A segurança de dados na tecnologia 6G: proposta de framework conceitual em conformidade com a Lei Geral de Proteção de Dados

Claudio Marcio Oliveira
Mackenzie Presbyterian University
São Paulo, Brazil
claudiomarcio.13@outlook.com

Eduardo Fernando de Oliveira
Mackenzie Presbyterian University
São Paulo, Brazil
eduardo.dobarce@gmail.com

Everton Knihs
Mackenzie Presbyterian University
São Paulo, Brazil
tomspsp@gmail.com

Ismar Frango Silveira
Mackenzie Presbyterian University
São Paulo, Brazil
ismarfrango@gmail.com

Abstract—This work seeks to understand what to expect after the era of 5G data transmission technology. 6G technology will arrive, still under study, but which will determine a greater speed of data transmission and a new evolutionary form of technological capabilities. Therefore, this work seeks to collect information and analyze the characteristics of data transmission by 6G technology related to security, and thus, identify vulnerabilities and transparency of data transmitted in accordance with the Brazilian General Data Protection Law. Due to the increase in data transmission through 6G technology, vulnerabilities may arise that put the transmitted data at risk and that do not meet the requirements found in national legislation on the protection of personal data.

Keywords—6G, Data transmission, Vulnerabilities, data protection

.

Resumo— Este trabalho busca compreender o que esperar após a era da tecnologia de transmissão de dados 5G. Chegará a tecnologia 6G, ainda em estudo, mas que determinará uma maior velocidade de transmissão de dados e uma nova forma evolutiva das capacidades tecnológicas, dessa forma, este trabalho busca levantar informações e analisar as características de transmissão de dados pela tecnologia 6G relacionadas com a segurança, e assim, identificar vulnerabilidades e a transparência dos dados transmitidos em conformidade com a Lei Geral de Proteção de Dados brasileira [16]. Devido ao aumento da transmissão de dados através da tecnologia 6G poderá surgir vulnerabilidades que coloquem em risco os dados transmitidos e que que não preencham os requisitos encontrados na legislação nacional sobre proteção de dados pessoais.

Palavras-chave—6G, Transmissão de dados, Vulnerabilidades, Proteção de dados.

I. Introdução

Na década de 1980, foi criada a primeira geração da Internet móvel, que marcou o início da mobilidade móvel e da evolução; o 1G, (a letra "G" faz referências às gerações, onde cada geração uma traz evoluções tecnológicas significativas em relação às anteriores), que nessa época tecnologia de Internet móvel era analógica e tinha como missão viabilizar chamadas de voz por meio de um aparelho sem fio.

No início dos anos 1990, surgiu a segunda geração, o 2G, que se tornou mais presente no Brasil, vindo a se popularizar no fim da década, trazendo triunfos em relação a geração pioneira, como troca da tecnologia de analógica para digital, acréscimo de serviço de dados e a importante implementação do envio de mensagem SMS.

Nos anos 2000, a terceira geração da internet móvel foi lançada, o 3G. Esta geração apresenta as características mais próximas da internet móvel atual, com o aprimoramento de recursos, como capacidade de navegação e um suporte ainda incipiente ao streaming e chamadas de vídeo.

Essa etapa da internet móvel expandiu o uso da tecnologia para além dos celulares, como para notebooks, com a novidade, atividades começar a ser feitas em diferentes locais (não só em escritórios, por exemplo), as redes sociais começam a ser usadas massivamente, abrindo oportunidades em diversos setores, como comunicação, marketing e publicidade.

No cenário atual e nos últimos anos, o 4G, é a geração que domina os celulares no Brasil, com todas as funcionalidades da última geração melhorada, e com novos destaques, como o download mais rápido, uso de aplicativos e os importantes serviços em nuvens. Nos dias de hoje, a mais atual geração da internet móvel, 5G, traz melhorias expressivas, oferecendo ultra velocidade na transmissão de dados download e upload 10x mais rápido que 4G), baixa latência, assim, menor tempo de processamento da informação e um aumento na quantidade de aparelhos conectados simultaneamente, com ampliação das aplicações de uso.

Com a atual implementação do 5G no mundo, podemos perceber as grandes vantagens em relação a geração passada, e como é importante essa transição de uma geração para outra; pensando por este caminho, chegamos ao 6G, a futura geração da internet móvel que está em estudo para implementação.

Em contraste com esse cenário, com o constante aumento da transmissão de dados, podem surgir vulnerabilidades que coloquem em risco os dados

transmitidos, assim como ficam propensos a outros ciber ataques, o que motivou nossa proposta, para entender as características de transmissão de dados do 6G relacionadas com a segurança e vulnerabilidade dos dados transmitidos em conformidade com a Lei Geral de Proteção de Dados [16], lei que propõe diretrizes importantes e obrigatórias para armazenamento, uso, coleta e processamento de dados pessoais, se baseando em diversos valores, proporcionando assim novas regras que garantem a privacidade dos brasileiros.

Como problemática de pesquisa, analisou-se que a tecnologia 6G está em estudo de implantação para maior velocidade na transmissão de dados, uma nova forma evolutiva das capacidades tecnológicas após a era 5G. Com o aumento da transmissão de dados consequentemente surgem vulnerabilidades que colocam em risco os dados transmitidos, no caso poderão interferir na segurança se não preencherem os requisitos encontrados na legislação nacional sobre proteção de dados pessoais. Neste contexto, a pergunta que será respondida nesta pesquisa é: Como manter a segurança dos usuários na transmissão de dados 6G em conformidade com a LGPD?

Tem-se como hipótese de pesquisa, e respondendo o questionamento anterior, que a definição das características de segurança para identificar as vulnerabilidades na transmissão de dados através da tecnologia 6G e a construção de uma lista de requisitos essenciais, fazendo assim que usuários naveguem com segurança na internet.

Quando falamos de uma nova geração da internet móvel, pensamos principalmente no aumento na velocidade de download, além de outras grandes vantagens que chegam com uma nova geração, como é o caso do 6G, mas por outro lado, existe um constante aumento na transmissão de dados para que as novas evoluções funcionalidades flua da maneira certa e contínua, o que causa, o também aumento, podendo assim surgir vulnerabilidades que coloquem em riscos estes dados além de ficarem propensos a outros cibernéticos.

O objetivo geral deste artigo é analisar as características de transmissão de dados pela tecnologia 6G relacionadas com a segurança, e assim identificar vulnerabilidade e transparência dos dados transmitidos em conformidade com a Lei Geral de Proteção de Dados [16], propondo ao final um framework conceitual de suporte a futuras implementações. Os objetivos específicos incluem compreender a transmissão de dados através das tecnologias anteriores a 6G, elencar as características correlacionadas com os requisitos legais da LGPD de segurança de dados pessoais, identificar vulnerabilidades possíveis na tecnologia 6G, descrever os requisitos de segurança na transmissão de dados na tecnologia 6G em conformidade com a LGPD.

A motivação e justificativa relaciona-se sobre a cada passagem de geração da internet móvel, vão aparecendo diversas vantagens em relação a geração passada, nos dias de hoje, a atual implementação do 5G trouxe nitidez a esse ponto, por este caminho, olhamos para o futuro e pensamos na próxima geração da internet móvel que já está em estudo, 6G, que terá um upload de dados muito maior em relação a geração atual (5G), em contrapartida, isso faz com que ocorra um grande aumento na transmissão de dados, que podem acabar se convertendo em vulnerabilidades.

II. Referencial Teórico

Para entender os princípios básicos da rede 6G, vamos mostrar sua visão sobre seu futuro e como será em relação a sua segurança e privacidade, quais serão os desafios na implementação e criação dessa nova tecnologia.

Em relação ao cenário da segurança, é necessário frisar que o 6G é a sexta geração de comunicação celular que está sendo desenvolvida. Espera-se que o mesmo seja implantado em 2030 e tenha uma velocidade 50x maior que o 5G enquanto sua latência está projetada para 10-100µs. Pesquisadores projetam que o 6G expandirá a conectividade cobrindo mais áreas, incluindo oceano e até mesmo o espaço aéreo [9] .

Com essas mudanças substanciais há expectativas de que o 6G, relacionado a segurança e privacidade, seja pior que as antigas gerações. O artigo cita os exemplos de: O envolvimento da tecnologia com o corpo humano (implantes inteligentes) potenciais vazamentos de dados e informações pessoais [9].

Potenciais perdas por invasão hacker serão irrecuperáveis, não apenas no financeiro, mas também incorrendo em risco à vida, como na hipótese de um carro autônomo ser hackeado e causar um acidente fatal. Além disso, a evolução da inteligência artificial e sua integração com o 6G pode ser usada também como uma arma de vigilância massiva online. No contraste deste cenário temos também novas tecnologias como a computação quântica, livros distribuídos que podem ser a chave do sucesso para o 6G [9].

Entretanto a pesquisa sobre a segurança e privacidade do 6G está em estado inicial, dessa forma muitos componentes do 6G ainda não estão definidos.

A. Características e Segurança da rede 6G

A tecnologia 6G é a próxima geração de tecnologia móvel após a 5G, e ainda está em fase de desenvolvimento. Algumas das principais características esperadas da tecnologia 6G incluem [18]:

- Velocidades de dados ainda mais rápidas: A tecnologia 6G poderá oferecer velocidades de dados ainda maiores do que as redes 5G, com teóricas velocidades máximas de até 1 terabyte por segundo (TBps).
- Latência ainda mais baixa: A tecnologia 6G pode oferecer latência ainda mais baixa do que as redes 5G, potencialmente reduzindo o tempo de resposta para menos de 1 milissegundo (ms).
- Cobertura global: A tecnologia 6G poderá permitir a cobertura global de alta velocidade, possibilitando conexões de alta velocidade em áreas remotas.
- Rede inteligente: A tecnologia 6G pode permitir o uso de redes mais inteligentes e autônomas, usando

aprendizado de máquina e inteligência artificial para otimizar a rede e melhorar a eficiência.

- Maior eficiência energética: A tecnologia 6G pode oferecer maior eficiência energética do que as redes 5G, permitindo que os dispositivos móveis durem mais tempo com uma única carga de bateria.
- Suporte a novos casos de uso: A tecnologia 6G pode permitir novos casos de uso, como comunicações holográficas, comunicação via ondas cerebrais, comunicação com dispositivos quânticos, entre outros.

Em suma, a tecnologia 6G representa a próxima fase na evolução da conectividade móvel, sucedendo o 5G, com avanços significativos esperados em diversos aspectos. Entre os principais diferenciais esperados do 6G, estão velocidades de dados mais rápidas, com taxas de até 1 terabyte por segundo, e uma latência extremamente baixa, potencialmente inferior a 1 milissegundo, proporcionando respostas em tempo quase real. A cobertura global é outro objetivo, o que ampliaria a conectividade para áreas remotas com alta velocidade, algo essencial para viabilizar aplicações como IoT global e comunicação ininterrupta. Além disso, o 6G busca integrar inteligência artificial e aprendizado de máquina, possibilitando redes mais inteligentes e autônomas que otimizam automaticamente os recursos e aumentam a eficiência.

A Tabela I, que descreve a evolução das tecnologias de conectividade móvel, ilustra claramente o progresso das redes de 2G a 5G e fornece um contexto para o 6G, destacando como cada geração expandiu as capacidades de conectividade, velocidade, e eficiência. Enquanto o 5G aprimora a conectividade com maior velocidade e menor latência, o 6G projeta um salto ainda maior, com foco em eficiência energética e suporte a novos casos de uso, como comunicações holográficas e comunicação com dispositivos quânticos. Esse progresso contínuo, evidenciado na Tabela I, mostra a evolução das redes móveis e os avanços esperados com a chegada do 6G, o que abre portas para novas possibilidades tecnológicas e transforma a maneira como as redes conectam dispositivos e usuários em escala global.

Tabela I: Evolução das tecnologias de conectividade móvel

Geração	**Tecnologia de Modulação**	**Ano de Lançamento**	**Velocidade Máxima de Dados**	**Características Principais**
1G	AM	1980	2,4 kbps	Voz analógica
2G	PSK	1991	384 kbps	Voz e SMS digital
3G	CDMA/ WCDM A	2001	2 Mbps	Voz, dados móveis e multimídia
4G	OFDM A	2010	1 Gbps	Dados móveis de alta velocidade
5G	5G NR	2019	20 Gbps	Conectividade avançada e aplicações IoT
6G	Ainda em desenvolvimento	Previsto para 2030	Esperado acima de 1 Tbps	Eficiência energética, conectividade massiva, automação, IA entre outros

Fonte: Autores

B. Lei Geral de Proteção de Dados

A LGPD (Lei Geral de Proteção de Dados) [16] é uma legislação que tem como objetivo proteger os dados pessoais dos cidadãos brasileiros, regulamentando sua coleta, armazenamento, processamento e compartilhamento por empresas e instituições públicas e privadas. Sua implementação exige que essas organizações mapeiem o tratamento de dados pessoais, estabelecendo o ciclo de vida dos mesmos e mapeando os riscos de impacto direto dos celulares pela atividade de tratamento [16].

Para atenuar esses riscos, é preciso implementar medidas técnicas e administrativas, e também nomear um encarregado pelo tratamento de dados pessoais (DPO) - conforme exigido pelo artigo 5º, inciso VIII, da Lei 13.853/2018 - para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) [17].

No setor público, a LGPD estabelece um novo regime normativo para regulação das operações de tratamento de dados pessoais efetuadas pelo poder público. Nesse contexto, é fundamental que o tratamento de dados executado pelo poder público atenda apenas às finalidades públicas, com ênfase no interesse público, a fim de que possibilite a execução das atribuições legais do poder público [16].

A LGPD [16] começou a vigorar no Brasil em 18 de setembro de 2020 e isso fez com que o país se tornasse incluído no grupo de países que possui uma legislação específica para a proteção de dados dos seus cidadãos, proporcionando novas regras que garantem a privacidade dos brasileiros. A LGPD se baseia em diversos valores e possui como principais objetivos [16]:

- Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, através de práticas transparentes e seguras garantindo direitos fundamentais.
- Reforçar a segurança das relações jurídicas e

confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.
- Definir regras claras sobre o tratamento de dados pessoais.
- Propor a concorrência e a livre atividade econômica inclusive com a portabilidade

de dados.

Assim, tem-se que a LGPD) tem como principais objetivos garantir a privacidade e a proteção dos dados pessoais dos usuários, promovendo práticas seguras e transparentes que assegurem direitos fundamentais. A LGPD também busca fortalecer a segurança nas relações jurídicas, aumentando a confiança dos titulares no tratamento de dados e garantindo a liberdade econômica e a concorrência justa. Além disso, a lei define regras claras para o tratamento de dados e incentiva a portabilidade de dados, promovendo a livre atividade econômica e a competitividade.

C. Dados Pessoais

Este conceito foi definido como "informação relacionada a pessoa identificada ou identificável". Ou seja, um dados é considerado pessoal quando ele possibilita a identificação, direta e/ou indireta, da pessoa por trás dos dados. Exemplo de dados pessoais são:

- Nome e Sobrenome;
- Data de nascimento;
- Documentos pessoais (CPF, RG, CNH, Passaporte, Título de eleitor e carteira de trabalho);
- Endereço residencial e/ou comercial;
- Telefone;
- E-mail;
- Cookies;
- Endereço de Ip;

Neste sentido, a LGPD prevê a necessidade de consentimento para a coleta e o tratamento de dados pessoais. Esse consentimento deve ser livre, informado e inequívoco, e pode ser revogado a qualquer momento pelo titular dos dados. A LGPD também exige que os controladores de dados (empresas ou organizações que coletam e tratam dados) garantam a segurança e a privacidade dos dados pessoais sob sua responsabilidade, adotando medidas técnicas e organizacionais para prevenir o acesso não autorizado, o uso indevido, a perda ou a destruição desses dados [16].

D. Dados Sensíveis

A Lei Geral de Proteção de Dados (LGPD) define dados pessoais sensíveis como informações que se referem à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde ou vida sexual e dados genéticos ou biométricos. Esses dados são considerados mais delicados do que outras informações pessoais, pois podem ser usados para discriminar ou prejudicar indivíduos ou grupos.

O tratamento de dados pessoais sensíveis é mais restrito pela LGPD. As empresas só podem coletar, armazenar, utilizar e compartilhar essas informações com consentimento explícito e específico do titular dos dados ou em situações excepcionais, como em casos de proteção à vida ou à saúde do titular, para o cumprimento de obrigações legais ou regulatórias, entre outros [16].

Além disso, a LGPD exige que as empresas adotem medidas técnicas e organizacionais adequadas para proteger os dados pessoais sensíveis e evitar vazamentos, acessos não autorizados ou qualquer forma de tratamento indevido dessas informações. As empresas também devem designar um encarregado pela proteção de dados (DPO) para garantir o cumprimento da LGPD e atuar como ponto de contato com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD)[17].

E. Transmissão de dados em conformidade com a LGPD

A transmissão de dados refere-se ao processo de envio de informações de um ponto a outro, geralmente através de uma rede de comunicação. Esse processo pode ocorrer de diversas formas, como por exemplo, através de cabos de rede, conexões sem fio, satélites, entre outros.

Com o avanço da tecnologia, a transmissão de dados tornou-se fundamental para a troca de informações em diversos setores, desde a comunicação pessoal até transações comerciais. Porém, o aumento na quantidade de dados transmitidos também trouxe desafios relacionados à privacidade e segurança dos dados.

Nesse sentido, a transmissão de dados torna-se uma atividade que envolve o tratamento de dados pessoais, sujeita às regras estabelecidas pela LGPD. Essas regras visam proteger os dados pessoais dos titulares, estabelecendo medidas de segurança e privacidade para garantir que os dados sejam transmitidos de forma segura e responsável.

Para garantir a segurança na transmissão de dados, é importante que as empresas adotem medidas de segurança adequadas, como criptografia e autenticação de dados. Além disso, é importante que as empresas forneçam informações claras sobre a finalidade da transmissão, o destino dos dados e as medidas de segurança adotadas.

Caso ocorra alguma violação de dados durante a transmissão, as empresas devem notificar os titulares dos dados afetados e as autoridades competentes, além de tomar medidas para minimizar os danos causados pela violação. A transmissão de dados é, portanto, uma atividade que requer responsabilidade e cuidado por parte das empresas para garantir a privacidade e segurança dos dados pessoais dos usuários [16].

A LGPD também estabelece a obrigação de informar ao titular dos dados sobre a transmissão, bem

como sobre o destino e finalidade dos dados transmitidos. Caso ocorra alguma violação de dados durante a transmissão, a empresa responsável deve notificar as autoridades e os titulares dos dados afetados [6].

III. Requisitos e Vulnerabilidades

Como observado diante do referencial teórico no que se refere-se ao 6G e sua segurança destacamos as seguintes vulnerabilidades diante dessa nova tecnologia que vem sendo desenvolvida:

- Risco de invasões Hackers: Como verificado esse tipo de invasão tem consequências tanto financeiras (Como por exemplo uma invasão onde os hackers recolhem dados pessoais de clientes, documentos com informações financeiras e solicitam dinheiro para o resgate dessas informações que são valiosas para empresa e caso ocorra vazamento a empresa pode se prejudicar judicialmente sendo processada ou pelo MP ou pelos clientes que sofreram com o vazamento de suas informações, causando assim uma perda financeira considerável para empresa.) ou da vida (Onde uma invasão ilegal pode ocorrer em um carro autônomo, tomando o controle do mesmo e causando um acidente, dessa forma colocando em risco a vida não apenas do motorista/usuário mas de outras pessoas também) [18].
- Cyber ataques do tipo *data injection*: Em relação a esses tipos de ataques específicos, que na atualidade geralmente são comuns, foi verificado que os mesmos são mais "possíveis" por conta da alta velocidade e menor latência no 6G, com esses fatores uma invasão acontece de forma mais rápida sendo assim de difícil detecção pelas tecnologias já desenvolvidas. Esse tipo de invasão pode prejudicar servidores, sistemas, redes, IoT's e dessa forma comprometer a segurança dos mesmos.
- Vigilância Massiva Online: Uma das maiores preocupações da atualidade referente a segurança de dados/informação está relacionada a vigilância, todos nossos dados já estão nas redes e sendo compartilhados de forma que não damos autorização, dessa forma é possível traçar informações sobre sexualidade, religiosidade, posicionamento político, informações sobre saúde, dados que são considerados sensíveis pela LGPD.

De maneira resumida, tem-se que o risco de invasões hackers apresenta graves consequências financeiras e de segurança, afetando empresas e vidas. Um ataque pode levar ao roubo de dados pessoais e financeiros, seguido por extorsão, o que expõe a empresa a processos e sanções judiciais. Em casos mais graves, invasões em dispositivos críticos, como carros autônomos, podem comprometer a segurança física, colocando em risco a vida de usuários e de outras pessoas.

Os ataques de injeção de dados se tornam mais rápidos e difíceis de detectar com o aumento da velocidade e menor latência nas redes 6G, afetando servidores, sistemas, redes e dispositivos IoT, e comprometendo a segurança digital. Além disso, a vigilância massiva online é uma preocupação crescente, pois dados pessoais são compartilhados sem consentimento, permitindo inferências sobre informações sensíveis, como orientação sexual, crenças religiosas, preferências políticas e saúde, o que desafia as proteções da LGPD.

A. Requisitos técnicos para transmissão de dados 6G

A tecnologia 6G, projetada para ser uma rede altamente autônoma e inteligente, deve possibilitar a conexão entre dispositivos em ambientes diversificados, abrangendo redes em espaço, ar, terra e até submarinas. Com o suporte de tecnologias como inteligência artificial (IA), aprendizado de máquina, blockchain, comunicação por luz visível (VLC) e frequências de terahertz (THz), o 6G trará uma infraestrutura integrada e interconectada, ideal para o futuro da sociedade digital. A IA será crucial para o 6G, permitindo uma conexão perfeita entre dispositivos, monitorando o status da rede em tempo real, otimizando o desempenho e melhorando a qualidade da experiência do usuário. No entanto, a segurança da IA será essencial, pois ataques direcionados aos sistemas de IA podem comprometer o funcionamento e a integridade da rede 6G.

Blockchain emerge então como uma das tecnologias centrais para desbloquear o potencial do 6G, pois permite a criação de sistemas de segurança descentralizados, como a autenticação de identidade, reforçando a segurança das redes sem fio. Além disso, a comunicação por luz visível (VLC) apresenta um nível superior de segurança em relação aos sistemas de radiofrequência (RF), pois a luz não atravessa paredes, limitando as possibilidades de interceptação. No entanto, o risco de espionagem permanece em áreas públicas ou em locais com grandes janelas, onde a comunicação por luz pode ser exposta a observadores externos.

O desenvolvimento do 6G é voltado para atender às demandas da sociedade da informação inteligente, que exigirá uma rede ultraconectada e autônoma para lidar com o crescente número de dispositivos. Graças à IA, o 6G terá a capacidade de se autoconfigurar, autovigiar, se autorreparar e se auto-otimizar, minimizando a necessidade de intervenção humana. Esses avanços farão do 6G uma plataforma robusta e versátil, essencial para novas aplicações, como comunicação por hologramas, interações por ondas cerebrais e conexão de dispositivos quânticos, expandindo as possibilidades de interações e operações em uma rede global de alta performance e segurança.

IV. Análise dos Requisitos e Proposta de Requisitos

Espera-se definir os requisitos seguros prevenindo sobre vulnerabilidades sobre os dados transmitidos em

conformidade com a legislação definida na Lei Geral de Proteção de Dados.

A tabela II traz as vulnerabilidades e possíveis soluções e com vulnerabilidades baseadas em requisitos técnicos para a segurança na transmissão 6G:

Tabela II: Vulnerabilidades baseadas nos Requisitos Técnicos

Tecnolo-gia	**Vulnerabili-dades Técnicas**	**Possíveis soluções**
Terahertz (THz)	Ataques de controle de acesso e interceptaçã o de sinal	- Implementação de medidas de segurança mais rigorosas, como criptografia de dados, autenticação de usuários e monitoramento de acesso. Utilização de técnicas de feixes estreitos para melhorar a direcionalidade do sinal e minimizar a interceptação.
Blockchain	Ataques de 51% e Ataques de vetor de consenso	Implementação de mecanismos de consenso mais robustos, como o Proof-of-Stake. Aumento da descentralização da rede para tornar mais difícil um ator malicioso controlar a maioria dos recursos da rede.Desenvolvimento de soluções de governança para evitar que grupos de mineradores ou validadores se unam para controlar a rede.
Inteligência Artificial (IA)	Ataques adversariais e Viés algorítmico	Desenvolvimento de modelos de IA mais robustos e resistentes a ataques, que levam em consideração os possíveis cenários adversários.Utilização de conjuntos de dados mais diversos e inclusivos para minimizar o viés algorítmico.Desenvolvim ento de soluções de auditoria para detectar e corrigir problemas de viés algorítmico
VLC (Comunicação por luz visível)	Espionagem em áreas públicas e interferência de luz ambiente	Implementação de técnicas de criptografia de dados para proteger as transmissões de informações sensíveis.
Machine Learning	Ataques adversariais e Viés algorítmico	Desenvolvimento de modelos de aprendizado de máquina mais robustos e resistentes a ataques, que levam em consideração os possíveis cenários adversários

Fonte: Autores

A. Proposta de Implementação da Transmissão 6G em conformidade com a Legislação Nacional

A implementação da transmissão do G6 conforme a LGPD deve ser realizada com base nos princípios da lei, que buscam garantir a privacidade e a segurança dos dados pessoais. Para isso, é importante seguir algumas etapas, sintetizadas na tabela III:

Tabela III: Proposta para Análise de Vulnerabilidades e Requisitos

Etapas	O que deve ser feito	Como realizar
1. Mapeamento dos dados	Identificar quais dados pessoais serão transmitid os pelo 6G.	Realizar um inventário dos dados que serão coletados e transmitidos
2. Identificação das bases legais	Identificar qual base legal será utilizada para a transmiss ão do G6	Verificar se há consentimento dos titulares dos dados ou se há outra base legal que permita o tratamento dos dados

Etapas	O que deve ser feito	Como realizar
3. Implementação de medidas de segurança	Implementar medidas de segurança adequadas para proteger os dados pessoais	Utilizar criptografia, autenticação de usuários, backups regulares, controles de acesso e monitoramento de atividades suspeitas
4. Política de privacidade	Elaborar uma política de privacidade clara e acessível para os usuários do G6	Informar de forma transparente quais dados pessoais serão coletados e transmitidos, qual a finalidade da transmissão e como os dados serão tratados e protegidos
5. Treinamento de funcionários	Treinar todos os funcionários envolvidos na transmissão do G6 sobre a importância da privacidade e segurança dos dados pessoais	Elaborar um programa de treinamento e conscientização para os funcionários
6. Auditoria e Monitoramento	Realizar auditorias periódicas e monitoramento constante da transmissão do G6 para garantir a conformidade com a LGPD	Realizar auditorias internas, monitorar as atividades de transmissão e avaliar a eficácia das medidas de segurança implementadas

Fonte: Autores

B. Framework Conceitual de adequação da transmissão de dados 6G conforme a legislação nacional de proteção de dados

O framework conceitual da figura 1 apresenta a implementação de medidas de segurança adequadas é fundamental para proteger os dados pessoais. Isso inclui o uso de criptografia, autenticação de usuários, backups regulares, controles de acesso e monitoramento de atividades suspeitas. Essas medidas ajudam a prevenir o acesso não autorizado e garantem a integridade e confidencialidade dos dados.

Uma política de privacidade clara e acessível deve ser elaborada, informando aos usuários do 6G quais dados pessoais serão coletados e transmitidos, qual a finalidade da transmissão e como os dados serão tratados e protegidos. É essencial garantir transparência e possibilitar que os usuários exerçam seus direitos relacionados aos dados pessoais. Além disso, é necessário treinar os funcionários envolvidos na transmissão do 6G sobre a importância da privacidade e segurança dos dados pessoais. Um programa de treinamento e conscientização ajuda a criar uma cultura organizacional que valoriza a proteção de dados e promove boas práticas.

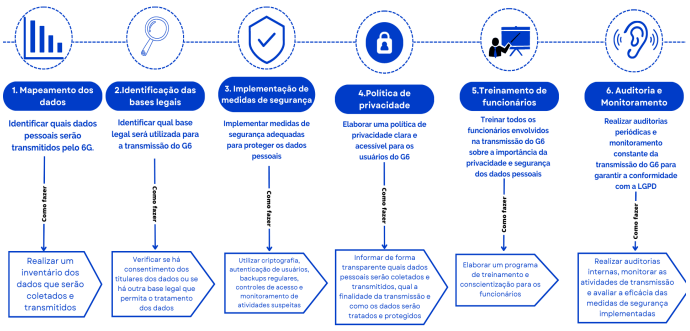

Fig. 2. Framework Conceitual de adequação da transmissão de dados 6G conforme a legislação nacional de proteção de dados

No último item do framework, tem-se a realização de auditorias periódicas e o monitoramento constante da transmissão do 6G são essenciais para garantir a conformidade com a LGPD. As auditorias internas e a avaliação da eficácia das medidas de segurança implementadas permitem identificar possíveis

vulnerabilidades e tomar ações corretivas necessárias. Seguindo essas diretrizes e etapas, é possível avançar na implementação do 6G de forma a garantir a privacidade e a segurança dos dados pessoais, em conformidade com a LGPD.

V. Considerações Finais

O trabalho apresenta um conjunto de etapas e um framework conceitual para garantir a segurança e a conformidade da transmissão de dados na tecnologia 6G com a Lei Geral de Proteção de Dados (LGPD), visando proteção e privacidade dos dados pessoais. Esse framework fornece orientações para novas tecnologias e redes de alta transmissão de dados, antecipando a segurança necessária para o 6G e futuros avanços.

É possível enfatizar o impacto potencial desse framework em cenários práticos, considerando a expansão da conectividade global e a diversidade de dispositivos conectados no ecossistema 6G. A aplicabilidade do framework poderia ser explorada em contextos de segurança emergentes, como na IoT e em veículos autônomos, áreas onde ataques de dados poderiam comprometer vidas e dados críticos. Além disso, a adoção de um framework baseado na LGPD pode incentivar outros países a desenvolverem legislações semelhantes, criando uma base regulatória global robusta para a proteção de dados no ambiente 6G, o que pode ser um diferencial para a segurança e confiabilidade das redes móveis do futuro.

VI. Referências

1. S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," *Sensors*, vol. 22, no. 5, pp. 1969, 2022. doi: 10.3390/s22051969.
2. M. C. Bodin de Moraes, "LGPD: um novo regime de responsabilização civil dito proativo," *Civilistica*, 2022. [Online]. Available: https://civilistica.emnuvens.com.br/redc/article/view/448. [Accessed: Nov. 18, 2022].
3. S. Dang, O. Amin, B. Shihada, et al., "What should 6G be?," *Nat Electron*, vol. 3, pp. 20–29, 2020. [Online]. Available: https://doi.org/10.1038/s41928-019-0355-6. [Accessed: Nov. 18, 2022].
4. S. H. D. A. S. V. F. V. L. G. Da Rosa Oliveira, "Marco Civil da Internet," *JICEX*, vol. 3, no. 3, 2015. [Online]. Available: https://unisantacruz.edu.br/revistas-old/index.php/JICEX/article/view/675. [Accessed: Nov. 18, 2022].
5. E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "5G: Evolução para Múltiplas Camadas Celular Sem Fio," 2013. [Online]. Available: https://repositorio.utfpr.edu.br/jspui/bitstream/1/20040/2/CT_TELEINFO_2013_1_06.pdf. [Accessed: Nov. 18, 2022].f
6. C. F. Lima Rapôso, H. Melo de Lima, W. F. de Oliveira Junior, P. A. Ferreira Silva, and E. de Souza Barros, "LGPD - Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação: Revisão Sistemática," *RACE - Revista de Administração do Cesmac*, vol. 4, pp. 58–67, 2019. doi: 10.3131/race.v4i0.1035.
7. M. Tariq, M. Ali, F. Naeem, and H. V. Poor, "Vulnerability Assessment of 6G-Enabled Smart Grid Cyber–Physical Systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5468-5475, Apr. 2021. doi: 10.1109/JIOT.2020.3042090.
8. M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281-291, 2020. ISSN 2352-8648.
9. V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Commun. Surveys Tuts.*, 2021. doi: 10.1109/COMST.2021.3108618. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9524814. [Accessed: Nov. 18, 2022].
10. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The Roadmap to 6G Security and Privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094-112, 2021. doi: 10.1109/ACCESS.2021.3120143.
11. V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaaki, "Security and Trust in the 6G Era," *IEEE Access*, vol. 9, pp. 142314-142327, 2021. doi: 10.1109/ACCESS.2021.3120143.
12. S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "Taxonomy about the Stages of Performing Automated Decision-Making Processing under GDPR in the Light of 6G Networks," in *2020 3rd World Symposium on Communication Engineering (WSCE)*, 2020, pp. 23-27. doi: 10.1109/WSCE51339.2020.9275570.
13. I. M. Takemoto, "Aplicação da tecnologia 5G em projetos de telefonia," B.Sc. thesis, Dept. Electrical Engineering, Universidade Estadual Paulista, Faculdade de Engenharia de Guaratinguetá, 2017. [Online]. Available: http://hdl.handle.net/11449/203704. [Accessed: Nov. 18, 2022].

14. C. S. de Teffé and M. Viola, "Tratamento de dados pessoais na LGPD: estudo sobre as bases legais," *Civilistica*, vol. 9, no. 1, pp. 1-38, 2020. [Online]. Available: https://civilistica.emnuvens.com.br/redc/article/view/510. [Accessed: Nov. 18, 2022].
15. Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2021, pp. 616-621. doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.
16. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l4020.htm. [Accessed: Apr. 14, 2024].
17. Lei nº 13.853, de 8 de julho de 2019. *Dispõe sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD)*. Brasília, DF: Presidência da República. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. [Accessed: Apr. 14, 2024].
18. M. B. Gracia, V. Malele, S. P. Ndlovu, T. E. Mathonsi, L. Maaka, e T. Muchenje, "6G Security Challenges and Opportunities," *2022 IEEE 13th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT)*, Cape Town, South Africa, 2022, pp. 339-343, doi: 10.1109/ICMIMT55556.2022.9845296. [Accessed: Apr. 14, 2024]