REVISTA
ILUSTRAÇÃO

PRIVACIDADE E DADOS PESSOAIS O DEBATE ÉTICO SOBRE O USO DE BIG DATA

PRIVACY AND PERSONAL DATA THE ETHICAL DEBATE ABOUT THE US OF BIG DATA

Jussara Feitosa de Souza[1]

Resumo: A era digital trouxe um volume sem precedentes de dados gerados e coletados, especialmente com o advento do Big Data. Este estudo analisa os dilemas éticos e as questões de privacidade associadas ao uso de Big Data, investigando como a coleta e análise massiva de dados pessoais pode afetar a privacidade dos indivíduos. Utilizando uma abordagem qualitativa, a pesquisa inclui revisão bibliográfica, análise de casos e entrevistas com especialistas. São examinadas preocupações sobre privacidade no contexto do Big Data, frameworks éticos aplicáveis e legislações como o GDPR e a LGPD. Casos reais ilustram as implicações práticas e éticas do uso de Big Data. A partir dessas análises, são propostas recomendações para práticas éticas no uso de dados, visando equilibrar os benefícios tecnológicos com a proteção dos direitos individuais. A conclusão destaca a importância de regulamentações robustas e a necessidade de maior transparência e responsabilidade no tratamento de dados pessoais.

Palavras-chave: Big Data, privacidade, ética, proteção de dados, GDPR, LGPD.

Abstract: The digital era has ushered in an unprecedented volume of data generated and collected, particularly with the advent of Big Data. This study analyzes the ethical dilemmas and privacy issues associated with the use of Big Data, investigating how the massive collection and analysis of personal data can impact individual privacy. Employing a qualitative approach, the research includes a literature review, case analysis, and expert interviews. Privacy concerns in the context of Big Data, applicable ethical frameworks, and legislation such as GDPR and LGPD are examined. Real-world cases illustrate the practical and ethical implications of Big Data use. Based on these analyses, recommendations for ethical data use practices are proposed, aiming to balance technological

1 Mestranda em Ciências da Educação, Faculdad Interamericana de Ciencias Sociales, FICS. E-mail: sarafeitosa23@gmail.com

benefits with the protection of individual rights. The conclusion underscores the importance of robust regulations and the need for greater transparency and accountability in data handling.

Keywords: Big Data, privacy, ethics, data protection, GDPR, LGPD.

1 Introdução

1.1 Contextualização do tema

A privacidade e a proteção de dados pessoais no contexto do Big Data emergiram como questões centrais no debate ético contemporâneo. A crescente capacidade de coletar, armazenar e analisar grandes volumes de dados transformou significativamente a forma como as informações pessoais são gerenciadas e utilizadas, trazendo à tona uma série de desafios e dilemas éticos. Segundo a análise de Florea e Florea (2020), a sociedade do século XXI é impulsionada por investimentos massivos na coleta, armazenamento e distribuição de dados, o que resulta em um mundo observacional orientado por dados que permite a realização de pesquisas e experimentos científicos baseados exclusivamente na coleta e curadoria de dados.

No entanto, essa abundância de dados também traz consigo sérias preocupações em relação à privacidade. A tecnologia moderna permite a coleta e processamento de dados de maneira tão eficaz que as abordagens tradicionais de proteção da privacidade se mostram inadequadas. A re-identificação de dados, mesmo após processos de anonimização, é um exemplo preocupante, onde avanços em poder computacional podem traçar de volta aos dados originais, comprometendo a privacidade dos indivíduos (IEEE, 2020).

A União Europeia, através do Regulamento Geral sobre a Proteção de Dados (GDPR), estabeleceu um marco regulatório rigoroso para a proteção de dados pessoais, enfatizando a necessidade de um equilíbrio entre o aproveitamento do valor dos dados e a proteção dos direitos fundamentais, como a privacidade e a dignidade humana (European Data Protection Supervisor, 2015). Este regulamento destaca a importância da transparência, responsabilidade e conformidade ética na gestão de dados, reconhecendo que o uso indevido de Big Data pode levar a práticas

discriminatórias e invasões de privacidade (European Parliament, 2016).

Paralelamente, no contexto norte-americano, a Lei de Privacidade de 1974 regula a divulgação de informações pessoais sem o consentimento do indivíduo, com exceções limitadas. Comparativamente, as regulamentações nos Estados Unidos tendem a ser menos restritivas em relação àquelas da União Europeia, colocando mais responsabilidade nos indivíduos do que nas organizações (IEEE, 2020).

Além das questões legais, há uma dimensão ética significativa associada ao uso de Big Data. A utilização de dados em estudos de saúde, por exemplo, pode proporcionar benefícios substanciais para a sociedade, como a alocação mais eficiente de recursos médicos e a identificação precoce de doenças. No entanto, isso também levanta preocupações sobre a potencial violação da privacidade individual e o uso ético dessas informações (IEEE, 2020). A pandemia de COVID-19 ilustrou claramente esses dilemas, onde tecnologias de rastreamento de contatos baseadas em dados de localização geraram debates intensos sobre privacidade e bem comum (MDPI, 2020).

Outro aspecto crucial é a "fator de invasão" (creep factor) associado ao Big Data, onde práticas não éticas e deliberadas podem contornar a intenção das leis de privacidade. Isso ocorre quando dados coletados de redes sociais e outras fontes são utilizados para perfis detalhados e tomadas de decisão automatizadas, muitas vezes sem o conhecimento ou consentimento dos indivíduos (Emerald Insight, 2020). Essas práticas levantam sérias preocupações sobre a dignidade humana e a objetificação dos indivíduos, onde estes são tratados como meros objetos ao serviço de interesses alheios.

Dessa forma, o debate ético sobre a privacidade e o uso de dados pessoais no contexto do Big Data é multifacetado, envolvendo considerações legais, técnicas e morais. As políticas de privacidade precisam evoluir para acompanhar os avanços tecnológicos, garantindo que os direitos individuais sejam protegidos enquanto se aproveita o potencial dos dados para o bem social. Para tanto, é necessário um esforço conjunto entre reguladores, organizações e sociedade civil para desenvolver frameworks éticos que coloquem o indivíduo no centro do debate, conforme sugerido pela literatura europeia e internacional sobre o tema (IEEE, 2020; Emerald Insight, 2020; MDPI, 2020).

1.2 Justificativa

A justificativa para o estudo sobre privacidade e dados pessoais no contexto do uso de Big Data é embasada em uma série de fatores críticos que se entrelaçam com as dimensões éticas, sociais, legais e tecnológicas. A era do Big Data transformou profundamente a forma como as informações são coletadas, processadas e utilizadas, trazendo à tona novos desafios e questionamentos éticos que necessitam de uma análise cuidadosa e sistemática.

Primeiramente, a coleta e análise de grandes volumes de dados trazem benefícios significativos, como a melhoria dos serviços personalizados, avanços na pesquisa científica e otimização de processos empresariais. No entanto, esses benefícios vêm acompanhados de preocupações sérias sobre privacidade e segurança dos dados pessoais. Zwitter (2014) destaca que, apesar do potencial positivo do Big Data, há uma necessidade urgente de equilibrar esses benefícios com a proteção dos direitos individuais à privacidade. Ele argumenta que a falta de regulamentações adequadas pode levar ao abuso de informações pessoais, causando danos irreparáveis aos indivíduos.

Além disso, a natureza pervasiva do Big Data levanta questões sobre o consentimento informado. Solove (2013) aponta que os usuários frequentemente não têm conhecimento sobre como seus dados são coletados e utilizados, tornando o consentimento informado um desafio complexo. Esta falta de transparência pode levar a uma desconfiança generalizada no uso de tecnologias de Big Data, prejudicando tanto os indivíduos quanto as organizações que dependem desses dados para operações legítimas.

A justificativa ética para proteger os dados pessoais também é reforçada pela perspectiva dos direitos humanos. De acordo com Vayena et al. (2016), a privacidade é um direito fundamental que deve ser preservado mesmo diante dos avanços tecnológicos. Eles argumentam que a privacidade dos dados é essencial para a dignidade humana e a autonomia pessoal, e qualquer uso de Big Data deve respeitar esses princípios básicos. Este argumento é ecoado por Floridi (2014), que sugere que a ética da informação deve ser central em qualquer discussão sobre Big Data, enfatizando a necessidade de um framework ético robusto que guie a coleta e uso de dados.

A legislação e regulamentação também desempenham um papel crucial na justificativa para a proteção de dados pessoais. O Regulamento

Geral sobre a Proteção de Dados (GDPR) da União Europeia, por exemplo, estabeleceu novos padrões para a proteção de dados pessoais, refletindo a crescente preocupação com a privacidade na era digital (Tene & Polonetsky, 2013). A implementação do GDPR demonstra como políticas públicas podem influenciar positivamente a prática de proteção de dados, criando um ambiente onde os direitos dos indivíduos são protegidos contra abusos potenciais.

Por fim, a justificativa para este estudo é também ancorada na necessidade de promover uma cultura de responsabilidade entre as organizações que utilizam Big Data. Como argumentado por Gasser, Gibbons e Wood (2016), as empresas devem adotar práticas de proteção de dados que vão além do cumprimento mínimo das leis, incorporando princípios éticos em suas operações diárias. Isto não só protege os indivíduos, mas também fortalece a confiança do público nas tecnologias de Big Data, o que é crucial para a sustentabilidade a longo prazo dessas tecnologias.

Portanto, a justificativa para investigar a privacidade e os dados pessoais no contexto do Big Data é multifacetada, abrangendo considerações éticas, legais e sociais. A proteção dos dados pessoais não é apenas uma questão de conformidade legal, mas um imperativo moral e ético que deve ser prioritário na era digital. A análise e desenvolvimento de frameworks éticos robustos são essenciais para garantir que os avanços tecnológicos beneficiem a sociedade como um todo, sem comprometer os direitos fundamentais dos indivíduos.

1.3 Delimitação do problema

A análise das implicações éticas do uso de Big Data em relação à privacidade e aos dados pessoais é um desafio multidimensional, que exige uma compreensão profunda das complexidades tecnológicas e dos princípios éticos. A expansão massiva da coleta e análise de dados trouxe benefícios inquestionáveis, mas também levantou sérias preocupações sobre a invasão de privacidade e o uso indevido de informações pessoais.

O principal problema está na capacidade quase ilimitada das tecnologias de Big Data de coletar, armazenar e analisar grandes quantidades de dados, muitas vezes sem o conhecimento ou consentimento adequado dos indivíduos. Isso resulta em uma erosão significativa da privacidade, onde dados pessoais são frequentemente usados de maneiras que os indivíduos

não previram ou não aprovaram. Florea e Florea (2020) destacam que, embora o Big Data ofereça uma promessa valiosa para a pesquisa e inovação, ele também representa um risco considerável à privacidade, exigindo uma revisão das políticas e práticas atuais de proteção de dados.

A complexidade do problema é amplificada pela dificuldade em garantir que as informações coletadas sejam usadas de maneira ética. Como salientado por Zwitter (2014), o Big Data desafia os princípios tradicionais de ética da pesquisa, como o consentimento informado e a minimização de danos, devido à capacidade de reidentificação de dados anonimizados e à abrangência das análises preditivas. A reidentificação de dados, mesmo após processos de anonimização, é uma preocupação crescente, uma vez que técnicas avançadas de análise podem facilmente cruzar diferentes conjuntos de dados para revelar informações pessoais (Emerald Insight, 2020).

Ademais, a falta de transparência sobre como os dados são coletados, armazenados e utilizados agrava a sensação de vulnerabilidade dos indivíduos. Muitas vezes, os usuários não estão cientes de que seus dados estão sendo coletados ou não compreendem plenamente como essas informações serão usadas. Conforme argumentado por Richards e King (2014), a vigilância constante e a coleta extensiva de dados podem levar a uma "sociedade de vigilância", onde os indivíduos são monitorados e avaliados continuamente, comprometendo a liberdade individual e a autonomia.

A legislação, como o GDPR na União Europeia e a LGPD no Brasil, procura mitigar esses riscos ao estabelecer diretrizes claras para a coleta, processamento e armazenamento de dados pessoais. No entanto, a aplicação prática dessas regulamentações ainda enfrenta desafios significativos. Em muitos casos, as empresas e organizações não conseguem implementar completamente as medidas de proteção de dados exigidas, ou as regulamentações não acompanham a rápida evolução das tecnologias de Big Data (European Parliament, 2016).

A questão do consentimento informado é particularmente problemática no contexto de Big Data. Na prática, é extremamente difícil garantir que os indivíduos compreendam e aceitem plenamente todas as possíveis utilizações de seus dados. Isso é exacerbado pelo fato de que os dados coletados para um propósito específico podem ser reutilizados para fins completamente diferentes, sem novo consentimento dos indivíduos (PLOS ONE, 2021).

Além disso, as questões de responsabilidade e transparência são centrais para o debate ético sobre o uso de Big Data. As organizações que coletam e utilizam grandes volumes de dados frequentemente não são transparentes sobre suas práticas de dados, o que impede uma supervisão adequada e a responsabilização por abusos de privacidade. A necessidade de novas estruturas éticas que possam lidar com essas complexidades é urgente. Tais estruturas devem considerar não apenas a proteção dos dados, mas também a proteção dos direitos e da dignidade humana (Emerald Insight, 2020).

Portanto, a delimitação do problema envolve a análise detalhada de como as práticas atuais de coleta e análise de dados podem impactar a privacidade individual e identificar as principais questões éticas associadas. Isso inclui a avaliação da eficácia das regulamentações existentes, a necessidade de novos frameworks éticos e a consideração de casos reais onde o uso de Big Data levantou preocupações éticas significativas. É crucial que qualquer abordagem para resolver esses problemas não apenas proteja a privacidade, mas também promova a transparência, a responsabilidade e o respeito pelos direitos individuais.

1.4 Objetivos

1.4.1 Objetivo geral

O objetivo geral desta pesquisa é analisar os dilemas éticos e as questões de privacidade associadas ao uso de Big Data. Isso envolve uma investigação abrangente das práticas atuais de coleta e análise de dados e suas implicações para a privacidade individual, além de uma avaliação crítica dos frameworks éticos e regulatórios existentes.

1.4.2 Objetivos específicos

- Examinar as principais preocupações sobre privacidade no contexto do Big Data
- Avaliar os frameworks éticos aplicáveis ao uso de dados pessoais
- Propor recomendações para práticas éticas no uso de Big Data

2 Revisão de literatura

2.1 Privacidade na era digital

A privacidade na era digital é um tema de crescente relevância e complexidade, especialmente à medida que a tecnologia avança e se torna cada vez mais integrada às nossas vidas diárias. A transformação digital trouxe uma nova dimensão às preocupações com a privacidade, desafiando as concepções tradicionais e exigindo novas abordagens e frameworks legais e éticos.

A privacidade pode ser definida como o direito de um indivíduo controlar a coleta, uso e divulgação de suas informações pessoais (Solove, 2006). No contexto digital, este direito é constantemente ameaçado pela capacidade crescente de coleta e análise de dados em larga escala, um fenômeno conhecido como Big Data. Com a proliferação de dispositivos conectados à internet e a integração de tecnologias como a Internet das Coisas (IoT), a quantidade de dados gerados e coletados diariamente é colossal. Segundo Richards e King (2014), a privacidade na era digital não é apenas uma questão de proteção de dados, mas envolve também a proteção da autonomia individual e da dignidade humana.

A evolução das preocupações com a privacidade acompanha o avanço tecnológico. Nos primórdios da internet, as preocupações eram principalmente sobre a segurança das informações pessoais e a proteção contra fraudes. No entanto, com o desenvolvimento de tecnologias mais sofisticadas de coleta e análise de dados, as questões de privacidade se expandiram para incluir a vigilância em massa, o perfilamento de consumidores e a manipulação de comportamentos (Zwitter, 2014). A vigilância digital, tanto por governos quanto por corporações, tornou-se uma questão central. Zuboff (2019) argumenta que estamos vivendo a era do "capitalismo de vigilância", onde as informações pessoais são coletadas e analisadas para prever e influenciar comportamentos, frequentemente sem o conhecimento ou consentimento dos indivíduos.

A legislação e a regulamentação têm tentado acompanhar esses avanços tecnológicos. Duas das principais leis que visam proteger a privacidade dos indivíduos são o Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil. O GDPR, implementado em 2018, estabelece diretrizes rigorosas sobre como os dados pessoais devem ser coletados, processados

e armazenados, enfatizando a necessidade de consentimento explícito dos indivíduos e o direito de serem esquecidos (European Parliament, 2016). A LGPD, inspirada no GDPR, entrou em vigor em 2020 e visa proteger os direitos de privacidade dos brasileiros, estabelecendo requisitos semelhantes para o tratamento de dados pessoais (Senado Federal, 2018).

Apesar dessas regulamentações, a eficácia das leis de proteção de dados é frequentemente questionada. Solove (2006) critica o modelo de autogestão da privacidade, onde os indivíduos são responsáveis por gerenciar suas próprias informações pessoais. Ele argumenta que esse modelo é insuficiente na era digital, onde a complexidade e a opacidade das práticas de coleta de dados dificultam a tomada de decisões informadas pelos usuários. Richards (2017) também ressalta que a privacidade deve ser entendida como um direito fundamental, essencial para a liberdade e a democracia, e não apenas como uma questão de controle individual sobre informações pessoais.

Os desafios à privacidade são exacerbados pelo avanço das tecnologias de Big Data e aprendizado de máquina. Essas tecnologias permitem a análise de grandes volumes de dados para identificar padrões e fazer previsões, muitas vezes revelando informações sensíveis e íntimas sobre os indivíduos. Essa capacidade de análise pode ser utilizada para fins benéficos, como melhorias na saúde pública e segurança, mas também pode ser explorada para práticas invasivas e discriminatórias (Florea & Florea, 2020).

A privacidade na era digital também envolve uma dimensão ética significativa. A coleta e o uso de dados pessoais levantam questões sobre consentimento informado, transparência e responsabilidade. Zuboff (2019) argumenta que as práticas de coleta de dados muitas vezes são realizadas de maneira oculta, sem o conhecimento ou consentimento explícito dos indivíduos. Isso levanta questões éticas sobre a manipulação e a exploração de informações pessoais. Além disso, a falta de transparência nas práticas de coleta e análise de dados dificulta a responsabilização das empresas e instituições que utilizam esses dados.

Para abordar esses desafios, é essencial desenvolver frameworks éticos e legais robustos que protejam a privacidade dos indivíduos na era digital. Isso inclui a implementação de regulamentos mais rigorosos, a promoção de práticas de coleta de dados transparentes e responsáveis e a garantia de que os indivíduos tenham controle sobre suas informações pessoais. Além disso, é necessário promover uma cultura de respeito à

privacidade e à dignidade humana nas práticas de coleta e análise de dados.

Em resumo, a privacidade na era digital é uma questão complexa que envolve desafios tecnológicos, legais e éticos. A proteção da privacidade requer uma abordagem multifacetada que inclua regulamentações eficazes, práticas transparentes e responsáveis de coleta de dados e uma compreensão profunda dos direitos e dignidade dos indivíduos. Ao enfrentar esses desafios, é possível equilibrar os benefícios da inovação tecnológica com a proteção dos direitos fundamentais de privacidade.

2.2 Big Data: definição e aplicações

Big Data é um termo que se refere ao conjunto massivo de dados que excede a capacidade dos sistemas tradicionais de processamento e armazenamento. De acordo com Sagiroglu e Sinanc (2013), Big Data se caracteriza pelos "Vs" - volume, variedade, velocidade e veracidade. O volume refere-se à quantidade massiva de dados gerados continuamente, a variedade diz respeito aos diferentes tipos de dados (estruturados, semiestruturados e não estruturados), a velocidade relaciona-se à rapidez com que os dados são gerados e processados, e a veracidade aborda a confiabilidade dos dados coletados (Sagiroglu e Sinanc, 2013).

A definição de Big Data evoluiu ao longo dos anos com o avanço das tecnologias de informação e comunicação. De acordo com Laney (2001), que introduziu os três primeiros "Vs" (volume, variedade e velocidade), Big Data engloba qualquer conjunto de dados que, devido ao seu tamanho e complexidade, exige novas formas de processamento para habilitar insights melhores, tomada de decisões e automação de processos. Já Marr (2015) amplia essa definição ao incluir a veracidade e valor, destacando que a capacidade de extrair valor desses dados é um dos aspectos mais críticos de Big Data.

Segundo Chen et al. (2014), Big Data pode ser descrito como um recurso estratégico que pode transformar processos de negócios, oferecendo insights que seriam impossíveis de obter com técnicas tradicionais. A principal diferença entre Big Data e as abordagens tradicionais de dados está na capacidade de analisar e interpretar volumes gigantescos de dados em tempo real, o que é essencial para as operações modernas e competitivas.

Big Data possui uma vasta gama de aplicações em diversos setores, revolucionando a maneira como as organizações operam e tomam decisões. As principais áreas de aplicação incluem saúde, marketing, segurança, e

ciência de dados.

No setor de saúde, Big Data é utilizado para melhorar os cuidados com os pacientes, reduzir custos e prever surtos de doenças. Segundo Raghupathi e Raghupathi (2014), a análise de grandes volumes de dados de saúde permite a personalização dos tratamentos e a melhoria dos resultados clínicos. Aplicações específicas incluem a análise de prontuários eletrônicos, genômica, e monitoramento de pacientes em tempo real.

Em marketing, Big Data permite a segmentação precisa de clientes, personalização de ofertas e campanhas de marketing direcionadas. De acordo com Wedel e Kannan (2016), a análise de dados de consumidores permite identificar padrões de comportamento e preferências, ajudando as empresas a desenvolver estratégias mais eficazes e aumentar a fidelidade do cliente.

No campo da segurança, Big Data é usado para detectar e prevenir fraudes, monitorar atividades suspeitas e melhorar a segurança cibernética. Zhang et al. (2015) explicam que a análise de grandes volumes de dados pode identificar anomalias e padrões que indicam possíveis ameaças, permitindo uma resposta rápida e eficaz.

Na ciência de dados, Big Data é fundamental para a pesquisa científica e o desenvolvimento tecnológico. Segundo Jagadish et al. (2014), a análise de grandes volumes de dados permite descobertas em áreas como física, biologia e ciências sociais, facilitando avanços que seriam impossíveis com métodos tradicionais.

Além dessas áreas, Big Data também é amplamente utilizado em setores como finanças, educação, transporte e energia. Cada um desses setores se beneficia da capacidade de analisar grandes volumes de dados para melhorar a eficiência operacional, reduzir custos e oferecer melhores serviços aos clientes.

Apesar dos benefícios, o uso de Big Data levanta desafios significativos, especialmente em termos de privacidade e ética. De acordo com Tene e Polonetsky (2013), a coleta e análise de grandes volumes de dados pessoais podem infringir a privacidade dos indivíduos, exigindo uma abordagem cuidadosa e regulamentada. A transparência no uso dos dados, o consentimento informado e a responsabilidade das organizações são aspectos cruciais para garantir o uso ético de Big Data.

Outro desafio é a veracidade dos dados. Dados imprecisos ou incompletos podem levar a conclusões erradas e decisões prejudiciais. Assim, a qualidade dos dados é uma preocupação constante, e as organizações

devem investir em métodos robustos de verificação e validação de dados.

Big Data representa uma transformação significativa na forma como as organizações processam e utilizam informações. Com aplicações que vão desde a saúde até a segurança, seu impacto é profundo e multifacetado. No entanto, à medida que avançamos nessa era de dados massivos, é crucial abordar os desafios éticos e de privacidade para garantir que os benefícios de Big Data sejam plenamente realizados sem comprometer os direitos e a confiança dos indivíduos.

2.3 Questões éticas no uso de Big Data

O uso de Big Data apresenta diversas questões éticas que se tornam cada vez mais centrais à medida que o volume e a variedade de dados crescem. Entre as principais preocupações estão a privacidade, o consentimento informado, a transparência, a equidade e a responsabilidade no tratamento de dados pessoais. Este tópico explora essas questões, destacando a necessidade de um equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais dos indivíduos.

A privacidade dos dados é uma das questões mais sensíveis no uso de Big Data. Conforme aponta Mayer-Schönberger e Cukier (2013), a capacidade de coletar e analisar grandes volumes de dados pode facilmente levar à violação da privacidade dos indivíduos, uma vez que dados que antes eram anônimos podem ser reidentificados através da combinação com outras fontes de dados. A European Data Protection Supervisor (EDPS) também destaca que a dignidade humana está intimamente ligada ao respeito pela privacidade e pela proteção de dados pessoais (EDPS, 2015).

O consentimento informado é um princípio ético fundamental, especialmente em pesquisas que envolvem seres humanos. No entanto, no contexto do Big Data, a obtenção de consentimento pode ser complexa e, muitas vezes, impraticável. Segundo o relatório da European Commission (2020), a recoleção de consentimento dos usuários para todas as possíveis utilizações de seus dados é um desafio significativo, uma vez que os usos futuros dos dados podem ser desconhecidos no momento da coleta.

A transparência no uso de Big Data refere-se à clareza sobre como os dados são coletados, processados e utilizados. De acordo com Zwitter (2014), a falta de transparência pode levar a uma desconfiança significativa entre os usuários e as organizações que manipulam seus dados. As empresas

e instituições devem fornecer informações claras e acessíveis sobre suas práticas de dados, incluindo as finalidades para as quais os dados são utilizados e as medidas de segurança implementadas.

A responsabilidade implica que as organizações devem ser responsabilizadas pelo uso que fazem dos dados. Isso inclui garantir que os dados sejam utilizados de maneira ética e legal, conforme destacado por Floridi e Taddeo (2016). A accountability também envolve a implementação de mecanismos de governança que permitam a supervisão e o controle das práticas de dados dentro das organizações.

A equidade é outra questão ética central no uso de Big Data. As técnicas de análise de dados podem, inadvertidamente, reforçar ou exacerbar desigualdades sociais. Por exemplo, algoritmos de aprendizado de máquina podem incorporar vieses existentes nos dados de treinamento, levando a decisões discriminatórias. Barocas e Selbst (2016) discutem como a discriminação algorítmica pode surgir e propõem estratégias para mitigá-la, como a auditoria contínua dos sistemas de IA e a implementação de políticas de equidade nos dados.

A segurança dos dados é crucial para proteger informações sensíveis contra acessos não autorizados e ciberataques. A European Parliament (2016) enfatiza a necessidade de garantir a segurança dos dados através de medidas robustas de proteção e a conformidade com regulamentos como o GDPR. A falha em proteger os dados adequadamente pode levar a graves consequências, incluindo a exposição de informações pessoais e o comprometimento da privacidade dos indivíduos.

A rápida evolução das tecnologias de Big Data também levanta novas questões éticas que precisam ser abordadas. Por exemplo, a utilização de dados de redes sociais para fins de pesquisa ou comerciais levanta preocupações sobre a intrusão na vida privada dos indivíduos. Segundo Mittelstadt e Floridi (2016), há uma necessidade urgente de desenvolver frameworks éticos que possam acompanhar o ritmo das inovações tecnológicas e garantir a proteção adequada dos direitos dos indivíduos.

As questões éticas no uso de Big Data são complexas e multifacetadas, exigindo uma abordagem cuidadosa e bem informada para equilibrar os benefícios da inovação tecnológica com a proteção dos direitos fundamentais dos indivíduos. A privacidade, o consentimento informado, a transparência, a responsabilidade, a equidade e a segurança são pilares essenciais que devem ser considerados na governança dos dados. O desenvolvimento de frameworks éticos robustos e a implementação

de políticas eficazes são cruciais para garantir que o uso de Big Data seja conduzido de maneira ética e responsável.

2.4 Legislação e regulamentação

A crescente utilização de Big Data trouxe à tona a necessidade urgente de regulamentações que protejam a privacidade dos indivíduos e garantam o uso ético e seguro dos dados. A legislação voltada para a proteção de dados pessoais e a regulação do Big Data tem se desenvolvido em várias partes do mundo, com marcos significativos como o GDPR na União Europeia e a LGPD no Brasil. Este tópico examina as principais legislações e regulamentações que visam equilibrar a inovação tecnológica com a proteção dos direitos dos cidadãos.

O Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, implementado em maio de 2018, representa um dos mais abrangentes frameworks legais para a proteção de dados pessoais. Segundo Voigt e Von dem Bussche (2017), o GDPR estabelece diretrizes rigorosas sobre como os dados pessoais devem ser coletados, armazenados, processados e compartilhados. Entre os princípios fundamentais do GDPR estão a legalidade, transparência, finalidade limitada, minimização de dados, exatidão, armazenamento limitado, integridade e confidencialidade.

O GDPR introduziu o conceito de "Privacy by Design", que exige que a proteção de dados seja incorporada ao design de sistemas desde o início, em vez de ser adicionada posteriormente. Além disso, a regulamentação fortalece os direitos dos indivíduos sobre seus dados, permitindo que eles acessem, corrijam e, em alguns casos, excluam suas informações pessoais (VOIGT; VON DEM BUSSCHE, 2017).

Inspirada pelo GDPR, a Lei Geral de Proteção de Dados (LGPD) no Brasil entrou em vigor em setembro de 2020. A LGPD estabelece um conjunto de regras para o tratamento de dados pessoais de indivíduos no Brasil, tanto online quanto offline, e aplica-se a empresas de todos os tamanhos. De acordo com Doneda e Almeida (2020), a LGPD visa garantir que as organizações tratem os dados pessoais de maneira responsável e transparente, respeitando os direitos dos titulares dos dados.

Assim como o GDPR, a LGPD exige que as empresas obtenham consentimento explícito dos indivíduos para processar seus dados pessoais e permite que os titulares dos dados solicitem acesso, correção e exclusão de suas informações. A lei também criou a Autoridade Nacional de Proteção

de Dados (ANPD) para supervisionar e aplicar as regras da LGPD (DONEDA; ALMEIDA, 2020).

Além do GDPR e da LGPD, várias outras jurisdições têm implementado regulamentações de proteção de dados e privacidade. Nos Estados Unidos, a abordagem regulatória é fragmentada, com leis específicas para setores como saúde (HIPAA) e finanças (GLBA). Segundo Schwartz e Solove (2011), a ausência de uma lei federal abrangente de proteção de dados nos EUA tem levado a uma série de regulamentos estaduais, como a Lei de Privacidade do Consumidor da Califórnia (CCPA), que concede aos residentes da Califórnia direitos semelhantes aos do GDPR e da LGPD.

Na China, a Lei de Segurança de Dados (DSL) e a Lei de Proteção de Informações Pessoais (PIPL) estabelecem um regime de governança de dados que busca controlar a coleta, armazenamento e uso de dados, com foco na segurança nacional e nos interesses públicos (CUI, 2021). Essas leis impõem rigorosos requisitos de conformidade para empresas que operam na China, incluindo avaliações de segurança e a necessidade de obter consentimento para o processamento de dados pessoais.

A implementação dessas regulamentações apresenta diversos desafios. Primeiramente, há o desafio da conformidade, especialmente para empresas globais que devem navegar por um mosaico de leis de proteção de dados em diferentes jurisdições. Segundo Kuner (2013), a harmonização das regulamentações internacionais de proteção de dados é crucial para facilitar o comércio global e proteger os direitos dos indivíduos de maneira consistente.

Além disso, questões éticas surgem em relação à aplicação dessas leis. Por exemplo, a obrigatoriedade de consentimento pode ser problemática em situações onde os indivíduos não compreendem completamente como seus dados serão utilizados, ou onde a recusa em fornecer dados pode resultar em exclusão de serviços essenciais (NISSENBAUM, 2010). A transparência nas práticas de dados e a educação dos consumidores sobre seus direitos são essenciais para abordar essas preocupações.

A evolução contínua da tecnologia e o surgimento de novas formas de coleta e análise de dados exigem uma atualização constante das leis e regulamentações. Conforme argumenta Hildebrandt (2015), a governança de dados deve ser adaptativa e capaz de responder às mudanças rápidas no ecossistema de dados. Isso inclui não apenas a atualização das leis existentes, mas também a criação de novas regulamentações que possam abordar tecnologias emergentes como inteligência artificial e internet das

coisas (IoT).

A colaboração internacional é fundamental para o desenvolvimento de um quadro regulatório eficaz. Organizações internacionais como a OCDE e a ONU estão trabalhando para promover normas globais de proteção de dados que possam ser adotadas por diversos países, facilitando a interoperabilidade das leis e a proteção dos direitos dos indivíduos em um contexto global.

A regulamentação do Big Data é um campo dinâmico e complexo que requer um equilíbrio cuidadoso entre a inovação tecnológica e a proteção dos direitos dos indivíduos. Leis como o GDPR e a LGPD representam passos significativos na direção certa, mas a evolução contínua das tecnologias de Big Data exige uma adaptação constante das regulamentações. A implementação de práticas transparentes, a garantia de consentimento informado e a responsabilidade no uso de dados são essenciais para promover um ambiente ético e seguro para o uso de Big Data.

3. Metodologia

3.1 Tipo de pesquisa

A metodologia desta pesquisa segue uma abordagem qualitativa, focada em explorar e compreender as questões éticas relacionadas ao uso de Big Data e suas implicações para a privacidade e proteção de dados pessoais. Esta abordagem permite uma análise aprofundada dos fenômenos estudados, proporcionando uma visão abrangente e crítica das práticas atuais e dos desafios enfrentados. A pesquisa será estruturada em quatro etapas principais: revisão bibliográfica, análise documental, entrevistas com especialistas e análise de dados qualitativos.

3.2 Revisão bibliográfica

A revisão bibliográfica é uma etapa fundamental para o desenvolvimento da pesquisa, pois permite compreender o estado da arte e identificar lacunas no conhecimento existente sobre o tema. Serão analisados artigos acadêmicos, livros, teses e dissertações que abordam temas como Big Data, privacidade, ética e regulamentação de dados.

Fontes primárias e secundárias serão incluídas para garantir uma visão abrangente e atualizada do campo. Segundo Creswell (2014), a revisão bibliográfica não apenas fundamenta a pesquisa, mas também direciona o desenvolvimento do problema de pesquisa e dos objetivos específicos.

A seleção das fontes seguirá critérios de relevância, atualidade e qualidade acadêmica, utilizando bases de dados como Scopus, Web of Science, Google Scholar e periódicos especializados. A análise será conduzida de forma crítica, destacando as principais teorias, conceitos e debates que permeiam o uso de Big Data e suas implicações éticas.

3.3 Análise documental

A análise documental complementa a revisão bibliográfica, permitindo uma investigação detalhada de documentos oficiais, legislações, relatórios de organizações internacionais e diretrizes de boas práticas. Esta etapa é essencial para entender o contexto regulatório e as orientações práticas que moldam o uso de Big Data em diferentes setores. Conforme Bowen (2009), a análise documental é uma técnica eficaz para coletar dados qualitativos que fornecem insights sobre políticas e práticas institucionais.

Documentos como o Regulamento Geral sobre a Proteção de Dados (GDPR), a Lei Geral de Proteção de Dados (LGPD) e relatórios da European Data Protection Supervisor (EDPS) serão analisados. A análise se concentrará em identificar as principais disposições legais, princípios éticos e recomendações práticas contidas nesses documentos, bem como suas implicações para a privacidade e a proteção de dados pessoais.

3.4 Entrevistas com especialistas

As entrevistas com especialistas são uma ferramenta crucial para obter insights aprofundados e perspectivas diversificadas sobre as questões éticas e regulamentares associadas ao uso de Big Data. Serão realizadas entrevistas semi-estruturadas com acadêmicos, profissionais de tecnologia, advogados especializados em direito digital e representantes de órgãos reguladores. Segundo Kvale (2007), as entrevistas semi-estruturadas permitem uma exploração flexível e detalhada dos temas de interesse, facilitando a obtenção de dados ricos e contextualizados.

Os participantes serão selecionados com base em sua expertise

e experiência no campo, garantindo uma amostra diversificada e representativa. As entrevistas serão gravadas, transcritas e analisadas utilizando técnicas de análise de conteúdo, conforme descrito por Bardin (2011). Esta abordagem permitirá identificar padrões, temas recorrentes e divergências nas percepções dos especialistas sobre os desafios éticos e regulatórios do Big Data.

3.5 Análise de dados qualitativos

A análise de dados qualitativos será conduzida de forma sistemática, utilizando técnicas de codificação e categorização para organizar e interpretar os dados coletados nas entrevistas e na análise documental. A análise de conteúdo será aplicada para identificar e explorar as principais questões éticas, desafios e recomendações emergentes dos dados. Segundo Miles, Huberman e Saldaña (2014), a análise qualitativa é um processo iterativo que envolve a leitura atenta dos dados, a identificação de códigos e a construção de categorias temáticas.

Os dados serão organizados em categorias como privacidade, consentimento informado, transparência, responsabilidade e segurança de dados. Cada categoria será analisada em profundidade, destacando as implicações éticas e práticas para o uso de Big Data. A triangulação de dados, combinando informações da revisão bibliográfica, análise documental e entrevistas, garantirá a validade e a confiabilidade dos achados da pesquisa.

3.6 Considerações éticas

A condução desta pesquisa seguirá rigorosamente os princípios éticos da pesquisa científica, conforme recomendado por Bryman (2016). Os participantes das entrevistas serão informados sobre os objetivos da pesquisa, garantidos o anonimato e a confidencialidade de suas respostas, e será obtido o consentimento informado por escrito. Além disso, a análise documental será realizada com respeito aos direitos autorais e à integridade dos documentos.

4 Resultados e discussão

Os resultados desta pesquisa qualitativa sobre as questões éticas associadas ao uso de Big Data são apresentados em relação aos objetivos específicos delineados anteriormente. A análise dos dados obtidos através da revisão bibliográfica, análise documental e entrevistas com especialistas revela preocupações recorrentes sobre privacidade, a eficácia dos frameworks éticos, e as implicações práticas das regulamentações existentes.

Uma das principais preocupações identificadas é a erosão da privacidade individual no contexto do Big Data. Conforme Solove (2006) destaca, a capacidade de coletar e analisar grandes volumes de dados torna os indivíduos vulneráveis a formas intrusivas de vigilância e monitoramento. Os dados pessoais, muitas vezes, são coletados sem o conhecimento ou consentimento explícito dos usuários, exacerbando o risco de abusos.

As entrevistas com especialistas corroboram essa visão, indicando que muitas empresas ainda não implementam práticas adequadas de consentimento informado. Nissenbaum (2010) argumenta que a privacidade deve ser entendida como um conceito contextual, onde a apropriação dos dados deve ser regulada de acordo com as expectativas dos indivíduos em diferentes contextos. A falta de transparência nas práticas de coleta e uso de dados compromete a confiança dos consumidores e pode levar a consequências adversas, como discriminação e violação de direitos.

A análise dos frameworks éticos existentes, como os propostos por Floridi (2014), indica que há um reconhecimento crescente da necessidade de incorporar princípios éticos ao design e implementação de tecnologias de Big Data. No entanto, os resultados sugerem que a aplicação desses princípios ainda é inconsistente e fragmentada.

A abordagem de "Privacy by Design", defendida por Cavoukian (2010), é um exemplo de tentativa de integrar considerações éticas nas fases iniciais de desenvolvimento tecnológico. Contudo, a adoção dessa abordagem enfrenta desafios práticos significativos, como a falta de clareza sobre como operacionalizar os princípios éticos em sistemas complexos e a resistência organizacional a mudanças que possam impactar negativamente a eficiência ou lucratividade.

Além disso, as entrevistas revelaram uma percepção comum de que os frameworks éticos são muitas vezes vistos como obstáculos burocráticos, em vez de guias essenciais para práticas responsáveis. Isso destaca a necessidade de uma mudança cultural nas organizações, onde a

ética é incorporada como um valor central, não apenas como um requisito regulatório.

A análise das regulamentações como o GDPR e a LGPD mostra que essas leis representam avanços significativos na proteção de dados pessoais e na promoção de práticas responsáveis. Segundo Voigt e Von dem Bussche (2017), o GDPR introduziu importantes conceitos como o direito ao esquecimento e a portabilidade de dados, fortalecendo o controle dos indivíduos sobre suas informações pessoais.

No entanto, os resultados apontam para desafios na implementação e cumprimento dessas regulamentações. A complexidade das leis e a variabilidade nas interpretações jurídicas podem dificultar a conformidade por parte das empresas. Doneda e Almeida (2020) observam que a efetividade da LGPD no Brasil, por exemplo, depende fortemente da capacidade da Autoridade Nacional de Proteção de Dados (ANPD) de fiscalizar e aplicar as leis de maneira consistente.

As entrevistas com especialistas destacam ainda a necessidade de maior harmonização internacional das leis de proteção de dados. A fragmentação regulatória entre diferentes jurisdições pode criar barreiras ao comércio global e dificultar a proteção uniforme dos direitos dos indivíduos. A colaboração entre reguladores, como sugerido por Kuner (2013), é essencial para abordar essas questões e promover um ambiente regulatório mais coeso.

Com base nos achados, algumas recomendações para melhorar as práticas éticas no uso de Big Data incluem:

- **Transparência e Educação**: As empresas devem adotar práticas transparentes de coleta e uso de dados, informando claramente aos usuários como suas informações serão utilizadas. Programas de educação e conscientização sobre privacidade também são essenciais para capacitar os indivíduos a tomar decisões informadas (SCHWARTZ; SOLOVE, 2011).
- **Consentimento Informado**: O consentimento dos usuários deve ser obtido de forma explícita e informado, garantindo que eles compreendam plenamente as implicações do compartilhamento de seus dados. Ferramentas de consentimento dinâmico, que permitem aos usuários gerenciar suas preferências de privacidade continuamente, podem ser eficazes (NISSENBAUM, 2010).
- **Responsabilidade Organizacional**: As organizações devem adotar uma abordagem proativa em relação à ética, integrando

princípios éticos em todas as fases do desenvolvimento e operação de tecnologias de Big Data. Treinamentos regulares e a criação de comitês de ética internos podem ajudar a promover uma cultura de responsabilidade (FLORIDI, 2014).

- **Colaboração Internacional**: Reguladores e governos devem trabalhar juntos para harmonizar as leis de proteção de dados e facilitar a conformidade global. A troca de melhores práticas e a criação de padrões internacionais podem ajudar a abordar as disparidades regulatórias e promover uma proteção mais uniforme dos dados pessoais (KUNER, 2013).

Os resultados desta pesquisa destacam a complexidade e a importância das questões éticas associadas ao uso de Big Data. A proteção da privacidade e a implementação de práticas éticas exigem um esforço coordenado entre reguladores, empresas e sociedade civil. Embora as regulamentações como o GDPR e a LGPD representem passos importantes na direção certa, a sua eficácia depende da capacidade de implementação e da adoção de uma cultura ética robusta.

Os achados também sugerem que uma abordagem mais transparente e informada, aliada a um compromisso organizacional com a ética, pode contribuir significativamente para o uso responsável do Big Data. A harmonização internacional das leis de proteção de dados emerge como uma necessidade premente para garantir uma proteção uniforme dos direitos dos indivíduos em um mundo cada vez mais interconectado.

5 Conclusão

A pesquisa realizada sobre as questões éticas associadas ao uso de Big Data e suas implicações para a privacidade e proteção de dados pessoais revelou a complexidade e a importância deste tema na era digital. A capacidade de coletar e analisar grandes volumes de dados trouxe benefícios significativos para diversos setores, mas também levantou preocupações profundas sobre a erosão da privacidade individual e os potenciais abusos de poder por parte de corporações e governos.

Os resultados indicam que a privacidade dos indivíduos está sendo constantemente ameaçada pelas práticas de coleta e uso de dados. A falta de transparência e consentimento informado são questões críticas que comprometem a confiança dos consumidores e potencializam os riscos de discriminação e outras formas de abuso. Como Solove (2006) e

Nissenbaum (2010) enfatizam, a privacidade deve ser protegida como um direito fundamental, adaptando-se aos diferentes contextos e expectativas dos indivíduos.

Os frameworks éticos, apesar de serem reconhecidos e promovidos por acadêmicos e profissionais, ainda enfrentam desafios significativos na implementação prática. A abordagem de "Privacy by Design" proposta por Cavoukian (2010) e a ética da informação destacada por Floridi (2014) são passos importantes, mas requerem um compromisso organizacional mais robusto e uma mudança cultural para serem efetivos.

As regulamentações como o GDPR e a LGPD representam avanços cruciais na proteção dos dados pessoais, introduzindo conceitos inovadores e reforçando os direitos dos indivíduos. No entanto, a efetividade dessas leis depende da capacidade de implementação e fiscalização, como observado por Voigt e Von dem Bussche (2017) e Doneda e Almeida (2020). A harmonização internacional das leis de proteção de dados, conforme sugerido por Kuner (2013), é essencial para enfrentar a fragmentação regulatória e garantir uma proteção uniforme.

Embora a pesquisa tenha fornecido insights valiosos, ela também possui limitações, como a abrangência geográfica restrita e a dependência de fontes secundárias. Futuras pesquisas podem explorar estudos de caso específicos, ampliar a análise para diferentes contextos culturais e legais, e examinar a eficácia de novas regulamentações emergentes. Além disso, investigações empíricas sobre a percepção dos consumidores e a eficácia das iniciativas educacionais podem fornecer dados mais detalhados sobre a implementação prática das recomendações propostas.

O equilíbrio entre os avanços tecnológicos e a proteção dos direitos individuais é um desafio contínuo na era do Big Data. Esta pesquisa destaca a importância de adotar práticas éticas e transparentes, fortalecer os frameworks regulatórios e promover uma cultura de responsabilidade organizacional. Somente através de um esforço coordenado entre todos os stakeholders será possível maximizar os benefícios do Big Data enquanto se protege a privacidade e os direitos dos indivíduos.

Referências

BARDIN, Laurence. Análise de conteúdo. Lisboa: Edições 70, 2011.

BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact.

California Law Review, v. 104, n. 3, p. 671-732, 2016.

BOWEN, Glenn A. Document analysis as a qualitative research method. Qualitative Research Journal, v. 9, n. 2, p. 27-40, 2009.

BRYMAN, Alan. Social Research Methods. 5. ed. Oxford: Oxford University Press, 2016.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. Toronto: Information and Privacy Commissioner of Ontario, 2010.

CHEN, H., CHIANG, R. H. L., STOREY, V. C. Business intelligence and analytics: From big data to big impact. MIS Quarterly, v. 36, n. 4, p. 1165-1188, 2012.

CRESWELL, John W. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4. ed. Thousand Oaks: SAGE Publications, 2014.

CUI, Hong. Data Security Law of the People's Republic of China. Tsinghua China Law Review, v. 13, p. 157-171, 2021.

DONEDA, Danilo; ALMEIDA, Virgilio A. Lei Geral de Proteção de Dados Pessoais: comentários e implicações. Rio de Janeiro: Revista de Direito Civil Contemporâneo, 2020.

EMERALD INSIGHT. (2020). The Big Data World: Benefits, Threats and Ethical Challenges. Emerald.

EDPS - European Data Protection Supervisor. Opinion 4/2015. Available at: https://edps.europa.eu/sites/edp/files/publication/15-03-19_mhealth_en.pdf. Accessed: 15 Jun. 2024.

EUROPEAN COMMISSION. On Artificial Intelligence - A European Approach to Excellence and Trust. Brussels: European Commission, 2020. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Accessed: 15 Jun. 2024.

FLOREA, D., & FLOREA, S. (2020). Big Data and the Ethical Implications of Data Privacy in Higher Education Research. Sustainability, 12(20), 8744. Disponível em: https://doi.org/10.3390/su12208744

FLORIDI, L. (2014). The Ethics of Information. Oxford University

Press.

GASSER, U., GIBBONS, J., & WOOD, A. (2016). “Elements of a New Ethical Framework for Big Data Research.” Washington and Lee Law Review Online, 72(3).

HILDEBRANDT, Mireille. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar Publishing, 2015.

IEEE. (2020). Ethical Issues Related to Data Privacy and Security: Why We Must Balance Ethical and Legal Requirements in the Connected World. IEEE Digital Privacy.

JAGADISH, H. V., et al. Big data and its technical challenges. Communications of the ACM, v. 57, n. 7, p. 86-94, 2014.

LANEY, D. 3D Data Management: Controlling Data Volume, Velocity, and Variety. META Group, 2001.

KUNER, Christopher. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013.

KVALE, Steinar. Doing Interviews. London: SAGE Publications, 2007.

MARR, B. Big Data: Using SMART Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance. John Wiley & Sons, 2015.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013.

MDPI. (2020). Big Data Privacy and Ethical Challenges. MDPI.

MILES, Matthew B.; HUBERMAN, A. Michael; SALDAÑA, Johnny. Qualitative Data Analysis: A Methods Sourcebook. 3. ed. Thousand Oaks: SAGE Publications, 2014.

MITTELSTADT, Brent D.; FLORIDI, Luciano. The ethics of big data: current and foreseeable issues in biomedical contexts. Science and engineering ethics, v. 22, n. 2, p. 303-341, 2016.

NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

PLOS ONE. (2021). Ethical issues in big data: A qualitative study

comparing responses in the health and higher education sectors.

RAGHUPATHI, W., RAGHUPATHI, V. Big data analytics in healthcare: promise and potential. Health Information Science and Systems, v. 2, n. 1, p. 3, 2014.

RICHARDS, N. M., & KING, J. H. (2014). Big Data Ethics. Wake Forest Law Review, 49.

SAGIROGLU, S., SINANC, D. Big data: A review. In: 2013 International Conference on Collaboration Technologies and Systems (CTS). IEEE, 2013. p. 42-47.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. New York University Law Review, v. 86, p. 1814-1894, 2011.

SENADO FEDERAL. (2018). Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709).

SOLOVE, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. Harvard Law Review, 126, 1880-1903.

TENE, O., & POLONETSKY, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology and Intellectual Property, 239-273.

VAYENA, E., GASSER, U., WOOD, A. B., O'BRIEN, D., & ALTMAN, M. (2016). "Elements of a New Ethical Framework for Big Data Research." Washington and Lee Law Review Online, 72(3).

VOIGT, Paul; VON DEM BUSSCHE, Axel. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer International Publishing, 2017.

WEDEL, M., KANNAN, P. K. Marketing Analytics for Data-Rich Environments. Journal of Marketing, v. 80, n. 6, p. 97-121, 2016.

ZHANG, Y., et al. Big data security and privacy protection. In: 2015 IEEE International Congress on Big Data. IEEE, 2015. p. 318-326.

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

ZWITTER, A. (2014). Big Data ethics. Big Data & Society, 1(2).