIZ DE FORA
JULHO, 2023

ÉTICA E PRIVACIDADE:
Um Estudo Sobre os Problemas da Coleta de Dados Pessoais nas Redes Sociais

Victor Guerra Horta

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Aprovada por:

Edelberto Franco Silva
Doutor em Computação

Alex Borges Vieira
Doutor em Computação

Luciana Conceição Dias Campos
Doutora em Engenharia Elétrica

JUIZ DE FORA
01 DE JULHO, 2023

Resumo

No contexto atual do tratamento de dados pessoais impulsionado pelo *Big Data*, a prática automatizada de coleta de dados, conhecida como *data scraping*, ganha relevância, especialmente na *web* e na obtenção de dados pessoais. Esta pesquisa analisa os dilemas éticos do direito à privacidade nas redes sociais, examinando a efetividade da proteção dos usuários e os princípios de liberdade e autonomia na internet. Além disso, explora temas como propaganda direcionada, *marketing* digital e compartilhamento excessivo de dados, contextualizando-os em relação à privacidade e apresentando estratégias de remediação.

Conforme revisão da literatura acerca do tema privacidade e *Big Data*, o estudo se destaca por explorar casos de estudo específicos, visando oferecer reflexões aprofundadas sobre dilemas éticos e garantia dos direitos fundamentais. Esses aspectos ressaltam a importância da manutenção do Estado Democrático de Direito, considerando a interseção entre a proteção de dados pessoais e a vivência democrática no ciberespaço.

Ao examinar leis relevantes, como a Lei Geral de Proteção de Dados, o Regulamento Geral de Proteção de Dados da União Europeia e o marco civil da internet, a pesquisa contribui para uma compreensão mais ampla dos desafios éticos na coleta de dados pessoais nas redes sociais.

Palavras-chave: Privacidade. Ética da informação. Redes sociais. Lei Geral de Proteção de Dados Pessoais.

Abstract

In the current context of personal data processing driven by big data, the automated practice of data collection, known as data scraping, gains relevance, especially on the web and in obtaining personal data. This research examines the ethical dilemmas of the right to privacy on social networks, analyzing the effectiveness of user protection and the principles of freedom and autonomy on the internet. Additionally, it explores topics such as targeted advertising, digital marketing, and oversharing, contextualizing them in relation to privacy and presenting remediation strategies.

Through a literature review on the subject of privacy and big data, the study stands out for exploring specific case studies, aiming to provide in-depth reflections on ethical dilemmas and the guarantee of fundamental rights. These aspects highlight the importance of maintaining the Democratic Rule of Law, considering the intersection between personal data protection and democratic experiences in cyberspace.

By examining relevant laws such as the Brazilian General Data Protection Law, the General Data Protection Regulation of the European Union, and the civil framework of the internet, the research contributes to a broader understanding of the ethical challenges in collecting personal data on social networks.

Keywords: Privacy. Information ethics. Social networks. Brazilian General Data Protection Law.

Agradecimentos

Gostaria de expressar minha profunda gratidão a todas as pessoas contribuíram para a realização deste trabalho de conclusão de curso. Sem o apoio e a orientação dessas pessoas, este projeto não seria possível. Portanto, é com grande satisfação que dedico esta seção para expressar minha gratidão a todos.

Primeiro, quero agradecer aos meus familiares. Aos meus pais, Glauco e Paula, devo um agradecimento especial. Eles foram os pilares do meu crescimento, fornecendo amor e apoio ao longo de toda a minha vida. Sua dedicação e sacrifícios permitiram que eu trilhasse meu caminho para chegar onde estou hoje.

Em seguida, gostaria de agradecer ao Professor Doutor Edelberto por sua orientação e incentivo ao longo de todo o processo de elaboração deste TCC. Sua experiência e conhecimento foram fundamentais para a realização deste trabalho. Sou imensamente grato pela sua paciência, atenção e pelos valiosos conselhos que recebi durante todas as etapas deste projeto.

Não posso deixar de mencionar meus amigos, em especial Bernardo, Caio, Daniel, João e Pedro que estiveram sempre ao meu lado. Agradeço a todos pelo apoio, pelos momentos compartilhados e pelo incentivo constante. Nossas discussões e trocas de ideias contribuíram significativamente para o meu crescimento pessoal e acadêmico.

Por fim, gostaria de estender meu agradecimento aos membros da banca examinadora, por dedicarem seu tempo e esforço para revisar e avaliar este trabalho. Suas contribuições e sugestões foram extremamente valiosas para o aprimoramento deste TCC.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações e Siglas

ANPD Autoridade Nacional de Proteção de Dados. 37, 39

LGPD Lei Geral de Proteção de Dados. 9, 14, 17, 18, 20, 23–25, 31, 35–37, 39

MCI Marco Civil da Internet. 14–16, 20, 35

RGPD Regulamento Geral de Proteção de Dados. 9, 14, 16, 17, 20, 25, 35

UE União Europeia. 9, 16, 17, 20, 25

1 Introdução

1.1 Apresentação do Tema

A coleta de dados pessoais nas redes sociais é um assunto complexo que envolve questões éticas como privacidade, consentimento e uso dos dados. Ela é necessária para o funcionamento dessas plataformas, mas também pode ser utilizada para fins comerciais, o que pode levar a violações de privacidade e direitos dos usuários.

De acordo com um estudo realizado por Acar e Yildirim (2019), a coleta de dados pessoais nas redes sociais pode ser dividida em dois tipos: a voluntária, quando os usuários fornecem informações de forma consciente, e a involuntária, quando os mesmos não são conscientes de que suas informações estão sendo coletadas. Ambos os tipos podem levar a questões éticas, como a falta de transparência e o uso indevido dos dados.

Grewal e Kannan (2017) destacam a importância do consentimento dos usuários nesse contexto. Eles argumentam que os usuários devem ser informados sobre como seus dados serão usados e dar sua permissão antes de serem coletados. Além disso, os usuários devem ter a capacidade de controlar e excluir suas informações pessoais.

Stutzman (2018) também discute esse tema, ele defende que a falta de consentimento pode levar a violações de privacidade e direitos daqueles que utilizam a plataforma. Ele reforça a necessidade de transparência e segurança dos dados coletados.

Por fim, Taddeo e Floridi (2018) expõem que a ética na coleta de dados pessoais nas redes sociais deve ser baseada em princípios como transparência, privacidade, responsabilidade e respeito aos direitos dos usuários. Eles destacam a importância de regulamentações para garantir que esses princípios sejam seguidos e os usuários tenham seus direitos protegidos.

1.2 Contextualização

As redes sociais, como Facebook, Instagram e Twitter são utilizadas por milhões de pessoas em todo o mundo e são uma fonte valiosa de dados pessoais, tais como informações demográficas, interesses e hábitos de consumo (GARCIA; CALLE, 2016). Esses dados são usados para fins comerciais, como publicidade e *marketing* personalizado. No entanto, eles também podem ser explorados de maneira prejudicial, por exemplo, criando perfis falsos e manipulando pessoas por meio de técnicas enganosas conhecidas como engenharia social (FURNELL; WARREN, 2016).

A coleta de dados pessoais nas redes sociais tem sido tema de debate entre especialistas e governos, devido aos riscos que essa prática pode representar para a privacidade dos usuários e ao uso indevido desses dados (LYON, 2014). Além disso, existe a preocupação com a falta de transparência nas políticas de privacidade das redes sociais e com a falta de mecanismos de controle para os usuários (STUTZMAN, 2011). Com a crescente automação dos sistemas de processamento de dados, se tornou necessária a criação de uma regulamentação capaz de proteger seus usuários (MOOR, 2005).

Os primeiros debates sobre o tema originaram-se na União Europeia (UE), em especial com o partido *The Greens*, que se consolidaram na promulgação do RGPD - Regulamento geral de Proteção de Dados (GDPR - General Data Protection Regulation), tendo como tema central a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (PECK, 2016).

Ao entrar em vigor, o RGPD inspirou outros continentes e países a tomarem caminhos semelhantes. Assim, em 14 de agosto de 2018 foi publicada a Lei Nº13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), que dispôs sobre a proteção de dados no Brasil e passou a ter sua vigência em agosto de 2020. A nova legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico (BEDENDO et al., 2019).

1.3 Descrição do Problema

Estamos inseridos em uma cultura que incentiva a exposição de dados pessoais, ao mesmo tempo que não garante a proteção da privacidade do indivíduo no ambiente digital. O hábito de compartilhar de forma excessiva informações muitas vezes sensíveis, também conhecido como *oversharing*, impulsiona cada vez mais a quantidade de dados disponíveis no ambiente digital (FUGAZZA; SALDANHA, 2017).

O comércio de dados pessoais tem se tornado cada vez mais presente na sociedade atual, devido ao aumento da relevância das redes sociais e à facilidade de acesso à internet. No entanto, esse comércio pode trazer sérios problemas à privacidade e à segurança das pessoas. De acordo com Kwok e Wang (2019), o comércio de dados pessoais pode levar à exposição de informações pessoais sensíveis, como dados financeiros e de saúde, o que pode resultar em fraudes e roubo de identidade. Além disso, esses dados podem ser utilizados para fins maliciosos, como a segmentação de público para campanhas políticas desonestas (GUSTAFSSON; JOHNSON, 2019).

Além disso, as redes sociais mantêm seus termos de uso e privacidade propositalmente complexos e extensos, que conduzem o usuário à desinformação. Isso permite que o mesmo concorde, sem a devida noção, com cláusulas de uso irrestrito dos seus dados e solicitações oportunistas de organizações que coletam dados sem nenhum vínculo com o serviço em questão, muita das vezes para fins ilegítimos (TANNER, 2013).

Em Março de 2018, ocorreu o caso[1] de vazamento de dados do Facebook, em que a empresa Cambridge Analytica obteve informações de milhões de pessoas sem o seu consentimento. As informações incluíam dados pessoais, como interesses, amigos e informações de perfil, e foram usadas para criar perfis psicológicos altamente detalhados dos usuários. Para cada pessoa, a Cambridge Analytica coletava dados individuais que podiam chegar a mais de 9.000 pontos sobre a personalidade de cada indivíduo, abrangendo desde sua movimentação geográfica diária, contatos periódicos, nível cultural, extratos bancários, até suas mais sutis preferências, desejos, medos e anseios. Esses perfis psicológicos permitiam que a empresa segmentasse os usuários individualmente ou

[1] https://www.theguardian.com/membership/2018/sep/29/cambridge-analytica-cadwalladr-observer-facebook-zuckerberg-wylie

em grupos específicos, adaptando as mensagens políticas e propagandas de acordo com suas características psicológicas. Por exemplo, uma pessoa mais sensível poderia receber uma imagem que remetesse a emoções específicas. (CADWALLADR, 2018).

O acesso aos dados dos usuários do Facebook pela Cambridge Analytica ocorreu através de uma aplicação de teste psicológico chamada "thisisyourdigitallife", desenvolvida por um pesquisador universitário. Os usuários que concordaram em fazer o teste permitiram que tanto seus dados pessoais quanto os de seus amigos do Facebook fossem coletados e usados para fins de pesquisa. No entanto, o pesquisador repassou indevidamente esses dados para a Cambridge Analytica, que os utilizou para fins políticos, indo além do que havia sido autorizado pelos usuários. Esse acesso não autorizado aos dados de milhões de pessoas levantou questões significativas sobre privacidade e ética, resultando em severas consequências para ambas as empresas envolvidas e gerando uma ampla discussão sobre a proteção de dados pessoais na era digital. (CADWALLADR; GRAHAM-HARRISON, 2018).

1.4 Justificativa

A coleta de dados pessoais nas redes sociais é um tema relevante e atual devido ao crescente uso dessas plataformas e ao impacto que elas têm na sociedade. A quantidade de informações pessoais que as pessoas compartilham nessas redes tem aumentado muito ao longo dos anos, e isso tem gerado preocupações com relação à privacidade e segurança desses dados (ACQUISTI, 2015; WANG; CHEN; CHEN, 2016).

Atualmente, empresas de tecnologia e outras organizações consomem informações demográficas e comportamentais de seus clientes com a finalidade de personalizar sua experiência. Dessa forma, os produtos dessas empresas se tornam cada vez mais específicos e atrativos para os usuários (GARCIA; CALLE, 2016). Nesse contexto, Bedendo et al. (2019) sustentam que:

> "A criação de leis específicas no sentido de proteção de dados pessoais avoluma gradativamente com a crescente expansão tecnológica e com os desdobramentos da globalização, que trouxe como uma de suas consequências a valorização

da informação, podendo-se dizer que o acesso a dados é o mesmo que o acesso ao poder."

Em suma, o tema é importante e complexo, envolvendo questões éticas como privacidade, consentimento e uso dos dados. É necessário que haja regulamentação e mecanismos de proteção para garantir que os usuários tenham seus direitos protegidos e possam controlar suas informações pessoais (União Europeia, 2016).

1.5 Objetivos

O objetivo geral desse trabalho é refletir sobre os dilemas do direito à privacidade no contexto das redes sociais, pontuando problemas quanto à efetividade da garantia de proteção da privacidade de seus usuários e os princípios da liberdade e autonomia no ambiente digital.

E os objetivos específicos são:

- Discutir como a tecnologia afeta a privacidade e como as políticas de privacidade e as práticas dos usuários precisam ser aprimoradas;
- Evidenciar crimes cibernéticos e suas implicações para a privacidade e segurança de dados.
- Sugerir direções futuras para pesquisas e regulamentações no tema privacidade de dados no contexto *Big Data* .

1.6 Organização do Trabalho

Este trabalho está estruturado em seis capítulos, cada um abordando aspectos específicos. Após esta introdução (Capítulo 1), o Capítulo 2 apresenta uma base teórica, explorando conceitos importantes relacionados à proteção de dados. Em seguida, o Capítulo 3 detalha os trabalhos relacionados utilizados como referência, realizando uma breve comparação entre eles para destacar as lacunas a serem preenchidas. No Capítulo 4, são analisados casos pertinentes que contribuem para a compreensão e exemplificação dos aspectos abordados neste trabalho. O Capítulo 5 é dedicado à discussão aprofundada dos resultados

obtidos, explorando suas implicações e relacionando-os à base teórica e aos trabalhos relacionados. Por fim, o Capítulo 6 traz as considerações finais deste trabalho, englobando uma síntese dos principais resultados e contribuições, juntamente com sugestões para trabalhos futuros, que podem expandir e aprofundar os temas abordados.

2 Fundamentação Teórica

Para o entendimento desta pesquisa, esse capítulo busca deixar claro termos e expressões que serão utilizados com frequência. Além disso, também serão definidos os conceitos considerados de maior importância. Ao final, foram feitas considerações levando em conta os temas discutidos. Assim, os conceitos utilizados nesta pesquisa são: Privacidade, Marco Civil da Internet (MCI), LGPD, Regulamento Geral de Proteção de Dados (RGPD) e Técnicas de Coleta de Dados Pessoais.

2.1 Privacidade

O direito à privacidade é um direito fundamental previsto no Artigo 5º, incisos X e XII da Constituição da República Federativa do Brasil de 1988. No entanto, com o desenvolvimento da tecnologia e a intensificação dos fluxos de informação, surgem novas possibilidades de coleta, armazenamento, utilização e manipulação de informações pessoais, refletindo em mudanças no conceito de direito à privacidade. Riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido dos dados pessoais, cadastro e classificação dos indivíduos, propagandas de *marketing* invasivas, publicidade comportamental, vigilância estatal, utilização indevida da *Big Data*, coleta de dados através da Internet das coisas, entre outros (FINKELSTEIN; FINKELSTEIN, 2020).

A coleta, armazenamento e uso de dados pessoais pelas empresas e pelo Estado têm sido alvo de críticas e questionamentos, especialmente com a popularização das redes utilizadas pelos meios jornalísticos. Nesse contexto, tornou-se evidente que a liberdade de imprensa e o direito à privacidade entraram em conflito. Finkelstein e Finkelstein (2020) explicam que a privacidade na Internet é semelhante à imprensa no sentido de que ela pode expor informações pessoais embaraçosas e usar métodos questionáveis para coletar informações. No primeiro caso, é clara a semelhança com a imprensa: divulgar informações ou fatos que prejudiquem a intimidade, a vida privada, a honra e a imagem

de uma pessoa na Internet constitui uma violação da privacidade. No entanto, a Internet traz um agravante: o fato pode ser divulgado em escala global, o que nunca foi possível com outros meios de comunicação de massa.

De acordo com o estudo de Ferreira (2017), as redes sociais têm sido cada vez mais utilizadas como fonte de notícias e informação, e isso tem afetado a forma como as notícias são veiculadas e consumidas. Por outro lado, como apontado por Silva e Almeida (2019), a utilização das mídias como fonte de notícias tem levado à fragmentação do público e à crescente competição entre veículos de comunicação. Além disso, as plataformas apresentam desafios, como a disseminação de notícias falsas e a exposição a conteúdo seletivo, o que pode comprometer a privacidade e a segurança das pessoas na internet.

2.2 Marco Civil da Internet

O Marco Civil da Internet (MCI) é uma lei brasileira que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Ela garante o direito à privacidade dos usuários da internet, incluindo a proteção de dados pessoais, bem como a liberdade de expressão e acesso à informação. A lei estabelece também responsabilidades para provedores de serviços de internet, como a neutralidade da rede e a preservação da liberdade de expressão e acesso à informação (Brasil, 2014).

Ademais, o MCI aborda questões importantes como a responsabilidade dos provedores de serviços de internet em relação a conteúdo ilegal, como a pirataria ou conteúdo que viole direitos autorais. Nesses casos, os provedores devem remover o conteúdo após receberem uma notificação. Além disso, a lei aborda o armazenamento de dados dos usuários, garantindo que as informações sejam mantidas de forma segura e que as autoridades só possam acessá-las mediante autorização judicial (Brasil, 2014).

O Artigo 7º do MCI é de suma importância, uma vez que trata diretamente dos direitos e garantias dos usuários. Ele estabelece a obrigação de obtenção de consentimento prévio dos usuários para o tratamento de seus dados pessoais e a possibilidade de revogação desse consentimento a qualquer momento. O Artigo prevê também a possibilidade do usuário solicitar a exclusão de seus dados pessoais, exceto quando esses dados são necessários para o cumprimento de obrigações legais ou contratuais. Por último, é

estabelecido o direito de informações claras e completas, com detalhamento sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais (Brasil, 2014).

Embora seja amplamente reconhecido como um passo importante na proteção dos dados e das liberdades na internet, o MCI ainda enfrenta desafios significativos. A implementação efetiva das regras pode ser um desafio devido à falta de recursos e capacidade técnica, e a lei não possui mecanismos eficazes para garantir que as empresas sigam as regras estabelecidas para proteger os dados dos usuários. Além disso, o mundo digital está em constante evolução, o que significa que as leis relacionadas a Internet também precisam ser atualizadas para enfrentar novos desafios, como o uso massivo de tecnologias de rastreamento e a coleta de dados por parte de empresas (LEMOS (2014)).

2.3 Regulamento Geral de Proteção de Dados Pessoais

A transparência é um elemento essencial do Regulamento Geral de Proteção de Dados Pessoais (RGPD), que entrou em vigor em maio de 2018 na União Europeia (UE). O RGPD estabelece a obrigação das empresas de informar os indivíduos sobre como seus dados pessoais estão sendo processados e notificar as autoridades de proteção de dados em caso de violações de segurança. Além disso, o regulamento concede aos indivíduos o direito de acessar suas informações pessoais, bem como corrigi-las ou excluí-las.

Apesar de ser uma medida positiva para proteger a privacidade e os dados pessoais dos cidadãos europeus, o RGPD também enfrenta desafios, como a complexidade e os custos de implementação. Nesse sentido, a literatura tem indicado que a implementação efetiva do RGPD requer uma avaliação de impacto à proteção de dados, a nomeação de um Encarregado de Proteção de Dados, a revisão dos contratos de processamento de dados e a implementação de políticas e treinamentos adequados para os funcionários (CORDERY; SIM, 2018).

A relevância do RGPD transcende as fronteiras da UE, tendo em vista que muitas empresas não estão localizadas na região, mas ainda processam dados pessoais de cidadãos da UE, tornando-se sujeitas ao RGPD. OLIVEIRA (2021) destaca que o RGPD teve um

impacto significativo em empresas de todos os tamanhos e setores, não apenas na UE, mas também em todo o mundo. A implementação efetiva do RGPD pode ajudar a fortalecer a confiança dos consumidores nas empresas e, ao mesmo tempo, garantir a proteção adequada dos dados pessoais.

Portanto, o RGPD é uma regulamentação importante para proteger os direitos e liberdades fundamentais dos cidadãos da UE, incluindo a proteção de suas informações pessoais. Dessa forma, as empresas que processam dados pessoais devem estar em conformidade com o RGPD, adotando medidas adequadas para proteger as informações pessoais, informar os indivíduos sobre o processamento de seus dados e notificar as autoridades de proteção de dados em caso de violações de segurança.

2.4 Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados (LGPD) brasileira foi sancionada em 2018 e entrou em vigor em agosto de 2020. Seu objetivo é proteger os direitos fundamentais de privacidade e liberdade de informação dos titulares de dados pessoais (Art. 1º) e garantir que esses dados sejam tratados de maneira segura e responsável (Art. 5º). A lei se aplica a todas as empresas, organizações e instituições que realizem tratamento de dados pessoais no Brasil, independentemente de seu porte ou ramo de atividade (Art. 2º).

De acordo com a LGPD, dados pessoais são informações relacionadas a pessoas físicas identificadas ou identificáveis (Art. 5º, I), como nome, endereço, data de nascimento, informações bancárias, entre outras (Art. 11). Os titulares dos dados têm o direito de controlar o tratamento de seus dados pessoais, incluindo a coleta, armazenamento, uso, compartilhamento e eliminação desses dados (Art. 8º e Art. 18).

Para proteger os dados pessoais, a LGPD exige que as empresas e organizações implementem medidas de segurança (Art. 31), como criptografia, controle de acesso, backup de dados e monitoramento de atividades. As empresas devem notificar os titulares de dados em caso de vazamento ou perda de dados (Art. 43) e obter o consentimento dos titulares antes de coletar, armazenar ou usar seus dados (Art. 7º e Art. 13).

A LGPD cria a figura do Encarregado de Proteção de Dados (Art. 45), responsável por garantir a conformidade da empresa com a lei e atuar como canal de comu-

nicação entre a empresa e os titulares de dados. A lei também estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD) (Art. 46), responsável por fiscalizar o cumprimento da lei e impor sanções em caso de descumprimento (Art. 52) (Brasil, 2018).

Sendo assim, a LGPD é uma lei importante para garantir a proteção dos dados pessoais dos cidadãos brasileiros e estabelecer regras claras para o tratamento de dados pessoais por parte das empresas e instituições. A lei visa proteger os direitos fundamentais de privacidade e liberdade de informação dos titulares de dados pessoais e deve ser cumprida rigorosamente para garantir a privacidade e segurança dos dados. A implementação da LGPD é uma medida necessária para que as empresas e organizações realizem o tratamento de dados pessoais de forma ética e responsável, evitando o uso indevido ou abusivo dessas informações. Além disso, a LGPD também pode trazer benefícios para as empresas que cumprem suas exigências, como a melhoria da reputação, a confiança dos clientes e o fortalecimento da proteção de dados em suas operações internas.

Portanto, é crucial que as empresas e organizações entendam a relevância da LGPD e ajam para aplicar as medidas necessárias a fim de assegurar a proteção dos dados pessoais dos titulares. Além disso, devem buscar a conformidade com a legislação vigente, evitando, dessa forma, possíveis sanções e danos.

2.5 Técnicas de Coleta de Dados Pessoais

A coleta de dados pessoais é uma prática cada vez mais frequente no mundo digital, especialmente em ambientes *online*, que têm se tornado cada vez mais presentes no cotidiano das pessoas. É importante destacar que muitas vezes essas informações são compartilhadas entre empresas e organizações, o que pode aumentar ainda mais a quantidade de dados que são coletados sobre um indivíduo. Por isso, é fundamental que as empresas sigam regulamentações e normas de privacidade, além de garantir transparência e consentimento claro do usuário em relação ao uso de seus dados pessoais.

Uma das técnicas mais comuns de coleta de dados pessoais é a utilização de formulários de registro em sites ou aplicativos. Esses formulários geralmente solicitam informações como nome, endereço de *e-mail*, data de nascimento, gênero e outros dados

pessoais que podem ser utilizados para identificar o usuário. Essas informações podem ser utilizadas para fins diversos, desde a personalização de experiências *online* até a realização de análises de mercado (TRIVEDI et al., 2017).

Outra técnica de coleta de dados pessoais bastante utilizada são os *cookies*. Os *cookies* são arquivos de texto que são armazenados no computador ou dispositivo móvel do usuário quando ele acessa um site ou aplicativo. Esses arquivos contêm informações sobre a navegação do usuário, incluindo suas preferências, histórico de navegação e outros dados que podem ser utilizados para melhorar a experiência do usuário ou fornecer anúncios personalizados (DIMITRAKAKIS et al., 2011).

É importante notar que, ao dar consentimento para o uso de *cookies* em um site, o usuário geralmente está permitindo que o site colete informações sobre suas interações com ele. No entanto, o consentimento para o uso de *cookies* não implica automaticamente no compartilhamento de dados com outras empresas. As práticas relacionadas ao compartilhamento de dados coletados por meio de *cookies* podem variar de acordo com as políticas de privacidade do site em questão.

Além disso, as informações de navegação e compras também podem ser utilizadas para coletar dados pessoais. Essas informações incluem o histórico de navegação do usuário, os produtos ou serviços que ele pesquisou ou comprou, o valor gasto em compras, entre outras informações. Esses dados podem ser utilizados para criar perfis de usuários e oferecer produtos ou serviços personalizados, além de serem utilizados para fins de análise de mercado (KOSINSKI et al., 2014).

Além das técnicas mencionadas anteriormente, cabe destacar a raspagem de dados como outra importante metodologia para a coleta de informações. Também conhecida como *web scraping*, a técnica consiste em coletar dados a partir da análise do código-fonte das páginas *web* e, em seguida, armazená-los em um formato estruturado e manipulável, como um banco de dados ou um arquivo CSV (ELRAGAL; KLISCHEWSKI, 2017).

Para realizar a raspagem de dados, é necessário o uso de um programa especializado, conhecido como *scraper*. Esse programa utiliza algoritmos para identificar e extrair os dados desejados das páginas *web*, seguindo padrões de HTML, XML ou outras linguagens de marcação (BERTINI; CALABRÓ, 2019). O processo de raspagem pode

ser feito de forma manual ou automatizada, dependendo da quantidade de dados a serem coletados e da complexidade das fontes de informação.

2.6 Considerações

Considerando as circunstâncias descritas, é notável que a proteção da privacidade tem se tornado cada vez mais desafiadora no atual contexto de coleta, processamento e compartilhamento massivo e contínuo de dados pessoais. A rápida evolução tecnológica, juntamente com o crescente volume de dados gerados diariamente, demanda uma atenção especial no que diz respeito à salvaguarda dos direitos individuais e à manutenção da confiança dos usuários.

O MCI, a LGPD no Brasil e o RGPD na UE são marcos legais que estabelecem diretrizes para a proteção da privacidade e dos dados pessoais. Essas legislações possuem em comum o objetivo de equilibrar a coleta e o uso de dados com a necessidade de garantir a privacidade e a segurança dos indivíduos.

As técnicas de coleta de dados pessoais mencionadas podem ser submetidas a restrições e requisitos definidos por essas legislações. Por exemplo, os formulários de registro devem ser transparentes em relação às informações coletadas, sendo necessário obter o consentimento explícito dos usuários e informá-los sobre a finalidade da coleta. Além disso, os dados coletados devem ser tratados de forma adequada, seguindo os princípios de minimização, finalidade específica e segurança.

No caso dos *cookies*, o RGPD estabelece a necessidade de consentimento prévio, informado e inequívoco para a sua utilização, exceto em casos estritamente necessários para o funcionamento do serviço. Isso implica que as páginas da Internet devem informar claramente sobre o uso de *cookies* e permitir que os usuários tenham controle sobre sua utilização.

Quanto ao *web scraping*, é necessário observar as limitações impostas pelas leis de proteção de dados. É importante respeitar os princípios de finalidade, minimização e proporcionalidade na coleta de dados, bem como garantir a anonimização adequada dos dados obtidos.

Portanto, é fundamental que as organizações que utilizam essas técnicas de co-

leta de dados pessoais estejam conscientes das obrigações legais que recaem sobre elas. É necessário implementar medidas de conformidade, como a revisão das políticas de privacidade, a adoção de mecanismos de consentimento apropriados e a implementação de técnicas para proteger os dados pessoais.

3 Trabalhos Relacionados

3.1 Froomkin, A. e Obar A.

O artigo de Froomkin e Obar (2016), explora as implicações éticas do uso de técnicas de *data scraping* para coletar dados pessoais em grande escala e destaca as preocupações de privacidade que surgem em relação a essas práticas. Os autores começam o artigo descrevendo o crescimento do uso de *Big Data* e a coleta de dados em massa nos últimos anos, especialmente no que diz respeito à análise de comportamento do usuário na internet e mídias sociais.

A pesquisa destaca que muitas empresas e organizações utilizam técnicas de *data scraping* para coletar dados pessoais na Internet sem o conhecimento ou consentimento dos usuários. Esses dados podem ser vendidos para terceiros ou usados para fins de publicidade e *marketing*. Além disso, os autores destacam que as informações pessoais coletadas por meio de *data scraping* podem ser usadas para discriminar e prejudicar determinados grupos de pessoas.

Os autores também discutem as implicações éticas da técnica em relação ao direito à privacidade dos usuários. Eles argumentam que, embora os usuários possam ter concordado com os termos e condições das empresas ao criar contas em mídias sociais, muitas vezes eles não estão cientes de que suas informações estão sendo coletadas e usadas dessa maneira. Os autores apontam que a coleta de dados sem o conhecimento ou consentimento dos usuários pode ser considerada uma violação do direito à privacidade, especialmente se esses dados contêm informações sensíveis, como orientação sexual, religião ou opinião política.

Para lidar com essas preocupações éticas, os autores sugerem que as empresas devem ser mais transparentes sobre suas práticas de coleta de dados e dar aos usuários mais controle sobre suas informações pessoais. Eles também recomendam que as leis de proteção de dados sejam atualizadas para refletir o crescimento do *Big Data* e o uso de técnicas de coleta de dados. Os autores argumentam que, embora o uso de *data scraping*

possa ter benefícios em termos de inovação e análise de dados, esses benefícios não devem ser alcançados à custa da privacidade e dos direitos dos usuários.

Em suma, a pesquisa destaca a necessidade de um debate ético sobre o uso de técnicas de raspagem de dados para coletar dados pessoais em grande escala. Os autores enfatizam que as empresas devem ser mais transparentes sobre suas práticas de coleta de dados e dar aos usuários mais controle sobre suas informações pessoais. Além disso, o trabalho recorre a necessidade de atualizações nas leis de proteção de dados para garantir que os direitos dos usuários sejam protegidos no contexto abordado.

3.2 Barreto, L. e Monteiro, T.

A pesquisa de Barreto e Monteiro (2021), tem como objetivo analisar a adequação do *data scraping* à Lei Geral de Proteção de Dados (LGPD) brasileira. Para tanto, as autoras exploram as principais questões relacionadas à coleta automatizada de dados pessoais na Internet.

No início do artigo, as autoras apresentam uma visão geral da técnica, destacando suas principais características e formas de utilização. Elas veem uma ampla gama de usos potenciais do *data scraping* em diferentes setores da sociedade. Acreditam que essa técnica pode ser usada para coletar informações sobre o comportamento do consumidor, as tendências do mercado, a opinião pública e a atividade política. Além disso, a técnica pode ser usada em pesquisas acadêmicas, incluindo análises de redes sociais e estudos de mídia social. É enfatizado que, embora esses usos possam ser benéficos, é importante garantir que a coleta e o uso dos dados sejam éticos e estejam em conformidade com as leis e regulamentos aplicáveis.

Uma das questões centrais do artigo é a necessidade de obtenção do consentimento do titular dos dados. As autoras argumentam que o consentimento deve ser obtido de forma clara e explícita, levando em consideração a finalidade específica para a qual os dados serão utilizados. Além disso, elas destacam a importância da transparência no processo de coleta de dados, tanto em relação à identidade do coletor quanto aos métodos utilizados.

Outro ponto relevante abordado no artigo é a responsabilidade dos agentes envol-

vidos no processo da coleta de dados. As autoras argumentam que todos os envolvidos, incluindo os controladores e os operadores de dados, devem seguir as normas da LGPD e garantir a segurança e privacidade dos dados coletados. Além disso, elas apresentam algumas recomendações para a adequação do *data scraping* à LGPD, como a necessidade de realizar uma análise de riscos e a adoção de medidas de segurança adequadas.

O trabalho traz uma abordagem sobre a adequação do *data scraping* à LGPD, destacando questões como o consentimento do titular dos dados, a transparência no processo de coleta e a responsabilidade dos agentes envolvidos. As recomendações apresentadas pelas autoras podem ser úteis para empresas e organizações que utilizam o *data scraping* como ferramenta de coleta de dados pessoais na internet.

3.3 Benevenuto, F., Haddadi, H. e Gummadi, K. P.

O artigo de Benevenuto, Haddadi e Gummadi (2015) foi motivado pela crescente popularidade do *data scraping* e pela necessidade de entender as implicações éticas e legais do uso dessa técnica. Eles destacam a falta de clareza em torno das leis e regulamentos que regem essa técnica de coleta de dados e enfatizam a necessidade de explorar as implicações éticas e legais dessa prática.

O objetivo do estudo foi analisar esse contexto, buscando avaliar os riscos para a privacidade e a segurança dos usuários. Além disso, também visa examinar as práticas de coleta e uso de dados, com o objetivo de garantir a conformidade com as leis e os regulamentos relevantes.

A pesquisa trata de um estudo de caso em que uma ferramenta de raspagem de dados foi utilizada para obter as opiniões dos usuários em relação à privacidade na Internet. Os dados foram coletados a partir de comentários públicos em artigos de notícias selecionados. Eles usaram uma abordagem de análise de conteúdo para identificar as principais preocupações dos usuários em relação à privacidade. Além disso, revisaram a literatura existente sobre o tema, bem como as leis e regulamentos relevantes.

Os autores destacaram a importância de abordar as implicações éticas e legais da coleta de dados na rede e defenderam a necessidade de práticas responsáveis na coleta e uso de dados. Foi observado que o *data scraping* pode representar riscos para a privacidade

e a segurança dos dados pessoais e que os regulamentos relevantes, como o RGPD da UE, devem ser seguidos.

Os resultados do estudo de caso sugerem que os usuários estão cada vez mais preocupados com a privacidade e que as empresas precisam considerar essas preocupações ao coletar e usar dados. O trabalho recomenda que as empresas implementem políticas de privacidade claras e transparentes e que obtenham o consentimento informado dos usuários antes de coletar seus dados.

3.4 Considerações

Os trabalhos citados oferecem uma visão aprofundada e abrangente sobre os diversos aspectos relacionados à coleta e uso de dados na era digital. Eles ressaltam a importância de considerar a ética e a privacidade dos usuários durante a realização do processo de *data scraping*, bem como a necessidade de conformidade com as regulamentações de proteção de dados, como a LGPD.

Essas pesquisas evidenciam a necessidade de estabelecer diretrizes claras e regulamentações rigorosas para assegurar a proteção dos dados pessoais e promover uma utilização ética das técnicas de coleta de dados. Além disso, enfatizam a relevância de realizar investigações no contexto do comércio ilícito na Internet, sempre dentro dos limites éticos e legais, e empregando tecnologias avançadas para identificar e combater atividades ilegítimas.

Por outras palavras, esses estudos oferecem diferentes perspectivas para a compreensão das questões éticas e legais envolvidas na coleta e uso de dados, contribuindo para um debate mais amplo sobre a importância da proteção da privacidade e da conduta ética no cenário digital atual.

A tabela Tabela 3.1 realiza uma comparação entre os pontos que se destacam entre eles.

Tabela 3.1: Tabela comparativa entre os trabalhos estudados.

Trabalho	**Aspectos abordados**	**Metodologia**	**Resultados principais**
Froomkin e Obar (2016)	Ética da privacidade, impacto do *Big Data*	Análise teórica e revisão de literatura	Questões éticas e impactos do Big Data
Barreto e Monteiro (2021)	Conformidade com a LGPD, análise crítica	Análise jurídica e estudo de casos	Avaliação da adequação à LGPD
Benevenuto, Haddadi e Gummadi (2015)	*Data Scraping*, comércio online ilícito	Coleta e análise de dados, experimentos	Identificação de atividades ilegais

Enquanto o trabalho de Froomkin e Obar (2016) tem uma abordagem mais geral, discutindo a ética e os impactos do *Big Data*, os de Barreto e Monteiro (2021) e Benevenuto, Haddadi e Gummadi (2015) focam em questões mais específicas, como a conformidade legal e a aplicação do *data scraping* no combate ao comércio ilícito.

Ao contrário dos trabalhos relacionados, esse trabalho se concentra especificamente na análise da privacidade nas redes sociais. Compreendendo os desafios únicos enfrentados nesse contexto, onde há um compartilhamento significativo de informações sensíveis por parte dos usuários.

Além de identificar e analisar esses desafios, esse trabalho busca aprofundar o entendimento sobre as práticas de consentimento informado, a transparência na coleta de dados e as opções de privacidade oferecidas pelas plataformas de redes sociais.

4 Estudo de Caso

Este capítulo tem como objetivo abordar temas relevantes relacionados ao uso de tecnologias digitais e suas implicações nas esferas da privacidade, segurança e ética. Por meio da análise de estudos de caso selecionados, busca-se compreender os desafios e impactos associados a essas questões em diferentes contextos.

Ao explorar os temas apresentados nos estudos de caso, é almejado aprofundar a compreensão dos potenciais impactos negativos decorrentes do uso inadequado de tecnologias digitais. Além disso, refletir sobre a importância de políticas, regulamentações e práticas éticas para garantir a proteção da privacidade, segurança e dos direitos dos usuários envolvidos. A análise desses casos contribuirá para uma visão mais abrangente e consciente acerca do uso responsável e ético da tecnologia em nossa sociedade contemporânea.

4.1 Raspagem de Dados

No contexto atual, o *marketing* digital desempenha um papel fundamental na estratégia de empresas e marcas que buscam alcançar seu público-alvo de maneira eficaz e direcionada. Com o advento das redes sociais e a crescente presença das pessoas na internet, as empresas têm à disposição um vasto campo de possibilidades para promover seus produtos e serviços (KIETZMANN et al., 2011).

Uma das principais vantagens do *marketing* digital é a capacidade de segmentação e personalização das campanhas publicitárias. Nesse sentido, a coleta de dados pessoais se torna uma peça-chave para o sucesso dessas estratégias (LI; BERNOFF, 2011). Ao obter informações sobre os usuários, como preferências, comportamentos de navegação, histórico de compras e interesses, as empresas podem criar anúncios altamente relevantes e personalizados, aumentando significativamente as chances de conversão e fidelização.

Essa personalização das propagandas é possível graças ao uso de algoritmos inteligentes que analisam e interpretam os dados coletados. Por meio dessas análises, é

possível identificar padrões de comportamento e afinidades, permitindo que as empresas segmentem suas campanhas e entreguem anúncios específicos para diferentes grupos de usuários. Esse nível de personalização não apenas aumenta a eficácia das campanhas, mas também proporciona uma experiência mais relevante e satisfatória para o usuário (SOLIS, 2012).

No entanto, é importante ressaltar que a coleta de dados pessoais para fins de *marketing* deve ser realizada com responsabilidade e transparência. Os usuários devem ter ciência de quais informações estão sendo coletadas e como serão utilizadas, e devem ter a opção de fornecer ou não o seu consentimento. Além disso, a proteção e a privacidade dos dados pessoais devem ser garantidas, de acordo com as regulamentações vigentes em cada país (União Europeia, 2016).

No trabalho intitulado "*Scraping* e Análise de Dados no Aperfeiçoamento do Processo Seletivo de Programadores", é apresentado um *software* capaz de automatizar a seleção de candidatos para vagas de emprego no LinkedIn. Esse *software* utiliza o *web scraping* para extrair informações relevantes dos perfis dos candidatos, como experiência profissional e histórico de empregos anteriores. Em seguida, algoritmos são aplicados para avaliar e classificar os candidatos de acordo com critérios pré-estabelecidos, auxiliando os recrutadores na tomada de decisão.

O desenvolvimento desse *software* representa um avanço na automação e otimização do processo de seleção de candidatos, trazendo benefícios tanto para as empresas quanto para os candidatos em busca de oportunidades de emprego. Contudo, é imprescindível considerar os aspectos éticos e legais relacionados à coleta e uso de dados pessoais, garantindo a proteção da privacidade dos candidatos ao longo de todo o processo.

Neste contexto, este trabalho explora uma situação hipotética com o objetivo de ilustrar um novo uso potencialmente preocupante do *software* de automação de seleção de candidatos. O mesmo programa desenvolvido com o propósito legítimo de aprimorar o processo seletivo também pode ser utilizado de forma ilegítima.

Supondo que uma instituição de ensino renomada ou uma plataforma de ensino a distância reconheça a necessidade de promover seus cursos e atrair potenciais alunos, investindo estrategicamente em atividades de *marketing*. Com o objetivo de alcançar um

público-alvo mais específico e aumentar suas vendas e taxas de conversão, a instituição ou plataforma decide utilizar dados coletados por meio do software de automação de seleção de candidatos.

Nessa situação, a utilização dos dados coletados pelo software de automação possibilita a criação de propagandas personalizadas, destacando os cursos mais relevantes e atraentes para cada perfil de usuário, maximizando o potencial de vendas e aprimorando as campanhas de *marketing* da instituição ou plataforma.

Estudos, como o de Chen e Chen (2017), destacam que o uso de dados em estratégias de *marketing* permite identificar interesses individuais e personalizar a comunicação com os consumidores, melhorando a eficiência das campanhas de *marketing* e aumentando a taxa de conversão.

4.2 Estratégia de *Marketing*

Nessa seção, é apresentado um exemplo real, evidenciando a relevância do tema da privacidade e coleta de dados nas redes sociais no contexto do *marketing* digital. O estudo de caso selecionado aborda a estratégia de *marketing* de uma grande empresa de telecomunicações, que utilizou a funcionalidade de audiência customizada da plataforma Meta (anteriormente conhecida como Facebook) com o objetivo de alcançar potenciais clientes que ainda não possuíam vínculo com a empresa. A análise desse caso é essencial para compreender como as organizações podem aproveitar essas ferramentas para direcionar suas campanhas de maneira mais eficaz, visando atingir seus objetivos comerciais.

No contexto de avaliação da eficácia do serviço, a empresa do setor de telecomunicações conduziu um experimento comparativo, no qual foram implementadas duas campanhas distintas. Em um dos grupos, a campanha foi direcionada utilizando a audiência customizada disponibilizada pela plataforma Meta, enquanto no outro grupo foi direcionada para a base de clientes existente da marca. Vale ressaltar que todos os demais aspectos da ação, como investimento, conteúdo criativo e plataformas utilizadas (como Facebook, Instagram e Audience Network), permaneceram idênticos, sendo a diferença principal a segmentação da audiência (META, s.d.).

Como resultado, a empresa de telecomunicações constatou que a utilização da

audiência customizada disponibilizada pela plataforma Meta proporcionou a expansão de sua base de usuários, aumentando o alcance de seus anúncios. Além disso, também resultou na redução de custos e no aumento da taxa de conversão de potenciais clientes para clientes propriamente ditos. Os resultados obtidos foram tão positivos que a marca já planeja aplicar essa solução em outros produtos e realizar testes adicionais, comparando-a com outros públicos. A Figura 4.1 ilustra os resultados da campanha, sendo que a audiência customizada da Meta atingiu um alcance quatro vezes maior, com um custo 39% mais rentável e uma taxa de conversão cinco vezes superior.

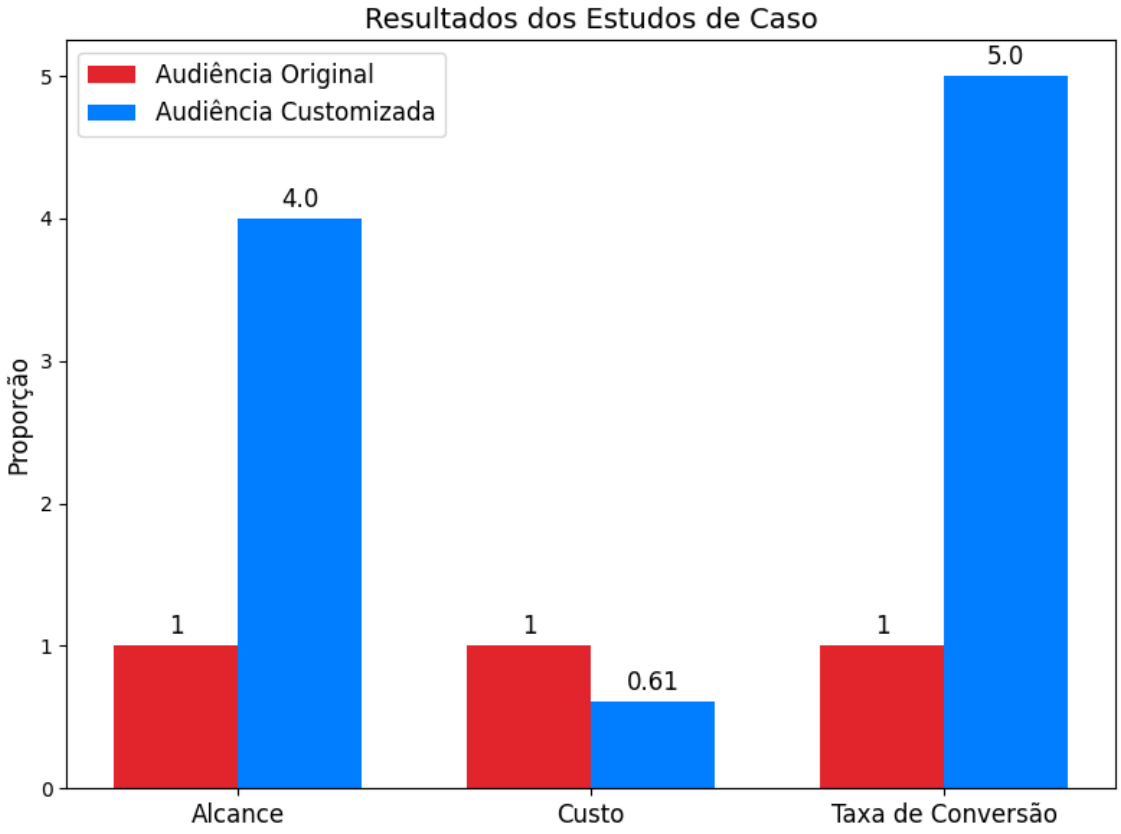

Figura 4.1: Comparação dos Resultados dos Estudos de Caso: Audiência Customizada vs. Audiência Original. Elaborado pelo autor.

Sendo assim, o direcionamento de propagandas com base em informações sensíveis, pode resultar em uma manipulação dos usuários, influenciando suas escolhas e decisões. Essa abordagem de propaganda personalizada, embora possa parecer vantajosa para as empresas e instituições que buscam maximizar o impacto de suas campanhas de *marketing*, levanta preocupações significativas em relação à privacidade e ética.

A coleta e o uso de dados pessoais para segmentar anúncios podem criar uma sensação de invasão de privacidade e gerar desconfiança por parte dos usuários. Além disso, a manipulação das informações e o direcionamento personalizado podem distorcer a percepção dos indivíduos, limitando sua exposição a diferentes perspectivas e reforçando bolhas de filtro, onde são expostos apenas a conteúdos alinhados com suas preferências pré-existentes. Essa manipulação sutil pode minar a autonomia e a liberdade de escolha dos usuários, prejudicando a formação de uma sociedade informada e plural. Portanto, é fundamental buscar um equilíbrio entre as estratégias de marketing personalizado e a proteção dos direitos individuais, garantindo que a coleta e o uso de dados ocorram de forma transparente e consentida. (TUFEKCI, 2014).

É fundamental que as empresas ajam em conformidade com os direitos estabelecidos pela LGPD. A lei estabelece, por exemplo, que a coleta e o processamento de dados pessoais devem ser realizados com o consentimento explícito do titular, conforme previsto no Artigo 7º da LGPD. Além disso, o Artigo 9º determina que o titular tem o direito de ser informado sobre como seus dados serão utilizados, assegurando a transparência no tratamento das informações. A LGPD também garante ao titular o direito de revogar o consentimento a qualquer momento, conforme estabelecido no Artigo 18º. Dessa forma, o *marketing* digital personalizado deve ser realizado dentro dos limites e princípios da LGPD, garantindo a proteção dos direitos dos usuários e o cumprimento das obrigações legais (Brasil, 2018).

4.3 Compartilhamento Excessivo

A divulgação excessiva de informações pessoais nas redes sociais pode ter um impacto negativo significativo, como evidenciado por um estudo de caso conduzido pelo Telegraph UK (BLOXHAM, 2011). Essa pesquisa entrevistou criminosos condenados por roubo, fornecendo informações sobre como eles utilizam plataformas como Twitter, Facebook e Google Street View para planejar atividades criminosas, especialmente roubos residenciais.

De acordo com o estudo, quatro em cada cinco criminosos afirmaram que usam ativamente as redes sociais para obter informações sobre possíveis alvos. Os usuários

compartilham detalhes sobre compras de alto valor, como televisores, além de informações sobre datas e horários em que estarão ausentes, o que pode ser acessado por ladrões. Além disso, o Google Street View permite que os criminosos visualizem fotografias de residências individuais, avaliando a segurança e a facilidade de acesso, em busca de alarmes e entradas laterais.

O estudo destaca que o mesmo número de criminosos afirmou que a presença de um simples sistema de alarme residencial dissuadiria-os de escolher uma propriedade como alvo. Isso ressalta a eficácia de medidas básicas de segurança na prevenção de crimes. A pesquisa também revelou que os criminosos roubam, em média, R$1407,43 de uma residência em uma única visita, destacando as consequências financeiras significativas decorrentes da falta de consciência sobre privacidade e segurança nas redes sociais.

Um dos criminosos entrevistados, Richard Taylor, afirmou que vivemos na era dos crimes digitais, onde as pessoas aproveitam as redes sociais para acessar informações sobre potenciais vítimas. Ele destacou como alguns usuários compartilham informações pessoais sensíveis, como divulgação de planos de férias, convidando os criminosos para suas próprias casas, sem considerar as consequências de suas ações.

Jonathan Lim, especialista da Friedland, empresa de segurança responsável pela pesquisa, enfatizou a importância de medidas simples, recomendando que as pessoas estejam atentas ao gerenciamento de sua privacidade nas redes sociais. Isso inclui revisar regularmente as configurações de privacidade e segurança das contas, garantindo que apenas as pessoas de confiança tenham acesso às informações pessoais compartilhadas.

O estudo de caso destaca a necessidade de conscientização sobre os riscos associados ao compartilhamento excessivo de informações pessoais nas redes sociais. Ele ilustra como os criminosos exploram essas plataformas para obter vantagem, ressaltando a importância da ética na coleta de dados pessoais e das medidas de segurança para proteger a privacidade e prevenir roubos residenciais.

5 Dicussão

5.1 Análise dos Resultados

Nesta seção, é feita a análise dos resultados obtidos nos casos abordados em nosso estudo de casos sobre privacidade e coleta de dados pessoais nas redes sociais. O primeiro caso, uma simulação envolvendo uma instituição de ensino que utiliza um *software* específico para coletar dados de forma ilegítima e criar propagandas direcionadas, destaca os possíveis riscos e implicações negativas para a privacidade dos usuários. O caso em si tem o propósito de ilustrar uma preocupação crescente em relação à coleta inadequada de dados pessoais.

Por outro lado, o segundo caso, uma situação real envolvendo uma empresa de telecomunicações e o uso da funcionalidade de audiência customizada da plataforma Meta, revelou resultados significativos. A audiência customizada da Meta permitiu à empresa alcançar potenciais clientes sem vínculo prévio com a empresa, resultando em um maior alcance, redução de custos e uma taxa de conversão superior. Esses resultados evidenciam o potencial dessas técnicas de coleta de dados personalizados para melhorar a eficácia das campanhas de *marketing* e impulsionar os resultados comerciais.

No entanto, é importante ressaltar que, embora os resultados tenham sido positivos, a utilização dessas práticas deve ser realizada com cuidado e em conformidade com a legislação de proteção de dados pessoais. Os princípios de privacidade, consentimento informado e transparência devem ser respeitados para garantir a confiança dos usuários e evitar abusos na coleta e uso de seus dados pessoais.

Já o terceiro caso de estudo foca no compartilhamento excessivo de informações por parte dos usuários e em como essas informações são usadas por criminosos. O estudo levanta questões sobre a necessidade de uma legislação que pressione as plataformas a assumirem a responsabilidade de proteger os dados pessoais dos usuários, bem como a importância da conscientização dos usuários para evitar a divulgação de informações sensíveis.

Os casos mencionados ressaltam a importância de equilibrar as estratégias de *marketing* e publicidade com a proteção da privacidade dos usuários. Para isso, é fundamental que as empresas sejam impostas por legislações e regulamentações, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, a adotarem práticas éticas e estarem em conformidade.

Diversas medidas são essenciais para proteger a privacidade dos usuários. Isso inclui oferecer opções claras de consentimento, implementar práticas de privacidade por padrão, minimizar a coleta de dados e garantir o armazenamento seguro dessas informações. As Legislações devem impor às empresas a obrigação de investir em educação e conscientização sobre a proteção de dados, fornecendo orientações claras aos usuários sobre como proteger seus dados e evitar a divulgação de informações sensíveis.

Adicionalmente, é importante que as empresas estabeleçam políticas de retenção de dados, determinando por quanto tempo essas informações serão armazenadas, e disponibilizem mecanismos para que os usuários possam excluir seus dados quando desejarem. A transparência é um elemento-chave, com as empresas fornecendo informações claras e acessíveis sobre a coleta, uso e compartilhamento de dados, além de explicar os direitos dos usuários em relação a essas informações.

5.2 Impactos na Privacidade

Nesta seção, vamos explorar os impactos na privacidade decorrentes das práticas de coleta de dados pessoais nas redes sociais, levando em consideração os casos apresentados nesta pesquisa.

No caso do vazamento de dados do Facebook ocorrido em março de 2018, envolvendo a empresa Cambridge Analytica, milhões de pessoas tiveram suas informações pessoais obtidas sem consentimento, incluindo dados pessoais, interesses, lista de amigos e informações de perfil. Esses dados foram utilizados para criar perfis psicológicos dos usuários, com o objetivo de influenciar suas opiniões políticas e comportamentos de voto.

No estudo de caso da parceria entre a plataforma Meta e uma grande empresa de telecomunicações, embora o consentimento do usuário seja obtido por meio do formulário de políticas de privacidade das redes sociais envolvidas, ainda assim não fica claro para

o usuário quais dados estão sendo coletados e qual é a finalidade dessa coleta. Empresas têm utilizado estratégias de *marketing* baseadas em dados coletados nas redes sociais para alcançar um público direcionado, mas essa prática pode resultar em uma invasão da privacidade dos usuários.

Além disso, é importante considerar o compartilhamento excessivo do usuário nas redes sociais. Muitos usuários compartilham informações pessoais de forma demasiada e sem considerar os riscos envolvidos, expondo-se a violações de privacidade, manipulação e uso indevido de seus dados. É necessário reforçar a responsabilidade dos usuários na proteção de seus dados sensíveis, enfatizando a cautela ao compartilhar informações pessoais com desconhecidos ou em plataformas não confiáveis.

As legislações vigentes, como a LGPD e o MCI, desempenham um papel fundamental na proteção da privacidade dos usuários e na regulamentação do uso de dados pessoais. Essas legislações estabelecem diretrizes importantes, como a necessidade de consentimento informado e a garantia dos direitos dos titulares dos dados. No entanto, é necessário buscar constantemente melhorias nessas regulamentações para lidar de forma mais efetiva com os desafios atuais relacionados à privacidade e coleta de dados.

Uma possível melhoria seria a exigência de que as políticas de privacidade sejam escritas de forma clara, acessível e compreensível, evitando linguagem técnica excessiva que possa confundir os usuários. Além disso, seria benéfico tornar obrigatória a divulgação detalhada das informações coletadas e a finalidade específica de sua utilização, fornecendo aos usuários uma visão clara e transparente sobre como seus dados serão tratados.

O RGPD também desempenha um papel relevante nesse contexto. Ele estabelece um padrão elevado de proteção de dados pessoais e influencia as práticas em todo o mundo. Um desses padrões que poderia ser incorporado na LGPD é o princípio do *Privacy by Design* (Privacidade desde a Concepção), que preconiza a incorporação de medidas de privacidade desde o início do desenvolvimento de sistemas e serviços. Essa abordagem proativa à proteção de dados desde a concepção dos produtos e serviços pode ser adotada na LGPD para garantir uma maior consideração pela privacidade dos usuários desde o início do processo.

5.3 Conformidade com a Legislação

Considerando os impactos na privacidade discutidos anteriormente e a necessidade de proteger os direitos dos usuários, é essencial analisar as regulamentações e leis que buscam garantir a segurança e o uso adequado das informações pessoais.

O consentimento é um aspecto de extrema importância quando se trata da coleta e do uso de dados pessoais nas redes sociais. No estudo de caso apresentado, onde uma empresa de telecomunicações utilizou a funcionalidade de audiência customizada da plataforma Meta para expandir sua base de usuários, o consentimento do usuário se torna fundamental. A LGPD destaca a importância do consentimento livre, informado e inequívoco do titular dos dados para o tratamento de suas informações pessoais.

Nesse contexto, é importante que a empresa obtenha o consentimento adequado dos usuários cujos dados serão utilizados nessa estratégia de *marketing*. Os usuários devem ser claramente informados sobre quais dados estão sendo coletados, como serão utilizados e com quem serão compartilhados. Além disso, eles devem ter a liberdade de consentir ou negar o uso de seus dados, tendo a opção de revogar o consentimento a qualquer momento.

Ao respeitar o direito ao consentimento, a empresa não apenas está em conformidade com a legislação de proteção de dados, como também demonstra respeito pela privacidade e autonomia dos usuários. Isso contribui para a construção de uma relação de confiança entre a empresa e seus clientes, resultando em benefícios mútuos, como a expansão da base de usuários, a redução de custos e o aumento da taxa de conversão.

Outro aspecto relevante é a finalidade da coleta de dados. A LGPD estabelece que os dados pessoais só podem ser coletados e tratados para finalidades legítimas, específicas e informadas aos usuários. Nas redes sociais, isso significa que os controladores devem informar claramente os propósitos para os quais os dados estão sendo coletados, como a personalização de conteúdo, a segmentação de anúncios ou a melhoria da experiência do usuário. A coleta e o uso de dados além dessas finalidades requerem um novo consentimento ou podem ser considerados inadequados sob a ótica da LGPD.

A responsabilidade dos controladores e operadores é outro aspecto-chave da LGPD. No contexto das redes sociais e do estudo de caso em questão, a empresa de telecomunicações atua como o controlador, sendo responsável por definir as finalidades da coleta de

dados e garantir a conformidade com a lei. Por sua vez, a plataforma Meta desempenha o papel de operadora, processando os dados em nome do controlador.

Tanto os controladores quanto os operadores têm a obrigação de adotar medidas técnicas e organizacionais adequadas para proteger os dados pessoais, evitando acessos não autorizados, perdas, alterações ou vazamentos. Além disso, ambos devem estar preparados para lidar com solicitações de acesso, retificação, exclusão e portabilidade de dados dos usuários, conforme estabelecido pela LGPD.

Em julho de 2023, o Brasil testemunhou o primeiro caso de sanção pela LGPD. A empresa de telecomunicações Telekall Inforservice tornou-se objeto de um Processo Administrativo Sancionador instaurado pela Autoridade Nacional de Proteção de Dados (ANPD), após indícios de infração à LGPD terem sido identificados. O desenrolar do processo resultou na aplicação de sanções à empresa, incluindo uma advertência e uma multa totalizando R$ 14.400,00, em virtude da violação do Artigo 7º da LGPD.

O Artigo 7º da LGPD estabelece as bases legais para o tratamento de dados pessoais, definindo princípios e condições que norteiam a coleta, uso e compartilhamento dessas informações. Sua violação pode resultar em penalidades significativas para as empresas, como o caso da Telekall Inforservice.

A empresa foi notificada para cumprir as sanções e apresentar recurso, caso desejasse, dentro do prazo estabelecido pela legislação. Esse caso evidencia a importância da conformidade com as regulamentações de proteção de dados e reforça a necessidade de as empresas garantirem o consentimento adequado dos usuários e cumprirem as finalidades legítimas e informadas para a coleta e tratamento de dados pessoais nas redes sociais. Ações como essa são fundamentais para estabelecer um ambiente seguro e confiável nas redes sociais, protegendo os direitos dos usuários e preservando sua privacidade.

A conformidade com a legislação de proteção de dados é necessária para estabelecer um ambiente seguro e confiável nas redes sociais. A adoção de práticas transparentes, o respeito aos direitos dos usuários e a implementação de mecanismos eficazes de proteção de dados são fundamentais para garantir a conformidade legal e a preservação da privacidade dos usuários.

5.4 Medidas de Proteção e Conscientização

A proteção da privacidade e a conscientização dos usuários são aspectos fundamentais no contexto da coleta de dados pessoais nas redes sociais. Para garantir a segurança e preservar a privacidade dos usuários, é importante adotar medidas de proteção e promover uma maior conscientização sobre a importância da privacidade *online*. Nesse sentido, é válido ressaltar iniciativas relevantes.

Em casos como o da Friedland, em que há a divulgação excessiva de informações pessoais, medidas de proteção e conscientização desempenham um papel crucial na mitigação de riscos. Ao implementar medidas técnicas de segurança, como criptografia e autenticação em dois fatores, as plataformas podem proteger os dados dos usuários contra acesso não autorizado.

É crucial implementar uma abordagem abrangente de conscientização que atinja todos os usuários, por meio de campanhas educativas e informativas em diferentes canais de comunicação, como mídias sociais, anúncios online, palestras e materiais informativos em escolas e instituições. O foco dessas iniciativas deve ser destacar os perigos do compartilhamento irresponsável de informações sensíveis, como datas de ausência da residência, aquisições, endereços ou informações médicas e financeiras, evidenciando os riscos de crimes como furtos, roubo de identidade e ataques de engenharia social. Combinar essas medidas de conscientização com a implementação de estratégias de proteção de dados é fundamental para preservar a privacidade e promover a segurança dos usuários nas redes sociais.

Para ampliar a conscientização, é possível promover campanhas educativas que informem os usuários sobre as práticas de coleta de dados, os potenciais impactos na privacidade e as medidas de proteção disponíveis. Essas campanhas devem ser acompanhadas pela disponibilização de materiais educativos, tutoriais e orientações claras sobre as configurações de privacidade nas plataformas. Dessa forma, os usuários serão capacitados a compreender e controlar melhor o compartilhamento de suas informações pessoais.

Além disso, as redes sociais devem ser transparentes em relação às suas práticas de coleta, uso e compartilhamento de dados pessoais. Isso implica na divulgação clara e acessível das políticas de privacidade, termos de uso e informações sobre as medidas de

segurança adotadas para proteger os dados dos usuários. As plataformas também devem assumir a responsabilidade pela proteção dos dados pessoais coletados e estabelecer mecanismos efetivos para lidar com reclamações, solicitações de acesso, retificação e exclusão de dados.

Outro aspecto crucial é a obtenção do consentimento informado dos usuários antes da coleta e do uso de seus dados pessoais. As redes sociais devem garantir que os usuários sejam adequadamente informados sobre quais dados estão sendo coletados, como serão utilizados e se serão compartilhados com terceiros. É essencial que o consentimento seja livre, específico, inequívoco e revogável a qualquer momento. Para facilitar a compreensão das políticas de privacidade, as plataformas devem oferecer mecanismos claros para que os usuários concedam ou revoguem seu consentimento.

É esperado que as regulamentações de proteção de dados, como a LGPD, sejam cada vez mais fortalecidas e rigorosamente aplicadas. A garantia de que a ANPD esteja plenamente operacional e com recursos adequados para fiscalizar e aplicar as regras da LGPD é essencial para assegurar o cumprimento das normas. Para tanto, é importante que a ANPD tenha autonomia e poder de atuação para supervisionar as práticas de coleta, uso e compartilhamento de dados pelas empresas e garantir que as penalidades sejam aplicadas de forma mais severa para aquelas que não estiverem em conformidade com as regulamentações. Além disso, é fundamental que a ANPD conduza investigações aprofundadas em casos de violação de dados, visando a proteção dos direitos dos usuários e a responsabilização das empresas que não respeitarem a privacidade e a proteção de dados pessoais.

5.5 Anonimização

Com base nas vulnerabilidades de privacidade identificadas nos estudos de caso, uma possível alternativa para remediar e fortalecer a proteção da privacidade dos usuários em redes sociais é considerar a criação de redes sociais anônimas. Essas redes permitem aos usuários compartilhar informações e interagir sem revelar sua identidade real. No entanto, é importante analisar cuidadosamente os prós e contras dessa abordagem.

As redes sociais anônimas oferecem privacidade aprimorada, pois tornam mais

difícil a associação direta de dados pessoais a indivíduos específicos, fornecendo uma camada adicional de proteção da privacidade. Além disso, a anonimidade pode encorajar a liberdade de expressão, permitindo que os usuários compartilhem opiniões sinceras e abertas sem medo de repercussões pessoais. Também podem fornecer um ambiente mais seguro para usuários que enfrentam perseguição ou assédio, protegendo sua identidade.

No entanto, as redes sociais anônimas apresentam desafios significativos. A anonimidade pode incentivar comportamentos abusivos, como disseminação de conteúdo ofensivo, discurso de ódio e *cyberbullying*, tornando a responsabilização por esses comportamentos mais difícil sem a identificação dos usuários. Além disso, a falta de identificação real dos usuários pode gerar desconfiança e dificultar a verificação da autenticidade das informações compartilhadas, comprometendo a credibilidade das interações e conteúdos na rede social. Há também o risco de que essas redes sejam utilizadas para atividades ilegais, como disseminação de conteúdo ilegal, fraudes e planejamento de crimes, o que pode trazer desafios para a aplicação da lei e questões éticas sobre a responsabilidade dos provedores de serviços.

Para mitigar essas vulnerabilidades de privacidade, uma possível abordagem seria o desenvolvimento de redes sociais anônimas com mecanismos de segurança e controle adequados. Isso pode envolver o uso de técnicas avançadas de anonimização, como criptografia de ponta a ponta, pseudônimos e minimização da coleta de dados pessoais. Além disso, é necessário implementar mecanismos de moderação eficazes para combater o abuso e a má conduta, sem comprometer a privacidade dos usuários.

No entanto, é essencial realizar pesquisas adicionais para avaliar a viabilidade e os impactos dessas soluções, bem como considerar as implicações legais e éticas envolvidas.

5.6 Conclusão

Neste capítulo, foram discutidos os resultados do estudo de caso sobre privacidade e coleta de dados pessoais nas redes sociais. Um dos principais desafios identificados está relacionado à falta de transparência por parte das redes sociais em relação às suas práticas de coleta e uso de dados. Muitas vezes, os usuários não têm pleno conhecimento sobre quais informações estão sendo coletadas, como estão sendo utilizadas e com quem estão

sendo compartilhadas. Essa falta de clareza dificulta o exercício do controle sobre os próprios dados e mina a confiança dos usuários nas plataformas.

Foi observado que as práticas atuais apresentam desafios significativos para a proteção da privacidade dos usuários, exigindo medidas mais eficazes e uma conscientização maior por parte dos usuários e das próprias redes sociais. Os usuários devem estar cientes dos riscos associados à divulgação de suas informações pessoais e tomar precauções ao compartilhá-las nas redes sociais. É importante promover a conscientização sobre os direitos à privacidade e fornecer orientações claras sobre como proteger suas informações pessoais.

6 Considerações Finais

Ao longo deste trabalho, o objetivo principal foi analisar os desafios inerentes ao direito à privacidade no contexto das redes sociais, enfatizando a eficácia na proteção da privacidade dos usuários e os princípios de liberdade e autonomia no ambiente digital. Nesse sentido, houve um progresso na reflexão desses temas, trazendo à tona preocupações e desafios pertinentes.

Ao explorar as legislações, e investigar técnicas de coleta de dados pessoais, foi possível obter uma compreensão mais aprofundada da complexidade envolvida na preservação da privacidade no contexto das redes sociais. Durante esse processo, foram identificados questionamentos relacionados à proteção dos dados pessoais, assim como à necessidade de encontrar um equilíbrio entre a privacidade dos usuários e as demandas tecnológicas em constante evolução.

Ao trazer esses dilemas à discussão, o presente estudo contribuiu para ampliar a conscientização sobre os direitos individuais no ambiente digital, além de incentivar uma reflexão crítica sobre a eficácia das garantias de privacidade estabelecidas pelas regulamentações vigentes. Em particular, enfatizou-se a importância de ponderar a liberdade e a autonomia dos usuários frente aos desafios emergentes no mundo digital.

No entanto, é fundamental reconhecer que o campo da privacidade digital é complexo e está em constante transformação. Apesar do avanço, nas análises desses temas ainda existem áreas que demandam aprofundamento do conhecimento e enfrentamento de questões emergentes. Esse cenário requer uma constante atualização dos conhecimentos e uma adaptação às novas tecnologias, práticas e tendências que afetam a privacidade dos usuários. Além disso, a legislação relacionada à proteção de dados também está em constante mudança, com a introdução de novas regulamentações e a interpretação de casos jurisprudenciais, o que pode tornar desafiador acompanhar as últimas diretrizes e implicações legais.

A privacidade, como um conceito multifacetado, abrange diferentes dimensões, como a proteção de dados pessoais, a privacidade de comunicação e a privacidade de

comportamento. Cada dimensão apresenta suas próprias complexidades e questões éticas, exigindo uma abordagem abrangente e multidisciplinar para compreender plenamente as implicações da privacidade nas redes sociais.

Diante das dificuldades identificadas e com o objetivo de aprofundar o conhecimento e abordar as lacunas existentes, é importante explorar oportunidades de trabalhos futuros que possam contribuir para garantir a privacidade dos usuários e a aplicação efetiva das leis de proteção de dados. Nesse sentido, além das sugestões anteriormente apresentadas, é necessário considerar abordagens técnicas que fortaleçam a segurança e a privacidade das informações pessoais.

Uma área promissora para pesquisas futuras é o desenvolvimento e aprimoramento de técnicas de criptografia e segurança de dados. Estudos podem ser conduzidos para investigar novas metodologias de criptografia, permitindo um compartilhamento seguro de informações, preservando a privacidade dos usuários.

Além disso, é fundamental desenvolver protocolos de segurança robustos para redes sociais, que garantam a confidencialidade e a integridade dos dados pessoais. A avaliação da eficácia das leis existentes e a proposição de soluções técnicas para possíveis desafios também são linhas de pesquisa relevantes. Isso inclui a análise de casos reais de violação de privacidade, a identificação de brechas na implementação das leis de proteção de dados e o desenvolvimento de soluções tecnológicas capazes de prevenir e mitigar tais violações.

A colaboração entre pesquisadores, profissionais da área jurídica e empresas de tecnologia desempenha um papel fundamental nesse contexto. Essa colaboração pode incentivar o desenvolvimento de políticas e regulamentações mais eficazes e adaptáveis às rápidas mudanças no cenário digital, garantindo a proteção adequada da privacidade dos usuários.

Portanto, a combinação de estudos sobre a implementação das legislações existentes, as percepções dos usuários e as abordagens técnicas de segurança, como criptografia e anonimização, proporciona uma base sólida para avançar na proteção da privacidade nas redes sociais e no ambiente digital como um todo. Essas pesquisas futuras são essenciais para enfrentar os desafios emergentes e garantir que as leis e regulamentações existen-

tes sejam efetivas na prática, fornecendo aos usuários um ambiente digital mais seguro e preservando seus direitos de privacidade.

6.1 Trabalhos Futuros

O tema deste trabalho continua em constante evolução, impulsionado pelos avanços tecnológicos e pelas demandas crescentes dos usuários por maior controle sobre suas informações pessoais. Nesta seção, são discutidas algumas tendências e futuras considerações relevantes no contexto dessa temática.

Novas leis e normas podem surgir para abordar lacunas ou questões específicas relacionadas à privacidade e coleta de dados nas redes sociais. Portanto, é fundamental que as empresas e plataformas sejam obrigadas por lei a manter-se atualizadas e em conformidade com as regulamentações vigentes, bem como a acompanhar as mudanças legislativas.

Além disso, com o aumento da conscientização dos usuários sobre a importância da privacidade de seus dados, espera-se uma maior demanda por transparência e consentimento informado. As redes sociais devem aprimorar suas políticas de privacidade e termos de uso, tornando-os mais compreensíveis e transparentes para os usuários. Além disso, é provável que os usuários exijam opções mais claras e acessíveis para gerenciar suas configurações de privacidade e conceder consentimento para a coleta e uso de seus dados.

Com o objetivo de atender às preocupações dos usuários e melhorar a proteção de dados nas redes sociais, espera-se o desenvolvimento de tecnologias específicas de privacidade. Isso pode incluir soluções como ferramentas avançadas de criptografia, anonimização de dados, controle granular de permissões e sistemas de monitoramento e detecção de violações de privacidade. Essas tecnologias visam proporcionar um ambiente mais seguro e confiável para os usuários compartilharem suas informações pessoais.

Outra sugestão importante para o avanço da proteção de dados é o desenvolvimento de uma métrica padronizada para avaliar a segurança dos dados em redes sociais e plataformas digitais. Essa métrica poderia levar em consideração fatores como a robustez das medidas de segurança implementadas, a capacidade de detecção e resposta a violações de dados, a transparência das políticas de privacidade e a facilidade de gerenciamento das

configurações de privacidade pelos usuários. A criação de uma métrica eficaz permitiria ao Estado avaliar de forma mais objetiva e consistente o quão seguro estão os dados dos usuários e, assim, tomar medidas proativas para garantir a proteção adequada dos dados pessoais.

É importante destacar que a proteção da privacidade e a coleta responsável de dados pessoais exigem uma abordagem colaborativa entre os setores público e privado. Governos, empresas, sociedade civil e especialistas em privacidade devem trabalhar em conjunto para desenvolver padrões, diretrizes e melhores práticas que garantam a proteção dos direitos dos usuários e promovam a responsabilidade na coleta e uso de dados pessoais.

Bibliografia

ACAR, Y.; YILDIRIM, O. Social media data collection: An overview of ethical issues. *Journal of Business Research*, v. 98, p. 365–376, 2019.

ACQUISTI, A. Privacy in the age of augmented reality. *Communications of the ACM*, v. 58, n. 9, p. 90–98, 2015.

BARRETO, L.; MONTEIRO, T. Adequação do data scraping à lgpd: análise crítica. *Revista de Direito, Tecnologia e Inovação*, v. 10, p. 83–197, 2021.

BEDENDO et al. *LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DO COMÉRCIO ELETRÔNICO (LEI N. 13.709/2018)*. [S.l.]: Univel, 2019.

BENEVENUTO, F.; HADDADI, H.; GUMMADI, K. P. A systematic study of web crawling for illicit online trade. In: *24th International Conference on World Wide Web - WWW '15*. [S.l.: s.n.], 2015. p. 121–132.

BERTINI, M.; CALABRÓ, G. An exploratory study of web scraping tools in software engineering. In: . [S.l.: s.n.], 2019. v. 4, p. 465–475.

BLOXHAM, A. Most burglars using facebook and twitter to target victims, survey suggests. *The Telegraph*, 2011. Acesso em: 01/07/2023. Disponível em: ⟨https://www.telegraph.co.uk/technology/news/8789538/Most-burglars-using-Facebook-and-Twitter-to-target-victims-survey-suggests.html⟩.

Brasil. Marco civil da internet. 2014. Disponível em: ⟨https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm⟩.

Brasil. Lei geral de proteção de dados pessoais. 2018. Disponível em: ⟨https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm⟩.

CADWALLADR, C. I created steve bannon's psychological warfare tool': Meet the data war whistleblower. *The Guardian*, v. 17, 2018.

CADWALLADR, C.; GRAHAM-HARRISON, E. I created steve bannon's psychological warfare tool': Meet the data war whistleblower. *The Guardian*, v. 17, 2018. Disponível em: ⟨https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election⟩.

CHEN, C.; CHEN, F. Big data marketing: From data to knowledge. *Journal of Business Research*, v. 70, p. 253–256, 2017.

CORDERY, C. J.; SIM, D. *Dominant stakeholders, activity and accountability discharge in the CSO sector*. [S.l.: s.n.], 2018. v. 34. 77-96 p.

DIMITRAKAKIS, C. et al. *Privacy and Security Issues in Data Mining and Machine Learning: International ECML/PKDD Workshop, PSDML 2010, Barcelona, Spain, September 24, 2010. Revised Selected Papers*. [S.l.: s.n.], 2011. v. 6549.

ELRAGAL, A.; KLISCHEWSKI, R. Theory-driven or process-driven prediction? epistemological challenges of big data analytics. *Journal of Big Data*, v. 4, p. 1–20, 2017.

FERREIRA, A. Imprensa e redes sociais: o papel das mídias sociais na distribuição de conteúdo jornalístico. *Revista Brasileira de Mídia e Comunicação*, v. 3, n. 2, p. 1–15, 2017.

FINKELSTEIN, M. E.; FINKELSTEIN, C. Privacidade e lei geral de proteção de dados pessoais. *Revista de Direito Brasileira*, v. 23, n. 9, p. 284–301, 2020.

FROOMKIN, A.; OBAR, A. Big data, data scraping, and the ethics of privacy. *Big Data and Society*, v. 3, p. 1–13, 2016.

FUGAZZA, G. Q.; SALDANHA, G. S. Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais. *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*, v. 22, n. 50, p. 91–101, 2017.

FURNELL, S. M.; WARREN, P. Cyber crime: A review of the evidence. *Journal of Financial Crime*, v. 16, n. 4, p. 946–962, 2016.

GARCIA, D.; CALLE, E. Big data and social media: Current research and future opportunities. *Journal of Business Research*, v. 69, n. 12, 2016.

GREWAL, D.; KANNAN, P. K. Data collection and privacy in the digital age: Issues and implications. *Journal of Marketing*, v. 81, n. 2, p. 131–148, 2017.

GUSTAFSSON, A.; JOHNSON, M. The dark side of data trading: A systematic literature review. *Journal of Business Ethics*, v. 156, n. 4, p. 811–832, 2019.

KIETZMANN, J. et al. Social media? get serious! understanding the functional building blocks of social media. *Business Horizons*, v. 3, p. 241–251, 2011.

KOSINSKI, M. et al. Manifestations of user personality in website choice and behaviour on online social networks. *Machine learning*, v. 95, p. 357–380, 2014.

KWOK, R.; WANG, X. Privacy risks of personal data trading: A review. *Journal of Business Research*, v. 97, p. 280–292, 2019.

LEMOS, R. O marco civil como símbolo do desejo por inovação no brasil. *São Paulo: Atlas*, p. 3–11, 2014.

LI, C.; BERNOFF, J. *Groundswell: Winning in a world transformed by social technologies*. [S.l.]: Harvard Business Press, 2011.

LYON, D. Surveillance, snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, v. 1, n. 1, 2014.

META. Claro brasil: Expandindo a audiência com assertividade na meta. s.d. Disponível em: ⟨https://www.facebook.com/business/success/claro-brasil⟩.

MOOR, J. H. Why we need better ethics for emerging technologies. *Ethics and information technology*, Springer, v. 7, n. 3, p. 111–119, 2005.

OLIVEIRA, R. L. d. O impacto da proteção de dados (rgpd) no retalho omnicanal. 2021.

PECK, P. Direito digital. rev., atual. e ampl. *São Paulo: Saraiva*, 2016.

SILVA, A. P.; ALMEIDA, T. A. Imprensa e redes sociais: desafios e oportunidades. *Revista de Comunicação e Tecnologia*, v. 8, n. 2, p. 1–14, 2019.

SOLIS, B. The end of business as usual: Rewire the way you work to succeed in the consumer revolution. John Wiley & Sons, 2012.

STUTZMAN, F. Privacy in social networks. communications of the acm. v. 54, n. 8, p. 126–134, 2011.

STUTZMAN, F. Privacy and data collection in social media research: A review of the literature. *Journal of Computer-Mediated Communication*, v. 23, n. 3, p. 90–110, 2018.

TADDEO, M.; FLORIDI, L. Data ethics: An overview. in the oxford handbook of information and computer ethics. *Oxford University Press*, p. 3–28, 2018.

TANNER, A. Never give stores your zip code. here's why. *Revista FORBES. Disponível em: http://bit. ly/2UWih2w*, 2013.

TRIVEDI, S. K. et al. *Handbook of research on advanced data mining techniques and applications for business intelligence*. [S.l.: s.n.], 2017.

TUFEKCI, Z. Engineering the public: Big data, surveillance, and computational politics. *First Monday*, v. 7, p. 19, 2014.

União Europeia. Regulamento (ue) 2016/679 do parlamento europeu e do conselho. 2016. Disponível em: ⟨https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679⟩.

WANG, X.; CHEN, Y.; CHEN, H. Privacy concerns and trust in social media: An examination of the facebook-germany controversy. *Journal of Computer Information Systems*, v. 57, n. 1, p. 1–12, 2016.