Privacidade na era do 5G: problemas, princípios da LGPD e impactos sociais

Gabriela S. Lima[1], **Jeisa P. O. Domingues**[1], **Fernando A. A. Lins**[1]

[1]Departamento de Computação – Universidade Federal Rural de Pernambuco (UFRPE)
52.171-900 – Recife – PE – Brasil

{gabriela.slima,jeisa.domingues,fernandoaires}@ufrpe.br

Abstract. *With the arrival of 5G, in addition to the expansion and improvement of connectivity, new challenges related to the security of user information arise. In view of this, this article investigates the implications of 5G technology for privacy, examining its compliance with the principles established by the General Data Protection Law (LGPD). To this end, an ad hoc review was carried out that mapped and classified the main problems into three distinct categories. These categories were then analyzed to identify possible violations of the LGPD principles and their implications for different segments of society, especially those most vulnerable to data exposure.*

Resumo. *Com a chegada do 5G, além da ampliação e melhoria da conectividade, surgem novos desafios relacionados à segurança das informações dos usuários. Diante disso, este artigo investiga as implicações da tecnologia 5G para a privacidade, examinando sua conformidade com os princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Para tanto, foi realizada uma revisão ad hoc que mapeou e classificou os principais problemas em três categorias distintas. Em seguida, essas categorias foram analisadas para identificar possíveis infrações aos princípios da LGPD e suas implicações para diferentes segmentos da sociedade, especialmente aqueles mais vulneráveis à exposição de dados.*

1. Introdução

A crescente digitalização da sociedade tem intensificado os desafios relacionados à privacidade dos usuários à medida que um volume cada vez maior de dados pessoais é coletado, armazenado e compartilhado por empresas e plataformas digitais. Em 2024, mais de 5,5 bilhões de contas foram comprometidas, quase oito vezes o número registrado no ano anterior [Surfshark 2024], evidenciando a necessidade de uma análise crítica sobre as práticas de coleta e uso de informações pessoais.

Dentre os modelos adotados para regulamentar a privacidade digital, destaca-se o *notice & choice* (aviso e escolha), no qual os usuários devem consentir com o fornecimento de seus dados. No entanto, esse consentimento é frequentemente obtido de forma pouco transparente, tornando os dados uma moeda de troca para compartilhamento ou comercialização com terceiros [Khajuria and Skouby 2017]. Nesse contexto, as opções dos usuários se restringem a aceitar integralmente os termos impostos ou renunciar ao serviço desejado.

A tecnologia de comunicação 5G foi projetada para expandir os cenários de interação, conectando pessoas e máquinas independentemente de local, horário ou dispositivo utilizado [Wang et al. 2014]. Entretanto, essa ampla conectividade pode demandar o envolvimento de provedores de rede localizados em diferentes jurisdições [Rizou et al. 2020], trazendo desafios significativos à privacidade de dados, considerando a complexidade das regulamentações entre essas regiões.

Para mitigar práticas abusivas de captura e uso indevido de dados sensíveis, diversos países implementaram legislações específicas voltadas à proteção da privacidade e à regulamentação do tratamento dessas informações. A União Europeia (UE) estabeleceu a *General Data Protection Regulation* (GDPR), criada em 2016 e implementada em 2018, definindo diretrizes sobre o processamento de dados pessoais por instituições, órgãos e empresas, incluindo aquelas sediadas fora da UE que lidam com informações de indivíduos dentro do bloco econômico [GDPR-info.eu 2018]. No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi criada com o objetivo de preservar o direito fundamental à privacidade, estabelecendo regras para o tratamento de dados pessoais coletados em território nacional ou em operações que envolvam indivíduos localizados no Brasil. Inspirada na GDPR, a legislação brasileira impõe exigências de transparência e segurança no uso das informações, conferindo aos titulares maior controle sobre seus dados e estabelecendo responsabilidades claras para os agentes de tratamento [da República do Brasil 2018].

Por esse motivo, a implementação do 5G chamou a atenção dentro da UE em 2019, onde o Conselho da União Europeia fez um documento discutindo sobre os possíveis desafios com foco na aplicação das leis e perspectiva judicial. Vale ressaltar a crescente dificuldade para as autoridades judiciais interceptarem comunicações legais por conta dos altos níveis de segurança oferecidos pelo 5G [Statewatch 2019].

No meio de tudo isso, grupos que já dispunham de menos acesso ou necessitam diretamente da tutela de outras pessoas estão mais vulneráveis a esse tipo de risco, uma vez que podem ter dificuldades adicionais na compreensão e no exercício de seus direitos sobre os próprios dados. Crianças e indivíduos de baixa alfabetização, por exemplo, estão mais sujeitos a consentir com termos pouco transparentes ou a fornecer informações sensíveis sem plena consciência das consequências. Essa vulnerabilidade reforça a necessidade de regulamentações mais robustas, mecanismos de fiscalização eficientes e iniciativas de educação digital que promovam maior autonomia e proteção para esses grupos diante das dinâmicas do uso e comercialização de dados pessoais.

Diante desse cenário, torna-se essencial compreender os riscos à privacidade intensificados com a adoção da 5G. Nesse contexto, é fundamental analisar de que forma esses desafios se relacionam com os princípios estabelecidos na LGPD, identificando lacunas na legislação para mapear possíveis riscos à segurança e ao controle dos dados dos cidadãos em um ambiente cada vez mais interconectado.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta os conceitos básicos; na Seção 3, são discutidos os trabalhos relacionados; o processo metodológico utilizado é detalhado na Seção 4; a Seção 5 apresenta os resultados gerais obtidos; na Seção 6, são discutidas as implicações diretas para alguns grupos sociais; e a Seção 7 aborda possíveis trabalhos futuros e as considerações finais.

2. Conceitos básicos

Para facilitar a compreensão deste trabalho, serão apresentadas, nesta seção, informações básicas sobre a tecnologia 5G e a Lei Geral de Proteção de Dados Pessoais (LGPD).

2.1. Tecnologia 5G

De forma simplificada, a arquitetura da rede 5G consiste em: dispositivos celulares (como *smartphones* e *tablets*) cuja conectividade contínua é garantida por uma enorme quantidade de macrocélulas e microcélulas, formadas por estações rádio-base (ERBs) e *hotspots*; e um núcleo composto por roteadores e *gateways*, que recebem e transmitem os dados desses dispositivos de/para a conexão final com a Internet, que pode ocorrer por meio de servidores, *data centers* ou infraestruturas de nuvem [Sicari et al. 2020]. Assim, existem diversos envolvidos durante o processo de transmissão de dados por meio do 5G.

Outro ponto importante a ser considerado na acentuação dos problemas de privacidade é que, em comparação com as tecnologias de comunicação anteriores, o 5G trouxe avanços significativos, como taxas de transferência de dados mais altas, redução da latência, maior densidade de tráfego e suporte para conexões com um número maior de dispositivos. Por este motivo, o 5G tem contribuído para o aumento da quantidade de dispositivos conectados e, consequentemente, para o volume de dados transmitidos [Dangi et al. 2021].

2.2. Lei Geral de Proteção de Dados Pessoais - LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que regula o tratamento de dados pessoais, visando garantir a privacidade, transparência e segurança das informações. Sua implementação enfrenta desafios como a baixa cultura de proteção de dados, a adaptação de empresas de diferentes portes e setores, e a necessidade de fiscalização efetiva. Além disso, há dificuldades em equilibrar a proteção de dados com a inovação tecnológica e o uso intensivo de informações em ambientes digitais [Belarmino et al. 2024].

De acordo com o art. 6º da LGPD [da República do Brasil 2018], o tratamento dos dados pessoais deve ser regido pelos 10 princípios a seguir:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3. Trabalhos Relacionados

No âmbito da LGPD, encontra-se o artigo [Oliveira et al. 2021], que aborda a definição de princípio no contexto jurídico, além de apresentar os objetivos da lei, as definições de dados pessoais e os âmbitos de sua aplicação. Adicionalmente, os autores examinam cada um dos dez princípios que compõem a LGPD, utilizando diversas fontes para aprofundar as discussões sobre cada um deles.

Liyanage et al. (2018) apresenta algumas das inovações tecnológicas introduzidas pelo 5G. Sem abordar diretamente a legislação, o artigo propõe sugestões de possíveis soluções para os problemas de privacidade identificados, explorando diferentes estratégias, dentre as quais de destacam uma abordagem regulatória e outra baseada no conceito de *Privacy by Design*.

O artigo de [Rizou et al. 2020] é o que forneceu um maior embasamento para esse trabalho. Nele, os autores discutem os sete princípios do tratamento de dados estabelecidos pela GDPR, destacando os direitos e deveres previstos na legislação. Além disso, analisam como os avanços tecnológicos viabilizados pelo 5G podem conflitar com esses direitos e deveres. O estudo também investiga os problemas de segurança decorrentes da adoção do 5G e apresenta possíveis soluções à luz da GDPR.

Com a análise dos trabalhos relacionados, evidencia-se a necessidade de um estudo que não apenas mapeie os problemas de privacidade intensificados pelo 5G, mas também os compare aos princípios da LGPD, a fim de identificar quais podem ser infringidos e contextualizar a questão social do Brasil.

4. Metodologia

A metodologia utilizada no desenvolvimento nesse trabalho está ilustrada na Figura 1. O protocolo utilizado foi uma revisão ad hoc da literatura.

A pesquisa teve como critério a seleção de artigos que tratassem da privacidade no contexto da tecnologia 5G. Inicialmente, foram coletados cerca de 60 artigos que, em um primeiro momento, pareciam atender a esse critério. No entanto, uma análise mais aprofundada revelou que muitos desses estudos mencionavam privacidade, mas sem abordar

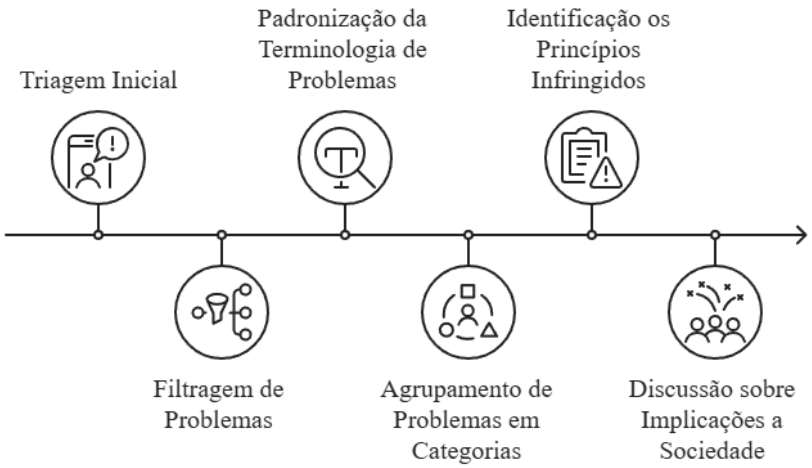

Figura 1. Processo Metodológico

especificamente os problemas introduzidos ou agravados pelo 5G. Como resultado, apenas 12% dos artigos inicialmente coletados foram considerados realmente relevantes, pois analisavam diretamente os problemas de privacidade acentuados pela 5G, sendo esses os selecionados para continuidade da pesquisa.

Em seguida, os problemas de privacidade abordados nos artigos selecionados foram organizados em uma planilha, juntamente com seus nomes originais e descrições. Após a leitura completa dos artigos, foram coletados 37 problemas no total. No entanto, ao analisar suas definições, identificou-se uma alta similaridade entre as descrições fornecidas pelos diferentes autores. Desta forma, para evitar a repetição de ideias com nomes diferentes, os 37 problemas foram condensados em 16 problemas distintos, sendo eles:

Ambiente Compartilhado (*Shared Environment*): compartilhamento de infraestrutura com terceiros pode facilitar acessos não autorizados [Liyanage et al. 2018], [Ahmad et al. 2017], [Arfaoui et al. 2018], [Khan et al. 2019], [Teatini and Matinmikko-Blue 2021], [Ahmad et al. 2019];

Confidencialidade de Dados Fim a Fim (*End to end (E2E) data confidentiality*): dificuldade em garantir a confidencialidade fim-a-fim aumenta devido à participação da grande quantidade de envolvidos no processo [Liyanage et al. 2018], [Khan et al. 2019];

Confidencialidade de Dados (*Data Confidentiality*): os envolvidos nos processos de transmissão devem firmar acordos de confidencialidade para prevenir acessos não autorizados e proteger os dados transmitidos [Teatini and Matinmikko-Blue 2021];

Privacidade de IoT (*IoT Privacy*): a segurança de dados raramente é priorizada durante o design de dispositivos IoT, o que aumenta os riscos de vulnerabilidades e invasões [Liyanage et al. 2018];

Gerenciamento de Identidades (*Managing identities*): o grande volume de identidades transmitidas aumenta o risco de que qualquer erro exponha informações pessoais do usuário [Ahmad et al. 2019];

Ausência de Barreiras Físicas (*No physical boundaries*): a ausência de barreiras físicas entre os inquilinos torna a segurança dependente dos regulamentos e

normas implementados por terceiros, elevando os riscos de acessos não autorizados [Ahmad et al. 2017];

Hacking: ocorre quando há acesso não autorizado aos dados, resultando em riscos à segurança e à privacidade dos dados [Liyanage et al. 2018], [Teatini and Matinmikko-Blue 2021];

Perda de Visibilidade (*Loss of Visibility*): perda de visibilidade das medidas de privacidade e segurança, dificultando o controle total sobre a proteção de dados [Liyanage et al. 2018], [Teatini and Matinmikko-Blue 2021];

Atores Diferentes (*Different Actors*): a grande quantidade de atores envolvidos aumenta as chances de conflitos entre os diferentes objetivos e leis aplicáveis, elevando os riscos à privacidade [Ahmad et al. 2017], [Ahmad et al. 2019];

Diferentes Objetivos para a Confiança (*Different objectives for trust*): a diferença nos objetivos e níveis de confiança entre os envolvidos aumenta os riscos e conflitos durante os processos de transmissão de dados [Liyanage et al. 2018], [Arfaoui et al. 2018], [Khan et al. 2019], [Teatini and Matinmikko-Blue 2021];

Perda da Propriedade dos Dados (*Loss of Data ownership*): o titular dos dados perde todos os direitos sobre eles, e o novo proprietário, um terceiro, pode utilizá-los livremente [Liyanage et al. 2018], [Ahmad et al. 2017], [Khan et al. 2019], [Ahmad et al. 2019];

Fluxo Transfronteiriço de Dados (*Trans-border data flow*): diferenças nas leis de privacidade de cada país pode gerar problemas durante transmissão, tratamento e armazenamento em diferentes jurisdições [Liyanage et al. 2018], [Ahmad et al. 2017], [Khan et al. 2019], [Ortiz et al. 2020], [Teatini and Matinmikko-Blue 2021], [Ahmad et al. 2019];

Fornecimento de Informações para Terceiros (*Providing information for third party*): refere-se ao compartilhamento ou venda dos dados do usuário, expondo informações pessoais para utilização por terceiros [Liyanage et al. 2018], [Khan et al. 2019];

Conflito de Estatutos (*Bylaw conflict*): em caso de crime, surge a dúvida sobre qual lei será aplicada—do país onde o crime foi cometido, da origem dos dados, do local de armazenamento ou do país destino dos dado [Liyanage et al. 2018];

Propriedade de Dados (*Data Ownership*): a ausência de parâmetros claros para definir o proprietário dos dados dificulta a proteção e o controle efetivo sobre as informações pessoais [Teatini and Matinmikko-Blue 2021];

Agências de Segurança (*Security Agencies*): refere-se à coleta e ao processamento de dados por empresas de segurança pública, levantando preocupações quanto à privacidade e ao uso ético das informações coletadas [Teatini and Matinmikko-Blue 2021];

O mapeamento dos nomes originais em inglês, nomes traduzidos e os artigos em que cada problema foi detectado pode ser encontrado no link [https://encurtador.com.br/fqWoa].

Posteriormente, os 16 problemas distintos de privacidade foram classificados de acordo com suas características, resultando nas três categorias abaixo:

1. Legislação: Os problemas causados por questões legais, seja devido às diferenças nas leis de privacidade dos países ou pela ausência delas, foram agrupados nesta categoria.
2. Confiança: Qualquer problema que ocorra quando há o risco de uma quebra na confiança entre os envolvidos no processo de transmissão de dados via 5G foi associado a esta categoria.
3. Segurança: Os problemas decorrentes de possíveis falhas na segurança envolvendo acessos não autorizados aos dados, tanto os armazenados quanto os em movimento, foram colocados nesta categoria.

A Tabela 1 apresenta a categorização final dos 16 problemas encontrados:

Categoria	**Problema**
Legislação	Fluxo Transfronteiriço de Dados
	Conflito de Estatutos
	Propriedade de Dados
Confiança	Ambiente Compartilhado
	Perda da Propriedade dos Dados
	Diferentes Objetivos para a Confiança
	Atores Diferentes
	Fornecimento de Informações para Terceiros
Segurança	Confidencialidade de Dados Fim a Fim
	Perda de Visibilidade
	Hacking
	Ausência de Barreiras Físicas
	Gerenciamento de Identidades
	Privacidade de IoT
	Confidencialidade de Dados
	Agências de Segurança

Tabela 1. Categorização dos problemas

É importante destacar que determinados problemas podem ser classificados tanto na categoria de Confiança quanto na de Segurança, dependendo da interpretação adotada. Um exemplo disso são os casos de Ambiente Compartilhado e Ausência de Barreiras Físicas, que possuem descrições semelhantes, mas se enquadram em categorias distintas.

No caso do Ambiente Compartilhado, a preocupação central está na confiança de que outros inquilinos ou até mesmo o proprietário da infraestrutura não tentarão acessar os dados, mesmo na ausência de uma barreira física que os separe. Por outro lado, a categoria Ausência de Barreiras Físicas trata especificamente da inexistência de uma separação física capaz de fornecer segurança adicional. Essa ausência de barreira física aumenta significativamente o risco de acessos não autorizados.

Em seguida, as categorias foram analisadas, com a identificação dos princípios possivelmente infringidos por cada uma delas. Além disso, foi realizada uma discussão

considerando dois grupos sociais, identificados como mais propensos aos riscos de privacidade examinados.

5. Resultados

A seção de resultados foi estruturada em três subseções, cada uma dedicada a apresentar uma das categorias mapeadas. Em cada subseção, são descritos alguns dos problemas de privacidade mais característicos da respectiva categoria, acompanhados da justificativa sobre como esses problemas podem ser agravados com a implementação do 5G. Além disso, discute-se quais princípios da LGPD apresentam maior risco de violação em cada categoria.

É importante destacar que nem todos os problemas foram descritos e discutidos nas subseções seguintes, pois o foco está nos problemas mais representativos e amplamente reconhecidos dentro de cada categoria, permitindo uma melhor relação com a LGPD.

5.1. Legislação

Nesta seção estão todos os problemas que se enquadram na categoria de legislação, ou seja, desafios que surgem devido às diferenças nas leis de proteção de dados entre países ou, em alguns casos, à ausência de regulamentações específicas de privacidade. Os problemas que foram identificados nesta categoria estão: Fluxo Transfronteiriço de Dados, Conflito de Estatutos e Propriedade de Dados.

Com o aumento do número de dispositivos conectados e da quantidade de dados transmitidos devido aos avanços do 5G, questões relacionadas ao armazenamento, tratamento e transferência de dados entre países tornaram-se um desafio, especialmente por conta das distintas legislações de privacidade digital. Dessa forma, é possível que um dado seja transmitido ou armazenado em um país onde ele é considerado sensível ou até mesmo ilegal, enquanto, em seu país de origem, o mesmo dado pode ser perfeitamente legal e não sensível [Liyanage et al. 2018].

Outro aspecto relevante dessa categoria é que, em casos de crimes ou vazamentos, surge a questão de qual legislação deveria ser aplicada. Entre as possibilidades, podem ser consideradas a lei do país de origem do dado, a lei de onde o crime foi perpetrado, como também a lei do país onde os dados estavam armazenados. Além disso, em situações de vazamentos de grande escala, que envolvem dados provenientes de múltiplos países, a complexidade legal torna-se ainda maior, dificultando a aplicação de respostas específicas para cada dado de forma diferenciada [Liyanage et al. 2018].

Considerando todos esses pontos, é possível inferir que o princípio mais impactado pelos problemas relacionados à Legislação seja o de Responsabilização e Prestação de Contas. Este princípio enfatiza a necessidade da "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." [da República do Brasil 2018].

5.2. Confiança

Os problemas de privacidade decorrentes da falta ou quebra de confiança entre os envolvidos em uma transmissão de dados via 5G foram agrupados na categoria de Confiança.

Seja pelo aumento da quantidade de dados armazenados em ambientes compartilhados por terceiros ou pelo crescimento do número de atores necessários para a realização do processo de comunicação, o 5G evidenciou ainda mais a importância da confiança entre todos os envolvidos. Essa dinâmica também ampliou os riscos associados à falta de uma relação de confiança no processo [Arfaoui et al. 2018].

Um exemplo prático dos problemas que podem surgir devido à falta de confiança entre os atores ocorre quando um cliente precisa realizar a transmissão de dados utilizando o 5G para acessar determinado serviço. Geralmente, seus dados percorrem diferentes operadores e torres até chegar ao destino final, o que aumenta o risco de que algum dos envolvidos possa utilizar, armazenar ou até mesmo vender esses dados [Ahmad et al. 2019]. Com o aumento das conexões promovido pelo 5G, a probabilidade de tais problemas ocorrerem é ainda maior. Assim, a governança e a segurança se tornam responsabilidades compartilhadas entre os atores em um acordo de confiança.

Além disso, o uso compartilhado de infraestrutura de terceiros, como ambientes em nuvem, limita a barreira de proteção física ao proprietário da infraestrutura e elimina essa proteção entre os inquilinos [Ahmad et al. 2017]. A depender de como a segurança digital é organizada pelo proprietário, há o risco de facilitar ainda mais um possível acesso não autorizado aos dados que estão em trânsito ou armazenados [Teatini and Matinmikko-Blue 2021].

Considerando que o principal objetivo do usuário ao transmitir seus dados é a utilização de um serviço ou a realização de uma comunicação, o tratamento, compartilhamento ou venda desses dados por terceiros envolvidos no processo pode não ter sido explicitamente informado. Dessa forma, o princípio de Finalidade seria comprometido, uma vez que este não permite o tratamento posterior de forma incompatível com as finalidades originalmente estabelecidas [da República do Brasil 2018].

O princípio de Adequação, por ser complementar ao de Finalidade, também se encaixaria, por deixar claro que é essencial que haja "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" [da República do Brasil 2018].

5.3. Segurança

Os problemas de privacidade associados aos riscos na segurança dos dados durante e após as transferências via 5G estão destacados nesta seção.

Com o aumento do número de dispositivos conectados à Internet das Coisas (IoT) viabilizado pelo 5G, surgem preocupações significativas quanto à privacidade dos dados, especialmente considerando que, em geral, esses dispositivos não são projetados com foco em segurança e privacidade. Além disso, caso sejam comprometidos, esses dispositivos podem ter seus dados capturados e até utilizados para ataques de negação de serviço (denominado de *Denial of Service* – DoS) [Liyanage et al. 2018].

O *hacking* é um dos problemas de privacidade e segurança com maior visibilidade na atualidade, caracterizando-se pelo acesso não autorizado a redes e/ou computadores [Teatini and Matinmikko-Blue 2021]. Com o avanço do 5G, esse problema é agravado devido ao aumento do uso de ambientes em nuvem, assim como de ataques baseados em *web* e IP [Liyanage et al. 2018]. Entre os principais riscos associados ao *hacking*

estão a alteração e/ou o download desses dados. A alteração compromete diretamente a qualidade e a precisão das informações. Um exemplo prático seria a alteração do CPF de um usuário, uma vez que esse dado é uma identidade única de cada cidadão brasileiro. Essa modificação poderia acarretar grandes implicações, como a associação da conta do usuário a outra conta, a impossibilidade de acessar serviços governamentais, entre outros prejuízos potenciais.

Por outro lado, o download de dados resulta na perda da propriedade sobre essas informações, impossibilitando prever ou controlar os fins para os quais serão utilizadas, podendo até mesmo serem empregadas em atividades ilegais.

Devido à maior capacidade de conexão de dispositivos e pessoas proporcionada pelo 5G, o volume de identidades transmitidas alcança níveis elevados. Assim, qualquer falha durante essas transmissões pode expor a identidade e informações pessoais dos usuários [Ahmad et al. 2019].

No âmbito da categoria de segurança, destacam-se três princípios que podem ser infringidos: Qualidade dos Dados, Segurança e Prevenção.

O princípio da Qualidade dos Dados pode ser comprometido, pois precisa existir a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento"[da República do Brasil 2018].

Outro princípio suscetível à violação é o da Segurança, que exige a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[da República do Brasil 2018].

Por fim, há o princípio da Prevenção, que consiste na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais"[da República do Brasil 2018].

6. Implicações Práticas à Sociedade

A implementação do 5G no Brasil tem o potencial de ampliar significativamente o acesso à Internet [Agência Nacional de Telecomunicações (Anatel) 2025], possibilitando um cenário que abrange tanto aqueles que não possuíam acesso devido a limitações das tecnologias de comunicação anteriores quanto crianças em seus primeiros anos de vida. No entanto, essa expansão também traz novos desafios, especialmente para a população analfabeta, que pode se tornar mais vulnerável devido à falta de familiaridade com tecnologias digitais. Essa vulnerabilidade é ainda mais acentuada em comunidades rurais [Instituto Brasileiro de Geografia e Estatística (IBGE) 2025], onde as infraestruturas de comunicação anteriores não eram suficientes para atender a esse grupo populacional.

6.1. A conectividade 5G sob a perspectiva dos analfabetos

O aumento da conectividade promovido pela implementação do 5G no Brasil tem o potencial de levar mais brasileiros à Internet, incluindo aqueles que estarão acessando a rede pela primeira vez [Agência Nacional de Telecomunicações (Anatel) 2025]. Contudo, essa expansão apresenta novos desafios, especialmente para a população analfabeta do país, que pode se encontrar em situação de maior vulnerabilidade.

Conforme o Censo Demográfico de 2022, verificou-se que 7% da população brasileira com 15 anos ou mais era analfabeta. Embora essa porcentagem esteja em declínio, ela ainda representa 11,4 milhões de brasileiros incapazes de ler ou escrever um bilhete simples [Instituto Brasileiro de Geografia e Estatística (IBGE) 2025].

Um dos desafios enfrentados por indivíduos analfabetos é a preservação da privacidade no ambiente digital. Isso se torna particularmente relevante porque os termos de privacidade de serviços e aplicativos frequentemente explicam, de forma detalhada, quais acessos são concedidos e como os dados coletados podem ser utilizados. No entanto, para este grupo específico de indivíduos, é provável que tais termos sejam aceitos sem a compreensão adequada de seu verdadeiro significado.

Essa situação cria lacunas para que empresas utilizem esses dados de forma antiética, como compartilhá-los com terceiros, coletar informações adicionais ou mesmo realizar tratamentos de dados que vão além do necessário. Apesar de tais práticas estarem conforme a legislação de privacidade vigente, baseando-se em um consentimento formal, são altamente questionáveis do ponto de vista ético devido à falta de entendimento por parte do usuário.

6.2. Desafios do controle parental de privacidade infantil na era do IoT e anúncios personalizados

Com suas conexões de alta velocidade e a capacidade de integrar um número ainda maior de dispositivos IoT, como *smartwatches*, brinquedos conectados e assistentes virtuais como *Alexa* e *Google Home*, o 5G possibilita a coleta contínua e em larga escala de dados. Esse avanço, embora traga benefícios em termos de conectividade e automação, também amplia significativamente os riscos à privacidade. Uma quantidade massiva de informações pessoais pode ser registrada sem que as crianças ou seus responsáveis tenham plena consciência do que está sendo coletado, como está sendo armazenado ou com quem está sendo compartilhado [Chu et al. 2018].

Esse cenário torna ainda mais desafiador o controle parental [Assis and Valença 2024], uma vez que os responsáveis podem não possuir as ferramentas ou o conhecimento necessário para gerenciar adequadamente os fluxos de dados gerados por esses dispositivos. Além disso, a interconectividade promovida pelo 5G pode dificultar a aplicação de medidas de segurança eficazes, permitindo que informações sensíveis sejam expostas a terceiros, intencionalmente ou não.

Apesar de a LGPD estabelecer diretrizes específicas para a proteção de dados pessoais de crianças e adolescentes [da República do Brasil 2018], a implementação dessas normas enfrenta desafios significativos. A transferência e o armazenamento de dados em diferentes países podem dificultar a aplicação da legislação nacional, expondo essas informações a regulamentações menos rígidas. Além disso, a falta de transparência na coleta e no processamento desses dados impede que os responsáveis legais compreendam plenamente quais informações estão sendo registradas e como são utilizadas. Essa opacidade, somada à dificuldade de monitorar as atividades das crianças em múltiplas plataformas e aplicativos, compromete a efetividade do controle parental e aumenta o risco de violações à privacidade.

A coleta massiva desses dados permite a criação de perfis detalhados sobre crianças, viabilizando a segmentação de anúncios altamente personalizados

[Smith and Shade 2018]. Essa prática pode estimular o consumo excessivo e influenciar hábitos de maneira invasiva, levando a impactos que vão além da esfera econômica, podendo até resultar em manipulação comportamental.

7. Conclusão

Ao final da análise dos problemas de privacidade intensificados pela tecnologia 5G, compreende-se que, embora a LGPD estabeleça princípios a serem seguidos, ela, por si só, não impede a ocorrência de problemas durante o uso da tecnologia. Afinal, a LGPD é uma legislação orientada a mitigar infrações relacionadas à quebra dos direitos de privacidade digital dos cidadãos, servindo como uma ferramenta instrutiva que, caso não seja seguida, assume um caráter punitivo.

Com suas leis que regulamentam o uso, tratamento e armazenamento de dados, a LGPD obriga as empresas a adotarem práticas de maior cuidado na gestão das informações pessoais, reduzindo as chances de uso inadequado, como compartilhamentos ou tratamentos incompatíveis com os serviços oferecidos. Nesse contexto, a categoria de confiança é a que apresenta mais problemas mitigados. Por outro lado, a categoria com uma maior quantidade de problemas, intensificados pela 5G, é a de segurança, devido aos problemas de privacidade relacionados a invasões mal-intencionadas, que comprometem a exatidão e a propriedade dos dados. O aumento de dispositivos IoT, vulneráveis a ataques e invasões, combinado à maior complexidade existente no processo de transmissão da 5G, torna a proteção da confidencialidade dos dados ainda mais desafiadora.

Conforme discutido, crianças e analfabetos estão entre os grupos sociais mais vulneráveis aos problemas de privacidade no mundo digital. Esses indivíduos estão sendo inseridos em um ambiente altamente conectado para o qual não estão amplamente preparados. No caso das crianças, é necessário um acompanhamento parental mais rigoroso para assegurar sua proteção. Já os analfabetos dependem de um suporte mais abrangente e eficaz por parte de iniciativas públicas, a fim de garantir que possam ser incluídos de forma mais segura no ambiente digital.

Este trabalho enfrentou algumas limitações, como a falta de artigos que estabelecem uma relação entre os problemas de privacidade com a implementação da 5G no Brasil. Um outro fator limitador foi a ambiguidade de como determinados problemas de privacidade seriam abordados pela LGPD. Além disso, por utilizar uma revisão ad hoc, é possível que nem todos os artigos e problemas relevantes as categorias possam ter sido mapeados.

Com isso, este trabalho tem como objetivo introduzir novos caminhos para estudos científicos, possibilitando uma pesquisa mais aprofundada sobre os impactos gerados pelas novas tecnologias nos grupos sociais mais vulneráveis, bem como alertar as empresas sobre os possíveis riscos de infringir os princípios da LGPD ao utilizar a tecnologia 5G.

Para trabalhos futuros, é possível explorar duas direções distintas. A primeira consiste em um estudo aprofundado sobre os potenciais riscos à privacidade de crianças com o uso de brinquedos inteligentes, analisando como esses dispositivos coletam, armazenam e compartilham dados sensíveis. A segunda envolve o mapeamento dos impactos da implementação da 5G em comunidades isoladas no Brasil, especialmente aquelas que, até então, não eram atendidas anteriormente por outros protocolos de comunicação.

Referências

Agência Nacional de Telecomunicações (Anatel) (2025). 5g completa dois anos de implantação no brasil. Acesso em: 15 mar. 2025.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., and Gurtov, A. (2017). 5g security: Analysis of threats and solutions. In *2017 IEEE conference on standards for communications and networking (CSCN)*, pages 193–199. IEEE.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., and Ylianttila, M. (2019). Security for 5g and beyond. *IEEE Communications Surveys & Tutorials*, 21(4):3682–3722.

Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Félix, E., Klaedtke, F., Nakarmi, P. K., Näslund, M., O'Hanlon, P., et al. (2018). A security architecture for 5g networks. *IEEE access*, 6:22466–22479.

Assis, J. V. and Valença, G. (2024). Is my child safe online?-on requirements for parental control tools in apps used by children. *Journal on Interactive Systems*, 15(1):823–838.

Belarmino, G. d. S., Ricarte, D. R., and Motta, G. H. (2024). A lei geral de proteção de dados do brasil à luz do regimento europeu: Um exame comparativo e prospectivo através de uma revisão sistemática. In *Workshop sobre as Implicações da Computação na Sociedade (WICS)*, pages 70–79. SBC.

Chu, G., Apthorpe, N., and Feamster, N. (2018). Security and privacy analyses of internet of things children's toys. *IEEE Internet of Things Journal*, 6(1):978–985.

da República do Brasil, P. (2018). Lei nº 13.709, de 14 de agosto de 2018 - lei geral de proteção de dados pessoais (lgpd). `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`. Acesso em: 14 mar. 2025.

Dangi, R., Lalwani, P., Choudhary, G., You, I., and Pau, G. (2021). Study and investigation on 5g technology: A systematic review. *Sensors*, 22(1):26.

GDPR-info.eu (2018). General data protection regulation (gdpr). `https://gdpr-info.eu/`. Acesso em: 14 mar. 2025.

Instituto Brasileiro de Geografia e Estatística (IBGE) (2025). Alfabetização. Acesso em: 15 mar. 2025.

Khajuria, S. and Skouby, K. E. (2017). Privacy and economics in a 5g environment. *Wireless Personal Communications*, 95:145–154.

Khan, R., Kumar, P., Jayakody, D. N. K., and Liyanage, M. (2019). A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, 22(1):196–248.

Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., and Ylianttila, M. (2018). 5g privacy: Scenarios and solutions. In *2018 IEEE 5G World Forum (5GWF)*, pages 197–203. IEEE.

Oliveira, A. C. R., da Cruz Ferreira, H., and Pires, F. I. (2021). Princípios da lei geral de proteção de dados (lgpd). *Seara Jurídica*, 1(19):1–12.

Ortiz, J., Fernández, P. J., Sanchez-Iborra, R., Bernabe, J. B., Santa, J., and Skarmeta, A. (2020). Enforcing gdpr regulation to vehicular 5g communications using edge virtual counterparts. In *2020 IEEE 3rd 5G World Forum (5GWF)*, pages 121–126. IEEE.

Rizou, S., Alexandropoulou-Egyptiadou, E., and Psannis, K. E. (2020). Gdpr interference with next generation 5g and iot networks. *Ieee Access*, 8:108052–108061.

Sicari, S., Rizzardi, A., and Coen-Porisini, A. (2020). 5g in the internet of things era: An overview on security and privacy challenges. *Computer Networks*, 179:107345.

Smith, K. L. and Shade, L. R. (2018). Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture. *Big Data & Society*, 5(2):2053951718805214.

Statewatch (2019). Eu council ctc 5g law enforcement document 8983/19. `https://www.statewatch.org/media/documents/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf`. Acesso em: 14 mar. 2025.

Surfshark (2024). Data breach recap 2024. `https://surfshark.com/research/study/data-breach-recap-2024`. Acesso em: 14 mar. 2025.

Teatini, S. and Matinmikko-Blue, M. (2021). Privacy in the 5g world: The gdpr in a datafied society. *The Wiley 5G REF: Security*.

Wang, C.-X., Haider, F., Gao, X., You, X.-H., Yang, Y., Yuan, D., Aggoune, H. M., Haas, H., Fletcher, S., and Hepsaydir, E. (2014). Cellular architecture and key technologies for 5g wireless communication networks. *IEEE communications magazine*, 52(2):122–130.