CRIPTOGRAFIA DE PONTA A PONTA E PROTEÇÃO DE DADOS ÌNTIMOS NO BRASIL: ANÁLISE JURÍDICA E TÉCNICA DO WHATSAPP

RESUMO

Este trabalho investiga o uso da criptografia ponta a ponta e a eficácia das leis brasileiras na redução do vazamento de dados na plataforma WhatsApp. O objetivo é aprimorar o entendimento e a eficácia da legislação brasileira no que diz respeito ao vazamento de dados íntimos investigando a aplicação da criptografia de ponta a ponta no WhatsApp, especialmente dados íntimos, garantindo a segurança nas comunicações digitais. A metodologia segue uma abordagem qualitativa, de caráter exploratório e descritivo. Foi realizada a da revisão bibliográfica de artigo se a análise documental das leis: LGPD e Carolina Dieckmann, da jurisprudência atual para alcançar o objetivo deste estudo. Por meio dos resultados, verificou-se que o WhatsApp, através da criptografia de ponta a ponta, garante a confidencialidade das mensagens, no entanto ainda enfrenta dificuldades para identificar tais conteúdos ilícitos e realizar sua remoção da plataforma, de modo a atender a legislação brasileira.

Palavras-chave: Criptografia ponta a ponta. Leis de proteção de dados. WhatsApp.

ABSTRACT

This study investigates the use of end-to-end encryption and the effectiveness of Brazilian laws in reducing data leaks on the WhatsApp platform. The objective is to improve the understanding and effectiveness of Brazilian legislation regarding the leaking of personal data by investigating the application of end-to-end encryption on WhatsApp, especially regarding personal data, ensuring the security of digital communications. The methodology follows a qualitative, exploratory, and descriptive approach. A bibliographic review of articles and a documentary analysis of the LGPD and Carolina Dieckmann laws, as well as current case law, were conducted to achieve the objective of this study. The results showed that WhatsApp, through end-to-end encryption, guarantees the confidentiality of messages; however, it still faces difficulties in identifying such illicit content and removing it from the platform, in compliance with Brazilian legislation.

Keywords: End-to-end encryption. Data protection laws. WhatsApp.

1 INTRODUÇÃO

A crescente digitalização de nossas vidas e o armazenamento massivo de informações pessoais online tem gerado uma necessidade urgente de proteção de dados pessoais, através da regulação da Internet e de políticas de informação (D” Oliveira e Cunha, 2024). Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) e a lei Carolina Dieckmann surgiram como marcos regulatórios cruciais para garantir

a segurança e a privacidade dos indivíduos. No entanto, a aplicação efetiva dessa legislação e o combate ao vazamento de dados continuam sendo desafios complexos, pois “a Internet representa uma ameaça significativa à privacidade dos indivíduos, pois permite aos prestadores de serviços trocar informações e monitorizar o comportamento virtual dos utilizadores na rede”.(Bispo e Binto, 2023; p.365)

O objetivo geral desta pesquisa é aprimorar o entendimento e a eficácia da legislação brasileira no que diz respeito ao vazamento de dados íntimos investigando a aplicação da criptografia de ponta a ponta no WhatsApp, especialmente dados íntimos, garantindo a segurança nas comunicações digitais.

Além disso, os objetivos específicos são: a) Trazer algoritmo de criptografia ponta a ponta e os métodos utilizados no WhatsApp, pontuando a estrutura e a metodologia por trás da sua aplicação; b) analisar, a partir da lei Carolina Dieckmann e LGPD, melhorias para potencializar as ferramentas jurídicas brasileiras em combate ao vazamento de dados íntimos; c) identificar quais os benefícios que esta ferramenta traz e as novas abordagens para o desafio do controle de vazamento de dados íntimos, detectando as boas práticas e as lições que podem ser aplicadas ou adaptadas ao contexto brasileiro.

Foi considerado como hipótese neste estudo, a utilização da criptografia de ponta a ponta tem o potencial de reduzir significativamente a incidência de vazamentos de dados em plataformas de comunicação, como o WhatsApp.

No entanto, os desafios relacionados à falta de conscientização dos usuários e ao limitado conhecimento técnico sobre essas ferramentas no contexto brasileiro criam uma lacuna na efetiva aplicação dessas medidas de segurança. A partir da investigação aprofundada do algoritmo de criptografia de ponta a ponta e do WhatsApp, aliada à análise da jurisprudência nacional, é possível promover um enfrentamento mais coerente, seguro e eficaz dos casos de exposição de dados íntimos no Brasil.

A partir do levantamento das aplicações criptográficas que são usadas em softwares e sistemas que são utilizados para proteção de vazamentos de imagens íntimas no Brasil reduzem significativamente a incidência de vazamentos de fotos e dados íntimos no Brasil, porém enfrenta desafios relacionados à conscientização do usuário, à eficácia das plataformas digitais e à lacuna na aplicação das leis existentes.

Além disso, é importante destacar que as principais vítimas dos crimes digitais são as mulheres, que representam cerca de 53% dos casos registrados envolvendo ameaças, ofensas, insultos ou divulgação de imagens sem consentimento (Norte Filho *et al.*; 2024). Daí se justifica o interesse por esta pesquisa, que surge do interesse pessoal das autoras que, enquanto mulheres, vivenciam cotidianamente a vulnerabilidade e a exposição enfrentadas pelo público feminino no ambiente digital.

Este trabalho é estruturado da seguinte forma: começa com a introdução, na qual apresenta a temática abordada. Em seguida, temos o referencial teórico, que se baseia em procedimentos bibliográficos e documentais sobre o tema. Nessa seção, é realizado um comparativo entre as diretrizes da lei Carolina Dieckmann e da LGPD, com ênfase no impacto específico da segurança e privacidade dos dados, especificamente, imagens íntimas, no Brasil. Logo depois temos a metodologia, que visa descrever o tipo de pesquisa realizada, que neste estudo, tem uma abordagem qualitativa, pois apresenta resultados através de percepções e análise, e é uma pesquisa bibliográfica, que tecnicamente consiste na revisão, análise de artigos e outros documentos do referido tema. Depois, a análise de resultados, a partir das informações coletadas durante a pesquisa. Por fim, as considerações finais, que é divulgado o significado e conclusões da análise deste estudo.

2 A LEI LGPD E LEI CAROLINA DIECKMANN NO CENÁRIO JURÍDICO BRASILEIRO

A Lei Geral de Proteção de Dados (LGPD) foi promulgada em 2018 e tem como objetivo adequar as práticas de tratamento de dados no Brasil, tendo sido inspirada na Diretiva (UE) 2016/680, também conhecida como Regulamento Geral sobre Proteção de Dados da União Europeia (GDPR), uma regulamentação da União Europeia que entrou em vigor em maio de 2018, tornando-se um marco regulatório essencial para garantir maior proteção e privacidade dos dados pessoais dos cidadãos europeus.

Segundo Nascimento e Silva (2023), antes da LGPD, as práticas relacionadas à proteção de dados no Brasil eram abordadas de maneira fragmentada por diferentes regulamentações e leis setoriais. Assim, a LGPD surge como uma resposta legislativa para preencher essa lacuna proporcionando uma

estrutura legal, mais abrangente e coesa do uso de dados pessoais no Brasil. A LGPD além de normas, diretrizes, regulamentações, princípios e trouxe consigo, a mudança de cultura nas instituições e organizações (pública e privada), agregando no tratamento de dados pessoais, maior responsabilidade. Isso é fato, o que possibilitou rever a forma de processamento e tratamento

Em seu artigo 17, a LGPD informa que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.” Com isso, reforça-se a necessidade de garantir a proteção dos direitos individuais dos usuários, num cenário de crescente preocupação com a privacidade digital e a segurança de dados.

Para os autores D'Oliveira e Cunha (2024), a LGPD estabelece:

> o tratamento de dados pessoais, por quem deve ser executado, quem deve ser responsabilizado, quais as hipóteses de tratamento, ou seja, estabelece regras claras sobre o tratamento de dados pessoais, além de apresentar os princípios que o regem como: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Há, igualmente, exigências de implementação de medidas por parte de pessoa natural ou por pessoa jurídica, de direito público ou privado, para que seja garantida a segurança e proteção de dados pessoais coletados em território nacional, respeitando seus princípios. (p.10)

Além disso, a lei prevê sanções para o descumprimento, os agentes de tratamento estão sujeitos a sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados, incluindo multas que podem atingir até 2% do faturamento anual da empresa, limitado a 50 milhões de reais (Brasil, 2018).

Além das penalidades aplicadas a partir da LGPD, também há implicações na área penal, a partir da Lei nº 12.737/2012, que ficou conhecida como Lei Carolina Dieckmann, que visa responsabilizar os indivíduos que cometem o crime de invasão de dispositivos eletrônicos. Segundo França (2024) esta lei é a pioneira no Brasil e proporcionou maior segurança jurídica em relação aos crimes digitais, que estão se tornando cada vez mais frequentes.

A Lei Carolina Dieckmann promulgada em 2012, surgiu como resposta aos incidentes de violação de privacidade e invasão de dados íntimos e divulgação de fotos e vídeos íntimos da atriz, na rede mundial de computadores, tendo como objetivo criminalizar os acessos não autorizados e o compartilhamento indevido dessas

informações pessoais (Machado e Duarte, 2021). Para tanto, a Lei 12.737 alterou o Código Penal Brasileiro, com o acréscimo dos artigos 154 A:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita [...]Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Brasil, 2012).

Como afirmam Borges e Novais (2021), esta lei estabelece que o crime ocorre quando há a invasão de dispositivos ou instalação de vulnerabilidades com o objetivo de obter vantagem ilícita, somente a partir da “violação indevida de mecanismo de segurança”, evidenciando que não havendo um sistema de segurança a ser invadido, não se aplica o artigo 154-A.

Ambas as legislações visam proteger os dados pessoais e garantir a privacidade dos indivíduos. Elas estabelecem direitos para os titulares de dados, como apresentamos no quadro 1, exigindo que as organizações sejam transparentes sobre como os dados são processados.

Quadro 1: Quadro comparativo entre a LGPD e a Lei Carolina Dieckmann

Lei Carolina Dieckmann	LGPD
Lei nº 12.737 promulgada em 30 de novembro de 2012	Lei nº 13.709 promulgada em 14 de agosto de 2018
Tem como objetivo criminalizar a invasão de dispositivos eletrônicos.	Proteger os dados pessoais e garantir direitos aos titulares.
Penal (criminal).	Civil e administrativa.
Tem como alvo indivíduos que invadem dispositivos informáticos.	Tem como alvo agentes de tratamento de dados (empresas, órgãos públicos).
Sanções previstas: Pena de 3 meses a 1 ano de prisão e/ou multa.	Sanções previstas :Advertência, multa (até R$ 50 milhões), bloqueio/exclusão de dados.
Regula a invasão de dispositivos, roubo de dados, instalação de vírus.	Regula o tratamento de dados pessoais, independentemente do meio, físico ou digital, realizado por pessoa física ou jurídica de direito público ou privado.

Fonte: Elaborado pelas autoras

Machado e Duarte (2021) consideram que tanto a lei Carolina Dieckmann quanto a LGPD apresentam falhas. A primeira, não apresenta punições quando o crime é cometido utilizando o dispositivo da própria vítima, e leva em conta a finalidade para o qual o crime foi cometido. Em relação à segunda lei, os autores afirmam que a LGPD possui algumas fragilidades pois, as penalidades são de natureza apenas cível, não havendo sanção penal. No entanto, autores como Norte Filho *et al.* (2024), recomendam que a implementação destas duas leis esteja associada para maior na proteção da privacidade das vítimas. Além disso, a dificuldade em aplicação das leis se deve a dinamicidade e a natureza global da internet, que possibilita o surgimento constante de ameaças cibernéticas, muitas vezes oriundos de outros países, inviabilizando a aplicação das leis locais (Borges e Novais ,2024).

3 A CRIPTOGRAFIA DE PONTA A PONTA E SEU USO NA PRÁTICA

A necessidade de troca de mensagens entre pessoas, uniu um propósito, assegurando que as informações não fossem acessíveis e disponíveis para pessoas não autorizadas (Oitechen; 2020). Conforme Viana *et al*. (2022) a criptografia:

> é uma técnica muito importante já que desempenha um papel com dois propósitos principais, sendo o primeiro de impedir a visualização dos dados sem algum tipo de autorização e o segundo, permitir a transmissão de dados de forma segura por locais ditos inseguros, para que os dados da origem cheguem ao seu destino sem qualquer alteração, ou seja a criptografia tem como objetivo principal garantir a confidencialidade, integridade e privacidade dos dados e está presente em dois dos pilares da segurança da informação (p. 226 -227)

Neste sentido desenvolve-se a criptografia, palavra que vem do grego, numa tradução:" *kripto*" que significa "oculto secreto" e "grapho" escrita. Desse modo, criptografar é proteger a informação da leitura indevida, bem como de alteração não permitidas, garantindo assim a sua integridade, sendo utilizada para ocultar mensagens mídia e outros dados, que apenas WhatsApp, mas também em outras situações, tais como pelas operadoras de cartões de crédito, por exemplo (Viana *et al*.; 2022), (Beiriz e Pedras; 2024).

Segundo Albarello (2019), existem dois tipos de criptografia, a simétrica e a assimétrica. Na simétrica uma única chave serve para codificar e decodificar a mensagem. Já a criptografia assimétrica é utilizada duas chaves diferentes, sendo uma pública que pode ser livremente compartilhada e a privada que seria usada em sigilo.

Beiriz e Pedras (2024), afirmam que embora estes dois tipos de criptografia sejam capazes de proteger o direito fundamental à privacidade dos usuários, há um risco de exposição de dados se a chave for revelada.

3 .1 Criptografia de ponta a ponta

Como cada vez mais temos que realizar trocas de informações, mensagens a criptografia de ponta a ponta (end-to-end encryption – E2EE) se mostra uma aliada em garantir a proteção desses dados, assegurando que apenas os usuários participantes dessas mensagens tenham acesso a esse conteúdo.

Segundo Beiriz e Pedras (2024):

> a criptografia de ponta a ponta desponta como grande empecilho a mencionado desiderato, uma vez que não permite a recuperação, a interceptação e o compartilhamento das mensagens ligadas à preparação, execução ou consumação de crimes que tenham sido trocadas dentro do aplicativo (p.94).

Diversos protocolos de segurança foram desenvolvidos, um deles é o Signal Protocol, um dos mais utilizados atualmente. Este protocolo é utilizado por aplicativos de mensagens sendo, juntamente com criptografia assimétrica, simétrica e Double Ratchet, outro protocolo para garantir confidencialidade e sigilo para essas mensagens (Antunes e Kowada; 2018).

Segundo Marlinspike e Perrin (2016) o Signal Protocol fornece segurança de encaminhamento e confidencialidade até mesmo em caso de comprometimento de chaves de longo prazo. O Signal Protocol é dividido em duas etapas: configuração da sessão e criptografia das mensagens. A configuração da sessão consiste em "estabelecer uma chave secreta compartilhada entre os dois indivíduos a partir de um conjunto de par de chaves pública-privada" (Antunes e Kowada; 2018, p. 182); e a criptografia das mensagens, que "consiste em gerar chaves seguras de criptografia simétrica para encriptação do texto a partir da chave secreta compartilhada e par de chaves pública-privada efêmeras" (Antunes e Kowada; 2018, p.182).

Viana *et al.* (2022) afirmam que a criptografia de ponta a ponta é do tipo assimétrica, e é um método utilizado para proteger informações do tipo: texto, áudios, vídeos, fotos e ligações durante a troca de mensagens.

Beiriz e Pedras (2024), este método opera a partir de uma "chave própria de 256 bits necessário decifrá-la para que se possa ter acesso a seu conteúdo por intermédio de interceptação, contudo, devido à quantidade de bits envolvidos, se torna extremamente dificultosa a realização da interceptação (, p.88)." Existe um diálogo controverso entre o judiciário brasileiro entre os métodos utilizados na criptografia ponta a ponta.

Esse recurso de segurança também apresenta desafios e limitações que precisam ser levados em conta. Um deles é o gerenciamento de chaves criptográficas, pois o gerenciamento inadequado pode gerar acessos não autorizados, invasões de dados. Outra questão é a dificuldade de monitoramento que pode ocorrer, no ponto de vista de organizações de segurança, autoridades legais a E2EE pode ser utilizada para ações criminosas e assim dificultando investigações importantes por parte

dessas autoridades que por vezes precisam desse recurso para seguir adiante em averiguações de criminalidade.

A E2EE é utilizada em vários serviços na internet como: e-mail, compartilhamento e armazenamento de arquivos, mensagens instantâneas, transações financeiras e internet das coisas, para assim assegurar que todas essas formas de utilidade sejam resguardadas aos indivíduos que fazem uso das mesmas.

Desta forma se nota que a criptografia de ponta a ponta é cada vez mais uma forma de proteção importante para se comunicar de forma digital e certificando a privacidade dos usuários.

3.2 Criptografia de ponta a ponta e sua aplicação em plataforma do WhatsApp

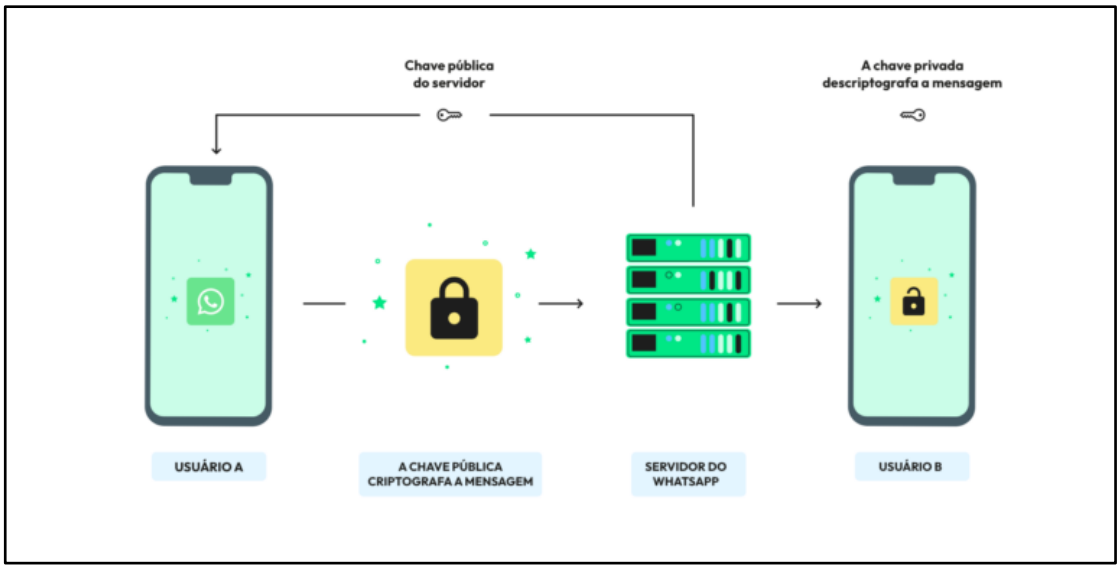
O WhatsApp é uma multiplataforma de envio de mensagens gratuitas e instantâneas, com envio de fotos, vídeos, áudios e documentos em diversos formatos, que surgiu em 2009, cuja dinâmica baseia-se na utilização do número de celular do próprio usuário como identificador exclusivo. O aplicativo conta com um sistema que se conecta aos usuários por meio da agenda telefônica, identificando automaticamente todos os contatos que também possuem o aplicativo instalado. A partir disso, é possível iniciar trocas de mensagens simples, além do compartilhamento de conteúdo mais complexos, como vídeos, imagens e documentos.

Segundo Antunes *et al.* (2018):

> a empresa (WhatsApp) fez uma parceria com a Whisper Systems para implementar o sistema de criptografia fim-a-fim chamado Signal Protocol de forma a proteger todas as mensagens transmitidas entre duas pessoas ou em um grupo com o fim de evitar qualquer acesso indevido de uma terceira pessoa aquela informação, seja ela hacker, governo ou até a própria empresa (p.2).

Segundo o documento técnico divulgado pelo WhatsApp, a criptografia de ponta a ponta (figura1) funciona como comunicações que se conectam entre um aparelho controlado por um remetente e um destinatário, neste caso terceiros não obtém acesso ao conteúdo que circula entre essa conexão, nem mesmo o WhatsApp.

Figura 1: Criptografia de ponta a ponta



Fonte:urtech.ca/

Como mostrado na imagem acima, a informação enviada pelo usuário **A** só pode ser decifrada por seu destinatário, o usuário **B**. Isso é possível graças ao par de chaves criptográficas gerado logo na primeira instalação do aplicativo no celular: uma chave pública, compartilhada com outros usuários, e uma chave privada, que fica armazenada com segurança no dispositivo. Ao iniciar uma conversa, o aplicativo realiza automaticamente a troca das chaves públicas entre os participantes, de forma discreta e segura, sem que o usuário perceba.

A mensagem é criptografada diretamente no dispositivo do remetente, tornando-se totalmente ilegível para terceiros. Em seguida, ela é enviada ao servidor do WhatsApp já protegida, garantindo que apenas o destinatário, em posse da chave privada correspondente, consiga descriptografá-la e acessar o conteúdo. O servidor do WhatsApp atua apenas como intermediário na transmissão da mensagem, sem jamais ter acesso ao conteúdo. Assim que o destinatário recebe a mensagem, utiliza sua chave privada para decodificá-la e visualizar o que foi enviado.

Conforme Brito (2024), há uma falta de comprometimento efetivo do WhatsApp em atuar de forma ágil e eficiente na remoção ou contenção desses conteúdos ilícitos. Essa postura revela uma independência excessiva e uma ausência de participação ativa no controle das informações que circulam em sua rede, contribuindo para a perpetuação de práticas que colocam em risco a segurança e a privacidade dos usuários.

4 METODOLOGIA

Este estudo segue uma abordagem qualitativa e mostrou-se adequada por permitir compreender os significados e as implicações das leis na prática sobre o vazamento de dados íntimos, investigando a aplicação da criptografia de ponta a ponta no WhatsApp e a privacidade dos usuários. Essa abordagem possibilita analisar as práticas humanas a partir de seus significados, considerando as subjetividades envolvidas e os contextos específicos em que os fenômenos ocorrem (Minayo, 2001).

O tipo de pesquisa exploratória e descritiva é justificado pela necessidade de explorar as complexas interações entre o uso da criptografia de ponta a ponta no WhatsApp e a proteção de dados no contexto jurídico brasileiro. Conforme Gil (2002), a pesquisa descritiva "é voltada para a observação, registro, análise e interpretação de fenômenos atuais" (p. 45). Assim sendo, a pesquisa descritiva foi utilizada para explorar de modo mais aprofundado como a criptografia de ponta a ponta atua na detecção de vazamentos e monitoramento proativo no WhatsApp, no contexto da legislação brasileira.

Quanto ao procedimento técnico, esta pesquisa se classifica como bibliográfica e documental. Segundo Gil (2002), “a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos” (p. 44). Enquanto a pesquisa documental: “vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa” Gil (2002, p.45).

Neste sentido, foram utilizados a análise documental da “LGPD” e “Lei Carolina Dieckman”, da jurisprudência e do documento técnico do WhatsApp. A revisão bibliográfica de artigos selecionados, a partir da utilização dos descritores: “criptografia de ponta a ponta’’, “WhatsApp”, “LGPD” e “Lei Carolina Dieckmann”, nas bases acadêmicas e nas ferramentas gratuitas de busca, como: Connected Papers, Google Acadêmico e Scielo, no período de abril à junho de 2025.

A coleta de dados foi realizada por meio da observação simples e da análise das fontes documentais, que foram analisados em busca de informações relevantes que respondam aos objetivos desta pesquisa.

5 ANÁLISE DOS RESULTADOS

A análise de resultados foi produzida a partir do levantamento bibliográfico, com base nos dados coletados a partir do exame técnico do funcionamento da criptografia de ponta a ponta e investigação do caso específico da plataforma do WhatsApp e revisão de artigos correlacionados ao tema proposto. Notou-se que a criptografia abordada e aplicada no WhatsApp, atua como uma barreira robusta contra o acesso não autorizado, transformando as mensagens em dados indecifráveis para terceiros, inclusive para o próprio servidor.

Os resultados também revelaram a tendência do WhatsApp de evitar assumir responsabilidade por vazamentos de dados e disseminação de desinformação, um exemplo disso, foi o caso da atriz Paolla Oliveira (figura 2).

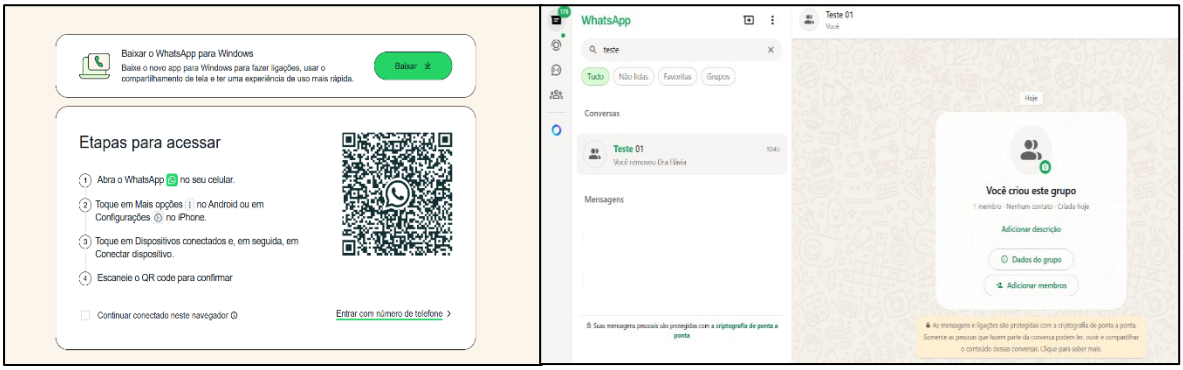
Figura 2: Vazamento de dados – Paolla Oliveira

Fonte: Folha de São Paulo – 01 de março 2018

A atriz Paolla Oliveira foi vítima de um grave vazamento de imagens íntimas, ocorrido em seu local de trabalho. Durante a gravação de uma cena da série “Assédio”, a atriz foi surpreendida por um indivíduo que registrou, de forma criminosa e sem seu consentimento, imagens suas de um momento reservado. Paolla formalizou denúncia junto às autoridades competentes e reforçou uma mensagem essencial: toda pessoa deve ter o direito de exercer sua atividade profissional com

respeito, dignidade e segurança, sem ser exposta ou explorada de maneira alguma. Assim, com a identificação deste conteúdo, para garantir o direito da vítima poderiam ser utilizados artifícios de mapeamento da URL para descobrir os usuários responsáveis por essa disseminação. Brito (2024) apresenta uma metodologia sugerida pela Secretaria Nacional de Segurança Pública, que tem como objetivo identificar a URL de encaminhamento de uma mídia pública do WhatsApp, conforme imagens apresentadas abaixo (figuras 2 a 6).

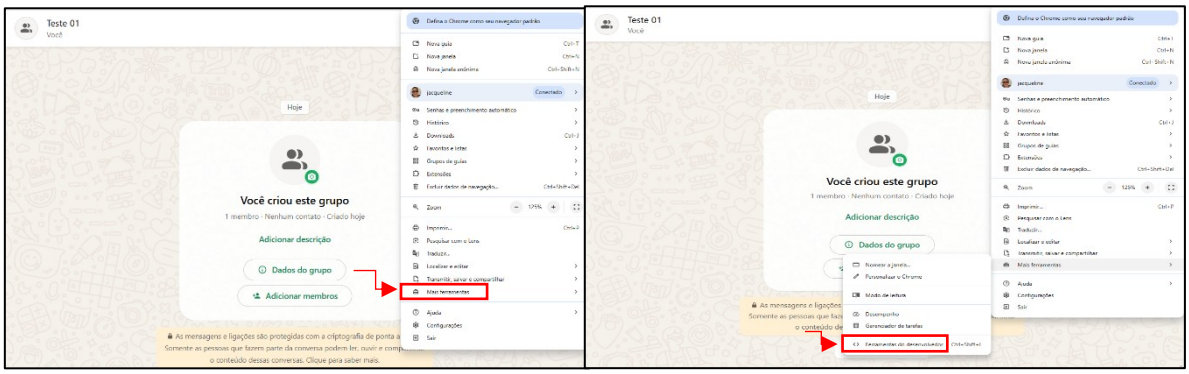
Figura 2 – Acesso inicial a página do WhatsApp Web e Criação de grupo “teste 01”



Fonte: Elaborado pelas autoras

Acesse o WhatsApp Web por meio do navegador Google Chrome. Em seguida, crie um grupo de teste, nomeado como “teste 01”, com o objetivo de encaminhar a mídia considerada ilícita. Esse procedimento é fundamental para facilitar a identificação rápida da URL do arquivo que se deseja localizar.

Figura 3 – Seleção da opção “Mais ferramentas” e depois “Ferramentas do desenvolvedor”

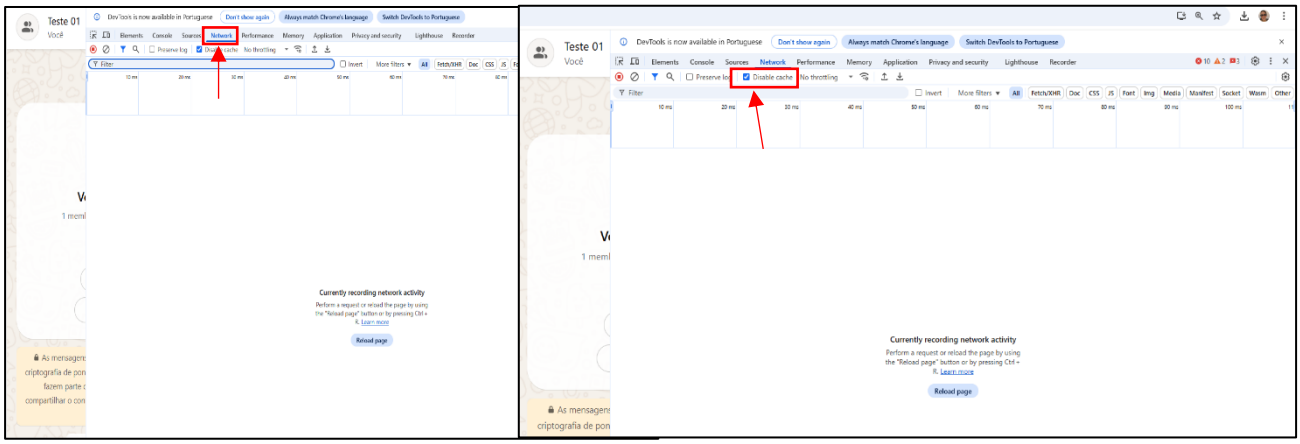


Fonte: Elaborado pelas autoras

Clique na parte superior direita na janela do Google, na barra de ferramentas do browser, em seguida acesse “mais ferramentas” e após clicar em “mais ferramentas”, clique em “ferramentas do desenvolvedor”. Esse processo tem como propósito abrir a janela “Network” para analisar neste caso, o tráfego de carregamento

de arquivos entre o navegador e os servidores enquanto a página é carregada ou está em uso.

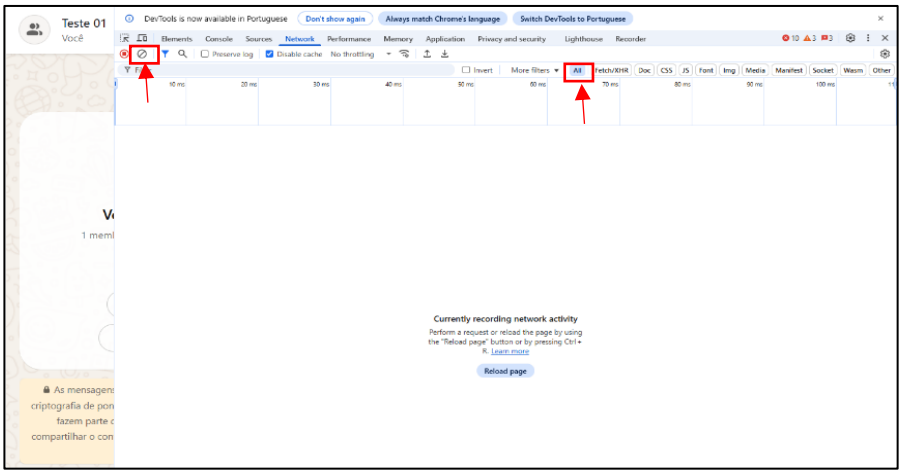
Figura 4 – Seleção da opção “Network” e “Disable cache”



Fonte: Elaborado pelas autoras

Na nova janela aberta selecione o botão “Network” após isso marque a opção “disable cache”. Ativando a opção disable cache, há uma garantia que todas as requisições sejam novas e atuais, para assegurar que o processo não seja influenciado por dados antigos do cache, está função é acionada para depurar as requisições de rede e manter sempre a versão mais atual do conteúdo, neste caso, o carregamento dos arquivos.

Figura 5 – Seleção da opção “All” e “clear”

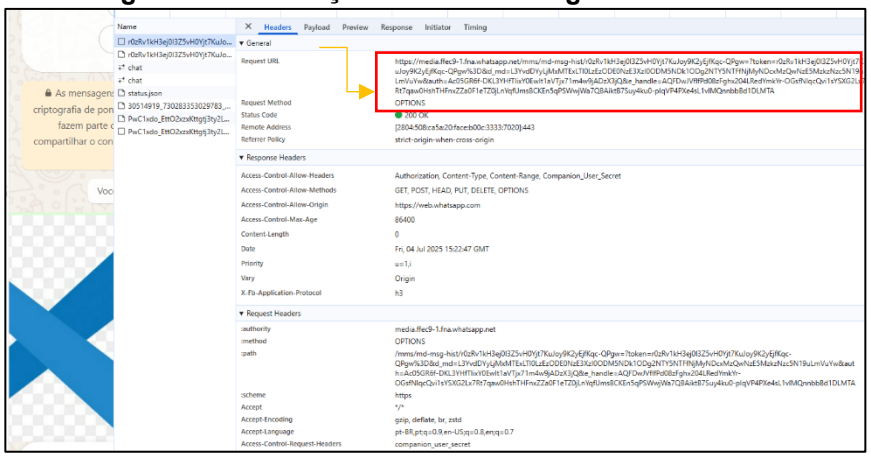


Fonte: Elaborado pelas autoras

Logo após selecione todos os arquivos clicando em “All” e faça a limpeza clicando em “clear”. Pronto, a mídia “ilícita” já pode ser enviada para o grupo teste. Este filtro “All” é padrão para exibição de todas as requisições de rede feita pela página, é usado para ter uma visão completa de tudo que está sendo carregado, a

função do botão “clear” representado pela bola cortada, é limpar a lista de requisições atuais da aba Network, usado para despoluir a visibilidade de uma nova tentativa de carregamento de dados.

Figura 6 – Verificação da URL da imagem “ilícita”



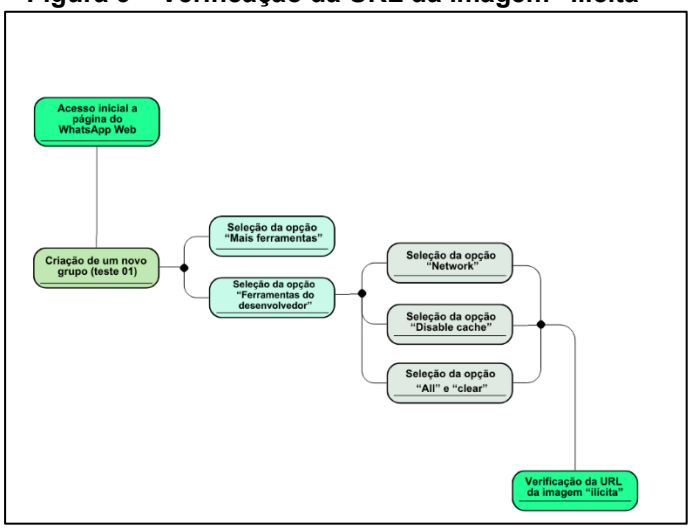
Fonte: Elaborado pelas autoras

Assim que a imagem é carregada vai aparecer algumas URLs na aba “Name”, a URL do arquivo encriptado será aquela com a transcrição blob:https://web.watsapp.com/**********. Ao selecionar o arquivo é possível copiar a URL com a identificação do mesmo, neste processo o objetivo é observar uma comunicação do WhatsApp e os seus servidores, apresentando os dados trocados entre o navegador e o back-end da aplicação, observa-se request URL, é o endereço completo da API da chamada.

Conforme Brito (2024) com a URL de encaminhamento sucessivo da mídia contestada em mãos, basta representar à autoridade policial ou judiciária para solicitar seu bloqueio ou suspensão junto ao WhatsApp. É importante criar um grupo específico para analisar essas mídias pelo WhatsApp Web. Este procedimento é usado para conseguir localizar a URL do arquivo, caso o arquivo representado não apareça na aba “Name” deve-se limpar o histórico do navegador e reiniciar o processo. Com a URL (identificador inequívoco de conteúdo - art. 19, §1º, MCI), encaminha-se para o judiciário para que o aplicativo bloquei o encaminhamento em massa da mídia contestada, como também, forneça o registro de acesso do autor responsável referente ao upload do arquivo. Baseando-se no caso de Paolla Oliveira seguindo este passo a passo e localizando a URL do arquivo, as autoridades poderiam localizar os usuários responsáveis por fomentar essa exposição íntima da atriz.

É apresentado abaixo um fluxograma que resume as ações para detectar a URL que contém uma mídia ilícita no WhatsApp, usando as ferramentas do desenvolvedor do Google Chrome (DevTools), este fluxo representa um procedimento de análise técnica e forense, para coleta de URL da imagem suspeita como uma evidência digital, neste caso com propósito de uma investigação para remoção de conteúdo sensível.

Figura 6 – Verificação da URL da imagem "ilícita"



Fonte: Elaborado pelas autoras

Diante de um comparativo com outras plataformas, como por exemplo o Telegram e Signal, que são outros aplicativos de troca de mensagens instantâneas, com o uso da criptografia de ponta a ponta (E2EE), observa-se diferenças consideráveis quanto á proteção de dados pessoais e a aderência aos princípios da LGPD. Com isso apresenta-se um esquema comparativo entre essas três plataformas, considerando elementos técnicos e jurídicos entre elas:

Figura 7 – Quadro comparativo de plataformas

Plataforma	Criptografia Padrão	Armazenamento em Nuvem	Aderência à LGPD e riscos
WhatsApp	Padrão de mensagens e chamadas por sistema E2EE	São feitos backups opcionais em nuvem (sem criptografia por padrão)	Política de privacidade adaptada à LGPD, porém criticada pela integração com o Facebook e pelo uso intensivo de metadados.
Telegram	Não utiliza o sistema E2EE como padrão (exclusivo para chats secretos)	Armazenamento voltado há servidores próprios	Baixo índice na transparência no tratamento de dados, não é adepto aos princípios da minimização e objetivo geral da LGPD; alto risco jurídico.
Signal	Utiliza o sistema E2EE em todas as comunicações, inclusive em metadados minimizados	Não realiza backups automáticos, nem coleta de dados sensíveis	Alto índice de aderência à LGPD e as diretrizes de privacidade; considerado o mais seguro e transparente.

Fonte: Elaborado pelas autoras

O comparativo permeia uma discussão mais aprofundada sobre as limitações da criptografia, sobre tudo neste contexto de crimes digitais. Uma das principais discussões é que ao impedir a terceiros ou até os próprios provedores, que tenham acesso aos conteúdos dos dados violados, ele dificulta as investigações criminais. Outro ponto forte por exemplo é quando o dispositivo do usuário é comprometido, por meio de malwares, spoofing, técnica de phishing ou engenharia social, os invasores podem ter acesso ao dispositivo antes da criptografia ser aplicada (no envio) ou após a descriptografia (na visualização da mensagem). Isto expõe outra problemática importante, que a segurança destes dados não reside apenas na criptografia, mas também no ambiente e na prática que este mecanismo é executado. Posto isso, há um conflito entre a proteção de dados privados individuais e segurança pública, aumentando a necessidade de soluções técnica, como procedimentos de auditoria criptográfica, interceptação técnica com supervisão dos poderes legais e a cooperação das empresas e autoridades, dentro das conformidades da LGPD. Diante de todo o conteúdo que reverbera este trabalho, expõe como exemplo a própria plataforma do WhatsApp, que majoritariamente das vezes isenta-se da responsabilidade em relação a esses casos. Para mostrar na prática um destes

casos, cita-se o processo REsp 2.172.296/RJ – pornografia de vingança e responsabilidade civil do WhatsApp, no qual houve a divulgação de imagens íntimas de uma menor de idade por um usuário da plataforma, sem seu consentimento. A vítima buscou a justiça para remoção do conteúdo e indenização por danos morais. No 1º grau, houve apenas a responsabilização do autor do compartilhamento, na 2ª instância houve a condenação do WhatsApp por danos morais, em caráter solidário, diante da condenação a plataforma recorreu declarando incapacidade e limitação técnica para a remoção das imagens íntimas, que neste caso seria a criptografia de ponta a ponta. Como resposta a corte negou a alegação de “incapacidade técnica”. E que caso fosse realmente inviável a exclusão do conteúdo o provedor deveria encontrar soluções alternativas, como bloqueio e suspensão de conta dos infratores, que diante dos termos de serviço e política de privacidade do WhatsApp, são identificados a partir do número de telefone.

Com isso a relatora, Ministra Nancy Andrighi, destacou:

> RECURSO ESPECIAL. PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZATÓRIA POR DANOS MORAIS. MARCO CIVIL DA INTERNET. QUESTÃO DE ORDEM. PEDIDO DE DESISTÊNCIA. "LEADING CASE". INTERESSE PÚBLICO. PROTEÇÃO DE MENOR CONTRA PORNOGRAFIA DE VINGANÇA. NÃO HOMOLOGAÇÃO. EMBARGOS DE DECLARAÇÃO. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. NEGATIVA DE PRESTAÇÃO JURISDICIONAL. NÃO OCORRÊNCIA. COMPARTILHAMENTO DE IMAGENS ÍNTIMAS SEM AUTORIZAÇÃO. APLICATIVO DE MENSAGERIA PRIVADA. CRIPTOGRAFIA. ORDEM DE REMOÇÃO DE CONTEÚDO COM IDENTIFICAÇÃO DO USUÁRIO INFRATOR. IMPOSSIBILIDADE TÉCNICA NÃO COMPROVADA. ELIMINAÇÃO OU MITIGAÇÃO DO DANO. ADOÇÃO DE MEDIDAS TÉCNICAS EQUIVALENTES. POSSIBILIDADE EM TESE. DESÍDIA CONFIGURADA. RESPONSABILIDADE SOLIDÁRIA. (...) 10. Não é razoável deixar vítimas de pornografia de vingança (especialmente se menores de idade) à mercê do "paradoxo da segurança digital" – i.e., quanto mais segura for a técnica de compartilhamento de conteúdo infrator, mais inseguras estão as vítimas dos abusos perpetrados por usuários que utilizam a robustez do sistema de mensageria privada para fins ilícitos. (BRASIL. STJ. REsp 2.172.296/RJ, Rel. Min. Nancy Andrighi, j. 04 fev. 2025).

O processo conclui-se, com a confirmação da indenização solidária do WhatsApp por não remover o conteúdo ilícito após ser solicitado, a consolidação do viés que se os provedores com E2EE não possuírem métricas de remoção do conteúdo, ao menos possam bloquear e suspender as contas dos infratores, ao serem identificadas. Ao final do julgamento a 3ª turma, após voto da relatora, decidiu negar o provimento ao recurso especial solicitado pela empresa, e manteve a decisão do pagamento da indenização solidária. Diante disto nota-se que existe ainda uma lacuna entre a robustez do ponto de vista técnico e judicial e mais ainda, a falta de

conscientização dos usuários e a disseminação de práticas simples, que podem auxiliar a um retorno mais eficiente diante de casos de vazamentos de dados, buscando de uma forma mais eficaz a justiça para uma resolução mais direta e rápida. Em síntese os resultados mostram a necessidade de uma prática multidisciplinar, com a integração da tecnologia, legislação, educação digital e não menos importante a responsabilização do aplicativo WhatsApp em relação aos casos de vazamentos e exposição de dados íntimos, já que a partir de pesquisas concisas há formas e métricas independentes que podem otimizar do processo de descoberta das fontes originárias dessas informações e vazamentos.

6 CONSIDERAÇÃO FINAL

Este projeto teve por objetivo aprimorar o entendimento e a eficácia da legislação brasileira no que diz respeito ao vazamento de dados íntimos investigando a aplicação da criptografia de ponta a ponta no WhatsApp. Os resultados deste estudo revelam que embora o WhatsApp ofereça uma estrutura técnica robusta contra acessos não autorizados, ainda enfrenta desafios significativos, sobretudo no que diz respeito ao rastreamento e à remoção de conteúdos ilícitos. Essas dificuldades não se devem à ausência de métodos técnicos ou de processos capazes de identificar tais conteúdos, mas sim à falta de políticas claras e de métricas efetivas por parte do WhatsApp para aplicar esses recursos de forma consistente e que atendam a legislação brasileira.

Torna-se evidente, portanto, a necessidade urgente de que a plataforma assuma uma postura mais ativa e responsável, através do desenvolvimento de tecnologias de permitam o rastreamento dentro do WhatsApp, facilitando a identificação e a rápida remoção de materiais sensíveis, em conformidade com as legislações vigentes e com respeito aos direitos fundamentais dos usuários. Somente através dessa integração será possível reduzir efetivamente os casos de vazamento de dados íntimos (BRITO, 2024), garantindo a proteção dos direitos fundamentais de privacidade e segurança, especialmente das mulheres que são as maiores vítimas desses crimes atualmente. O sentimento de exposição e vulnerabilidade que acompanha essas situações evidencia não apenas uma falha técnica ou jurídica, mas uma violação direta da dignidade humana. A impunidade e a lentidão nos processos

de remoção e responsabilização reforçam um ciclo de violência digital que precisa ser combatido com urgência.

No que se refere às leis LGPD e Lei Carolina Dieckmann, ambas se mostraram efetivas quando são aplicadas de forma associada, pois enquanto a primeira foca na proteção civil no âmbito digital a outra criminaliza fatos mais específicos, que neste caso são as invasões e violações de dispositivos.

Ainda este estudo destaca a importância do investimento em políticas públicas voltadas à segurança cibernética, bem como a necessidade de ampliar a disseminação de cartilhas educativas, conteúdos informativos que orientem os usuários sobre medidas preventivas e sobre os passos necessários caso se tornem vítimas desse tipo de crime. A adoção de boas práticas de privacidade, aliada à conscientização digital, configura-se como um caminho essencial para o enfrentamento desse problema social que, infelizmente, atinge de forma desproporcional as mulheres, não apenas no Brasil, mas em todo o mundo.

REFERÊNCIAS

ANTUNES, Igor; KOWADA, Luis Antonio. **Explorando o Sistema de Criptografia Signal no WhatsApp**. *In*: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18. , 2018, Natal. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018 . p. 181-195.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Altera o Código Penal, para tipificar crimes informáticos, conhecidos como Lei Carolina Dieckmann. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 2 jul. 2025.

BEIRIZ, Hudson Colodetti; PEDRA, Adriano Sant'Ana. **Criptografia de ponta a ponta no WhatsApp e deveres fundamentais de colaboração com a segurança pública e de cooperação judicial.** Revista Jurídica Cesumar - Mestrado, *[S. l.]*, v. 24, n. 1, p. 85–97, 2024. DOI: 10.17765/2176-9184.2024v24n1.e11387. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/11387. Acesso em: 30 maio 2025.

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. Crimes cibernéticos: **da ineficácia da lei carolina dieckmann na prática de crimes virtuais**. Revista Ibero-Americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 9, n. 11, p. 354–369, 2023. DOI: 10.51891/rease.v9i11.12291. Disponível em: https://periodicorease.pro.br/rease/article/view/12291. Acesso em: 07 de julho 2025.

BORGES, Matheus Barroso; NOVAIS, Thyara Gonçalves. **Desafios da legislação brasileira em relação aos crimes cibernéticos: uma análise das deficiências atuais.** Revista Ibero-Americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 10, n. 5, p. 4936–4956, 2024. DOI: 10.51891/rease.v10i5.14142. Disponível em: https://periodicorease.pro.br/rease/article/view/14142. Acesso em: 7 jul. 2025. Acesso em : 05 de maio de 2025.

BRASIL. Superior Tribunal de Justiça. REsp 2.172.296/RJ. Rel. Min. Nancy Andrighi**.** 3ª Turma. Julgado em 04 fev. 2025. Disponível em: https://processo.stj.jus.br/. Acesso em: 06 jul. 2025.

BRITO, Jorge Messias de. **Mídia ilícita no WhatsApp: uma análise da Representação Eleitoral nº 601686-42.2018 à luz do Marco Civil da Internet**. **Revista Sociedade Científica**, *[S. l.]*, v. 7, n. 1, p. 1920–1942, 2024. DOI: 10.61411/rsc202441917. Disponível em: https://journal.scientificsociety.net/index.php/sobre/article/view/419.. Acesso em: 2 jul. 2025.

D'OLIVEIRA, Nadine Passos Conceição ;CUNHA, Francisco José Aragão Pedroza. Lei Geral de Proteção de Dados (LGPD): a relação entre as políticas e os regimes de informação.RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação, Campinas, SP, v. 22, p.10, 2024.
Disponível em :https://www.scielo.br/j/rdbci/a/DWntpkXMB9GgCPKycFcxtts/abstract/?lang=pt
Acesso em : 25 de Abril de 2025.

FERNANDES, Clara. *Entendendo a segurança de dados no WhatsApp: criptografia de ponta a ponta e backups*. Wati, 16 set. 2024. Disponível em: https://www.wati.io/blog/whatsapp-seguranca-dados/. Acesso em: 2 jun. 2025.
GIL, Antônio Carlos. **Como elaborar projetos de pesquisa** 4. ed. - São Paulo: Atlas, 2002

MACHADO, Rafael Lopes Kassem; DUARTE, Neuziane Lima. Crimes Cibernéticos, Invasão de Privacidade e a Efetividade Da Resposta Estatal: os impactos da lei 12.737/2012 – Lei Carolina Dieckmann e da Lei Geral de Proteção de Dados no combate aos crimes cibernéticos de invasão de privacidade. **PROJEÇÃO, DIREITO E SOCIEDADE**, *[S. l.]*, v. 12, n. 2, p. 1–16, 2021. Disponível em: https://projecaociencia.com.br/index.php/Projecao2/article/view/1798. Acesso em: 2 jul. 2025.

MARLINSPIKE, Moxie; PERRIN, Trevor. The Double Ratchet Algorithm. Whisper Systems, 2016 (revisão 1, novembro de 2016). Disponível em: https://signal.org/docs/specifications/doubleratchet/.Acesso em: 2 jul. 2025.

MINAYO, Maria Cecília de Souza (org.). **Pesquisa Social. Teoria, método e criatividade**. 18 ed. Petrópolis: Vozes, 2001.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. Lei Geral de Proteção de Dados e repositórios institucionais: reflexões e adequações. Em Questão, Porto Alegre, v. 29, e-127314, 2023. Disponível em:. https://www.scielo.br/j/emquestao/a/w3xQNy4bnytwK6MxzgyKgsy/ Acesso em: 30 maio. 2025.

NORTE FILHO, A. F. do; SOUZA, D. de L.; CONSIGLIO, Y. M.; RIBEIRO, J. V. N. dos S.; GONÇALVES, B. C. C.; ROSÁRIO JUNIOR, B. G. E. do; SIMAS, D. C. de S. Proteção legal contra crimes virtuais: o enfrentamento da violência digital contra mulheres. CONTRIBUCIONES A LAS CIENCIAS SOCIALES, *[S. l.]*, v. 17, n. 10, p. e11922, 2024. DOI: 10.55905/revconv.17n.10-344. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/11922. Acesso em: 8 jul. 2025.

VIANA, C.; DATTEIN, G.; SILVA, J. V.; CAMPOS, P. CRIPTOGRAFIA E SEGURANÇA. **Revista Científica e-Locução**, v. 1, n. 22, p. 30, 2022.Disponivel em : https://periodicos.faex.edu.br/index.php/e-Locucao/article/view/506 Acesso em: 06 de jul. de 2025.

VOITECHEN, Dainara Aparecida. Análise e comparação de algoritmos para criptografia de imagens. 2020. Trabalho de conclusão de curso (Graduação em Ciência da Computação) – Universidade Tecnológica Federal do Paraná, Campus Cornélio Procópio, 2020. Disponível em: [repositório da UTFPR]. Acesso em: 2 jul. 2025.

UNIVERSIDADE DO ESTADO DA BAHIA - UNEB
DEPARTAMENTO DE CIÊNCIAS EXATAS E DA TERRA – CAMPUS II
CURSO: BACHARELADO DE SISTEMAS DE INFORMAÇÃO
COMPONENTE CURRICULAR: TRABALHO DE CONCLUSÃO DE CURSO

ATA DA SESSÃO DE DEFESA PÚBLICA DE TRABALHO DE CONCLUSÃO DE CURSO, DO CURSO DE BACHARELADO DE SISTEMAS DE INFORMAÇÃO DO PRIMEIRO SEMESTRE 2025.

No dia trinta e um de julho, às dez horas, no auditório do Departamento de Ciências Exatas e da Terra – Campus II, Universidade Estado da Bahia - UNEB, reuniu-se a Banca Examinadora composta pelo(a) professor(a) **José Roberto de Araújo Fontoura** (presidente da mesa e orientador(a)), professor(a) **Elaine Pereira Garrido** (professor(a) convidado(a)) e professor(a) **Roberto Luiz Souza Monteiro** (professor(a) co), para avaliar o Trabalho de Conclusão de Curso (artigo acadêmico), do(a) discente **JACQUELINE SANTOS COSTA e JÉSSICA SANTANA DOS SANTOS** intitulado **"CRIPTOGRAFIA DE PONTA A PONTA E PROTEÇÃO DE DADOS ÌNTIMOS NO BRASIL: ANÁLISE JURÍDICA E TÉCNICA DO WHATSAPP "** O presidente da Banca Examinadora abriu a sessão com os cumprimentos ao(a) candidato(a), aos demais membros da banca, esclarecendo, também, o caráter do evento e respectivas normas. A seguir, foi concedida a palavra ao autor do trabalho para apresentação por vinte minutos. Após esta exposição, os membros da Banca Examinadora realizaram suas considerações emitindo sugestões ao trabalho apresentado e em seguida à palavra foi devolvida ao(a) candidato(a). Após as necessárias considerações ao trabalho, a banca examinadora reuniu-se e o (a) professor(a) José Roberto de Araújo Fontoura atribuiu nota 9,5_ (Nove vírgula cinco), o(a) professor(a) **Elaine Pereira Garrido** atribuiu nota 9,0 (Nove) e o(a) professor(a) **Roberto Luiz Souza Monteiro** atribuiu nota 8,5(Oito virgula cinco). Para registro e finalidades legais, eu **Prof. José Roberto de Araújo Fontoura**, presidente da banca, lavrei a presente Ata que será assinada por mim e demais membros da Banca Examinadora.

Alagoinhas, 31 de julho de dois mil e vinte cinco.

gov.br Documento assinado digitalmente
JOSE ROBERTO DE ARAUJO FONTOURA
Data: 30/11/2025 21:56:59-0300
Verifique em https://validar.iti.gov.br

_____

Profº. José Roberto de Araújo Fontoura

Presidente da mesa e orientador(a)

gov.br Documento assinado digitalmente
ELAINE PEREIRA GARRIDO
Data: 30/11/2025 22:04:16-0300
Verifique em https://validar.iti.gov.br

_____

Profº Elaine Pereira Garrido

Professor(a) Convidado(a)

gov.br Documento assinado digitalmente
ROBERTO LUIZ SOUZA MONTEIRO
Data: 01/12/2025 06:16:08-0300
Verifique em https://validar.iti.gov.br

_____

Profº. Roberto Luiz Souza Monteiro

Professor(a) Convidado(a)