UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ)
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS (CCJE)
FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS (FACC)
CURSO DE BIBLIOTECONOMIA E GESTÃO DE UNIDADE DE INFORMAÇÃO (CBG)

PEDRO TAETS HOLSBACK DA ROSA

COMO OS APLICATIVOS DE MENSAGEM VIABILIZAM A PROPAGAÇÃO DE INFORMAÇÕES FALSAS

Rio de Janeiro
2023

PEDRO TAETS HOLSBACK DA ROSA

COMO OS APLICATIVOS DE MENSAGEM VIABILIZAM A PROPAGAÇÃO DE INFORMAÇÕES FALSAS

Trabalho de Conclusão de Curso apresentado ao Curso de Biblioteconomia e Gestão de Unidades de Informação da Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de bacharel em Biblioteconomia e Gestão de Unidades de Informação.

Orientador: Prof. Danilo Pestana de Freitas

Rio de Janeiro

2023

Ficha catalográfica

Rosa, Pedro Taets Holsback da
R789 Como os aplicativos de mensagem viabilizam a propagação de informações falsas / Pedro Taets Holsback da Rosa. – Rio de Janeiro, 2023.
45 f

Trabalho de conclusão de curso (graduação) – Universidade Federal do Rio de Janeiro, Faculdade de Administração e Ciências Contábeis, Bacharel em Biblioteconomia e Gestão de Unidades de Informação, 2022.

Orientador: Danilo Pestana de Freitas

1. Aplicativos de Mensagem. 2. Informações Falsas. 3. Desinformação. 4. Aplicativos. I. Freitas, Danilo Pestana de, oriente. II. Título.

CDD: 005.3072
CDU:316.773.331.677.632:316.776.23

PEDRO TAETS HOLSBACK DA ROSA

COMO OS APLICATIVOS DE MENSAGEM VIABILIZAM A PROPAGAÇÃO DE INFORMAÇÕES FALSAS

Trabalho de Conclusão de Curso apresentado ao Curso de Biblioteconomia e Gestão de Unidades de Informação da Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de bacharel em Biblioteconomia e Gestão de Unidades de Informação.

Rio de Janeiro, ____ de ____ de 20____.

_____
Prof. Dr. Danilo Pestana De Freitas (UFRJ)
Orientador

_____
Prof. Dr. Ana Maria Ferreira De Carvalho (UFRJ)
Membro interno

_____
Prof. Dr. Nysia Oliveira De Sá (UFRJ)
Membro interno

Dedico esse trabalho a todos os animais que me acompanharam e não estão mais aqui,
Luna, Sophia, Poly e Pandora. Eu sempre vou amar todas vocês.
E também dedico a nova membra da Família a Mary Jane.

AGRADECIMENTOS

Agradeço a todos que fizeram essa jornada da minha vida um pouco mais leve, sobretudo que me fizeram companhia pelos momentos especiais que vivi.

RESUMO

O presente trabalho de conclusão de curso tem como objetivo investigar como os aplicativos de mensagens viabilizam a propagação de informações falsas. A crescente preocupação acerca do tema nos leva a debruçarmos sobre o tema, a fim de entender quais são os males trazidos através dos aplicativos de mensagem. Nesse estudo será realizada uma análise sobre a desinformação, além de sobre aplicativos de mensagens e seus meios de compartilhar informações falsas protegendo os agentes que compartilham a desinformação. Foram obtidos resultados mediante a capacidade de compartilhamento de cada aplicativos e sobre a criptografia que os protege, junto a uma análise sobre a as motivações que tiveram os criadores de cada aplicativo e como essas motivações são importantes em discussões acerca das regulamentações que podem ser impostas em cada aplicativo. Por fim, serão discutidas possíveis estratégias e soluções para mitigar a propagação de informações falsas nesses aplicativos, envolvendo ações dos usuários, das empresas desenvolvedoras e das autoridades regulatórias. Para embasar a pesquisa, serão utilizados estudos acadêmicos, notícias de jornais, relatórios de organizações especializadas e exemplos concretos de desinformação e suas consequências.

Espera-se que este estudo contribua para um melhor entendimento sobre como os aplicativos de mensagens podem ser utilizados como ferramentas para a disseminação de informações falsas, incentivando a conscientização e a busca por soluções efetivas para lidar com esse desafio crescente na era da comunicação digital.

Palavras-chave: Aplicativos de Mensagem. Informações Falsas. Desinformação. Aplicativos.

ABSTRACT

This course completion paper aims to investigate how messaging applications enable the spread of false information. The growing concern about the subject leads us to look into the topic, in order to understand what are the evils brought about by messaging applications. In this study, an analysis will be made about disinformation, as well as about messaging applications and their means of sharing false information, protecting the agents who share the disinformation. Finally, possible strategies and solutions to mitigate the spread of false information in these applications will be discussed, involving actions by users, developers and regulatory authorities. To support the research, academic studies, newspaper reports, reports from specialized organizations and concrete examples of disinformation and its consequences will be used. It is expected that this study will contribute to a better understanding of how messaging applications can be used as tools for the dissemination of false information, encouraging awareness and the search for effective solutions to deal with this growing challenge in the age of digital communication.

Keywords: Messaging Applications. Fake Information. Misinformation. Apps.

SUMÁRIO

1 INTRODUÇÃO

No mundo contemporâneo, os avanços tecnológicos provocam uma transformação significativa na forma como nos comunicamos e compartilhamos informações. A revolução implementada pelos telefones inteligentes foi sem dúvidas uma nova era para a humanidade. Os meios de comunicação nunca foram tão ágeis em entregar informações independentemente da localização de cada indivíduo no planeta. Em alguns segundos pode-se disparar incontáveis informações para outros incontáveis usuários, estabelecendo um fluxo informacional imensurável.

Os aplicativos de mensagem, também conhecidos como mensageiros, como WhatsApp, Telegram e Facebook Messenger, tornaram-se parte essencial do cotidiano de milhões de pessoas ao redor do mundo, por serem algumas das plataformas que revolucionaram a comunicação. Essas plataformas oferecem uma maneira rápida, conveniente e acessível de trocar mensagens, imagens e vídeos com amigos, familiares e até mesmo com desconhecidos. No entanto, o crescente poder e alcance desses aplicativos também têm despertado preocupações em relação à disseminação de informações falsas ou desinformação.

As informações falsas são relatos enganosos, incorretos ou enganosos que podem levar ao surgimento de crenças equivocadas, preconceitos e, em alguns casos, até mesmo consequências letais para a sociedade. A propagação de informações falsas pode ocorrer de várias maneiras, mas os aplicativos de mensagem se destacam como um dos principais veículos para a disseminação dessas informações. Com a popularização desses aplicativos, a democratização do acesso à Internet e a democratização dos dispositivos eletrônicos capazes de utilizar aplicativos de mensagem, a capacidade de compartilhamento se torna incalculável.

Dito isso, a análise sobre os mensageiros se faz necessária a fim de compreender suas capacidades na hora do compartilhamento de informações falsas. Sobretudo, uma análise sobre a criação dos aplicativos mais usados no Brasil, para se obter informações acerca da motivação a qual cada aplicativo foi construído com suas respectivas funcionalidades. Junto isso devemos nos debruçar sobre as questões que levam aos agentes compartilhadores de desinformação a nunca serem rastreados pelas plataformas ou até órgãos governamentais.

Tudo isso para que se possa compreender por completo a estrutura do compartilhamento de informações falsas mediante de aplicativos de mensagem, e assim promover ideias para impedir a disseminação desenfreada de informações enganosas. Ademais, para que possamos um dia recuperar a confiança em notícias e informações recebidas por parentes e amigos, através de mecanismos que viabilizem a checagem de veracidade das informações recebidas.

1.1 PROBLEMA

Levando em conta o alcance que aplicativos de mensagem possuem na sociedade contemporânea brasileira, a abrangência que uma informação falsa pode atingir é imensurável. Esses aplicativos possuem ferramentas que viabilizam a propagação de desinformação irrastreável, assim facilitando que toda e qualquer informação enganosa possa ser encaminhada sem punições.

1.2 JUSTIFICATIVA

A compreensão das funcionalidades dos aplicativos de mensagem, em relação ao compartilhamento de informações, e a análise da proteção oferecida pelas plataformas aos agentes que disseminam informações falsas são elementos cruciais para combater a propagação da desinformação. Dada a alta taxa de usuários que utilizam regularmente esses aplicativos, torna-se ainda mais necessário examinar como essas plataformas facilitam a disseminação de informações falsas, a fim de conter o compartilhamento de conteúdo enganoso. Essa análise permite identificar possíveis melhorias nas políticas e práticas das plataformas, buscando uma maior responsabilização dos agentes envolvidos na disseminação de informações falsas. i)

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

O objetivo primordial desse trabalho é compreender como aplicativos de mensagem permitem que informações falsas sejam compartilhadas através de seus mecanismos de compartilhamento e proteção criptográfica.

1.3.2 OBJETIVOS ESPECÍFICOS

a) Compreender informação e informação falsa;

b) Entender, através de exemplos, como as informações falsas afetam indivíduos de formas diferentes;

c) Compreender a história da criação, funcionalidades, capacidade de compartilhamento e criptografia dos aplicativos de mensagem mais utilizados no Brasil;

d) Analisar como as informações falsas influenciam na propagação de desinformação.

2 PROCEDIMENTOS METODOLÓGICOS

Com o intuito de atingir os objetivos previamente delineados, optou-se pela adoção da metodologia de pesquisa bibliográfica, que consiste em explorar e analisar diversas fontes de informação disponíveis em diferentes materiais bibliográficos, como livros, artigos científicos, teses, dissertações, relatórios, periódicos, documentos eletrônicos, etc.. “A pesquisa bibliográfica busca a resolução de um problema (hipótese) por meio de referenciais teóricos publicados, analisando e discutindo as várias contribuições científicas” (BOCCATO, 2006) além disso, o mesmo autor sugere que “Esse tipo de pesquisa trará subsídios para o conhecimento sobre o que foi pesquisado, como e sob que enfoque e/ou perspectivas foi tratado o assunto apresentado na literatura científica” (BOCCATO, 2006). Em outras palavras, durante a pesquisa bibliográfica, o pesquisador busca identificar, selecionar e coletar as obras relevantes para a sua investigação. Esse processo envolve a realização de uma leitura crítica e analítica dos textos encontrados, com o intuito de extrair informações pertinentes, comparar diferentes perspectivas, identificar lacunas no conhecimento e estabelecer relações entre os conceitos abordados.

O artigo “A pauta da desinformação: "fake news" e análise de categorizações de pertencimento na eleição presidencial brasileira em 2018” de Mônica Chaves e Adriana Braga foi fundamental para a base do trabalho junto da pesquisa “Mensageria no Brasil” da Panorama Mobile Time/Opinion Box. Ambos forneceram informações relevantes que se alinharam com os objetivos propostos ao trabalho como um todo. O objeto de estudo utilizado para esse trabalho foram os aplicativos de mensagem: WhatsApp, Telegram, Facebook Messenger, Instagram Direct e Signal. A escolha deles foi baseada na pesquisa Mensageria no brasil (PANORAMA MOBILE TIME/OPINION BOX, 2023) que apontou os principais aplicativos utilizados no Brasil, que são justamente os mencionados anteriormente. Os dados sobre a desordem da informação e crise da credibilidade do jornalismo estão presentes na pauta da desinformação: "fake news" e análise de categorizações de pertencimento na eleição presidencial brasileira em 2018 (CHAVES; BRAGA, 2019).

Além disso, artigos de jornais foram utilizados para informações referentes aos estudos de casos sobre vítimas de informações falsas e ao agrupamento de informações sobre aplicativos de mensagens. Fontes como UOL e Globo, assim como fontes internacionais, foram utilizadas para extrair informações sobre os episódios das vítimas quanto para fundamentar pontos de importância para a história dos aplicativos. E por fim, fora utilizado os sites oficiais de cada aplicativo respectivamente para que se obtivesse informações acerca de suas funcionalidades e criptografia.

3 DESENVOLVIMENTO

3.1 O INÍCIO DA ERA DA INFORMAÇÃO

A informação desempenha um papel essencial na sociedade contemporânea, e a internet, que teve sua origem na Arpanet como uma rede de comunicação militar e transmissão de dados sigilosos entre departamentos governamentais (MDN WEB DOCS, 2022), evoluiu para se tornar uma poderosa ferramenta global de transmissão de dados e comunicação em larga escala. Atualmente, a internet é acessível em escala global e utilizada por pessoas ao redor do mundo através de uma ampla variedade de dispositivos habilitados para conexão. A velocidade com que as informações são compartilhadas na internet é responsável pelo fluxo imensurável de dados que testemunhamos atualmente. Essas informações estão disponíveis para uma grande parte da população mundial, graças à disseminação generalizada de dispositivos eletrônicos. No Brasil, por exemplo, estima-se que cada habitante possua em média 2,2 dispositivos digitais, de acordo com a 34ª edição da Pesquisa Anual do FGVcia, resultando em aproximadamente 464 milhões de dispositivos em uso, incluindo smartphones, notebooks, desktops e tablets.

Contudo, esse enorme fluxo de informações também traz consigo desafios significativos, como a disseminação de informações falsas. Com a facilidade de publicação na internet, é comum que a veracidade das informações não seja verificada antes de sua divulgação, o que possibilita a proliferação em larga escala de desinformação. No contexto do acesso à internet, a pesquisa anual do Cetic.br revela que, em 2022, cerca de 60 milhões de pessoas possuem acesso à internet no Brasil, e 142 milhões utilizam a internet diariamente. É interessante observar que 99% dos usuários de internet acessam a rede por meio de dispositivos móveis, principalmente smartphones, enquanto 55% utilizam a internet através da televisão e 38% a utilizam por meio de computadores. A disseminação de informações e a acessibilidade proporcionada pela internet trazem benefícios e desafios para a sociedade atual. É crucial que os usuários estejam cientes da necessidade de verificar a veracidade das informações antes de compartilhá-las, a fim de combater a propagação da desinformação. Além disso, medidas de educação e alfabetização digital são fundamentais para capacitar as pessoas a discernir informações confiáveis das falsas, promovendo um uso responsável e crítico da internet.

3.2 INFORMAÇÃO

A informação desempenha um papel fundamental no nosso cotidiano, mesmo que de forma sutil e muitas vezes imperceptível. Desde trocas de dados no ambiente de trabalho até as notícias sobre política que recebemos, a informação está presente em praticamente todas as ações realizadas por indivíduos na sociedade moderna. Ela impulsiona a troca de conhecimento,

o avanço científico, o desenvolvimento tecnológico e a tomada de decisões. Segundo Miranda (1999), informação é definida como "informação são dados organizados de modo significativo, sendo subsídio útil à tomada de decisão". Por sua vez, Le Coadic (1996) descreve a informação como "um significado transmitido a um ser consciente por meio de uma mensagem inscrita em um suporte espacial-temporal: impresso, sinal elétrico, onda sonora, etc.". É importante ressaltar que a informação é frequentemente representada por símbolos, sinais ou linguagens que possuem significado e são capazes de transmitir uma mensagem. Logo, ela pode ser expressa de diversas formas, como texto, imagem, som, vídeo, entre outras.

A essência da informação está na sua capacidade de transmitir significado e gerar conhecimento relevante para o receptor. Além disso, a informação está intimamente relacionada com o processo de organização e armazenamento de dados. Sistemas de gestão da informação e bancos de dados são exemplos de ferramentas que auxiliam na coleta, organização, recuperação e disseminação de informações em contextos científicos, empresariais, educacionais, entre outros.

No entanto, é importante destacar que a informação não se limita apenas a dados brutos. Ela requer contexto, interpretação e compreensão por parte do receptor para se tornar útil e significativa. A transformação de dados em informação envolve análise, avaliação crítica e atribuição de significado aos elementos em questão. A era digital e a proliferação da Internet têm desempenhado um papel significativo na disseminação e no acesso à informação em escala global. Atualmente, a quantidade de informações disponíveis é imensa e cresce exponencialmente. Nesse contexto, a capacidade de filtrar, avaliar a credibilidade e selecionar as informações relevantes torna-se cada vez mais essencial.

3.3 CONCEITO DE INFORMAÇÃO FALSA

Claire Wardle e Hossein Derakhshan através de um consórcio internacional chamado “Trust Project” aponta que o fenômeno da desordem da informação, a distribuição de informações erradas, descontextualizadas, distorcidas ou falsificadas, é conexo com 3 tipos de informações: Informação incorreta, informação falsificada e má informação (CHAVES; BRAGA, 2019). Informação incorreta sendo a informação falsa compartilhada sem a intenção de causar danos, informação falsificada quando é compartilhada a informação falsa, ciente da inverdade, com o intuito de causar danos, e má informação acontece quando a informação é verídica e é compartilhada para causar danos. O objeto de estudo desse trabalho é a informação falsificada ou informação falsa.

A disseminação de informações falsas não é um fenômeno novo, mas a era digital e a rápida disseminação de informações através da internet têm amplificado seu alcance e impacto. As informações falsas podem assumir diversas formas, desde notícias falsas, teorias da conspiração, boatos, rumores e falsos testemunhos até edições ou manipulações de imagens e vídeos. Há várias razões pelas quais a informação falsa pode ser criada e difundida. Alguns indivíduos ou grupos podem fazê-lo intencionalmente para influenciar a opinião pública, promover uma agenda política, obter ganhos financeiros ou simplesmente causar confusão e desordem.

A disseminação de informações falsas pode ter sérias consequências. Ela pode distorcer a realidade, prejudicar a confiança nas instituições e na mídia tradicional, incitar o ódio e a violência, minar a democracia e prejudicar a saúde pública. Um exemplo alarmante é a disseminação de desinformação relacionada à pandemia de COVID-19, que levou a crenças errôneas sobre tratamentos ineficazes, teorias da conspiração sobre a origem do vírus e a hesitação em relação às vacinas, o que contribuiu para um impacto negativo na saúde pública e na resposta global à pandemia.

4 ANÁLISE DOS APLICATIVOS DE MENSAGEM

O surgimento dos meios de troca de mensagens pela internet coincidiu com o advento das redes sociais e a disponibilidade de equipamentos, especialmente os computadores pessoais, juntamente com o acesso à internet. Durante a primeira década dos anos 2000, plataformas como Orkut, MSN, MySpace, entre outras, permitiram a troca de mensagens entre indivíduos, independentemente de sua localização geográfica, em uma escala sem precedentes. Pela primeira vez, era possível se comunicar com pessoas de outros estados ou até mesmo de outras nações, dependendo dos recursos oferecidos pelo serviço de internet e pela plataforma digital utilizada. A chegada dos smartphones ao mercado trouxe mais uma revolução nesse cenário. Com a democratização do acesso a telefones inteligentes, por meio de modelos mais acessíveis à classe trabalhadora, houve um impulso significativo nas vendas desses dispositivos. Acompanhando essa tendência, os aplicativos móveis ofereciam uma gama de facilidades que anteriormente não estavam disponíveis com tanta praticidade. Os aplicativos de mensagens mais populares, como Telegram e WhatsApp, surgiram cerca de uma década após o boom das redes sociais. Esses aplicativos foram criados com uma proposta simples: permitir a troca instantânea de mensagens entre um ou mais indivíduos. Ao longo dos anos, novas funcionalidades foram adicionadas, mas o foco principal desses aplicativos permaneceu o mesmo. Essa funcionalidade simples fez com que os brasileiros substituíssem o antigo sistema de mensagens via SMS que cobrava por mensagem enviada, pelo uso desses aplicativos que não cobram pelo envio de mensagens, apenas exigindo o custo de acesso à internet.

É importante ressaltar que a evolução dos meios de troca de mensagens e a popularização dos smartphones contribuíram para uma maior conectividade e alcance da comunicação instantânea. Esses avanços permitiram uma interação mais rápida e eficiente entre pessoas, rompendo barreiras geográficas e democratizando o acesso à informação em tempo real. Ao compreendermos a importância e o impacto dos aplicativos de mensagens na disseminação de informações, poderemos analisar de forma mais aprofundada como a desinformação é propagada através dessas plataformas, utilizando usas funcionalidades para divulgar conteúdos enganosos em grande escala. Dito isso, a seguir será analisado os aplicativos de mensagem mais utilizados no Brasil de acordo com a pesquisa “Panorama Mobile Time/Opinion Box - Mensageria no Brasil”. A partir dessa análise, será possível explorar estratégias para combater a desinformação e promover o uso responsável das ferramentas de comunicação disponíveis na era digital. Todas as informações foram coletadas das páginas da

Web dos respectivos aplicativos em sessões “FAQ”, e todas outras referências externas aos sites oficiais serão devidamente citadas.

Os critérios analisados serão: informações sobre a criação do aplicativo, suas funcionalidades, sua capacidade de compartilhamento da informação e seu sistema de criptografia. O contexto sob qual cada aplicativo foi fundado é relevante para entender com qual o propósito a existência de cada app se deu, pois, alguns fundadores possuem motivações além de lucro para com seus serviços. As funcionalidades foram selecionadas de acordo com sua relevância para o tema da pesquisa, visto que alguns aplicativos possuem dezenas de funções que não seriam coerentes com o resultado da pesquisa. Os mecanismos de compartilhamento de informação entre usuários serão analisados para que se possa entender como informações falsas possam ser propagadas utilizando-se das funcionalidades disponíveis. E por fim, a criptografia desempenha papel fundamental na coberta de rastros dos agentes difusores de informações falsas, ela serve como ferramenta protetora da privacidade de cada usuário mesmo que esse faça uso nocivo do aplicativo.

4.1 WHATSAPP

O WhatsApp, o maior aplicativo de troca de mensagens do Brasil, está presente em 99% dos aparelhos móveis. Foi fundado por Jan Koum e Brian Acton, que compartilharam duas décadas de experiência conjunta no Yahoo. Em 2014, o WhatsApp uniu-se ao Facebook, mas permaneceu como um aplicativo independente, mantendo seu destaque na oferta de um serviço ágil e confiável de mensagens em escala global, tudo isso de acordo com a sessão “sobre nós” no site oficial do WhatsApp.

Este aplicativo oferece uma ampla gama de funcionalidades, incluindo o envio de mensagens de texto, áudio, vídeos, documentos e localização. Além disso, os usuários podem fazer chamadas de voz e vídeo, e até mesmo realizar pagamentos. Essas características estão disponíveis tanto para uso individual quanto em grupos. Os grupos podem ter até 1.024 membros e podem ser criados em quantidade ilimitada. Uma das adições mais recentes ao aplicativo é a função "comunidade", que permite que um administrador de vários grupos se comunique com até 5 mil membros de diferentes grupos. Essa função foi desenvolvida para facilitar o fluxo de informações entre grupos com temas semelhantes e para melhorar a administração de grupos coordenados pelo mesmo indivíduo, tudo de acordo com a sessão “funcionalidades” e “centro de ajuda” do site oficial do WhatsApp.

Uma das principais vantagens do WhatsApp é que ele oferece esses recursos gratuitamente, diferenciando-se de muitos outros aplicativos de celular que lucram com

anúncios. O WhatsApp, no entanto, gera receita por meio de sua versão paga, o WhatsApp Business Premium. Essa assinatura paga oferece recursos adicionais, como perfil comercial, etiquetas e ferramentas de mensagem, aponta o WhatsApp em seu site oficial na sessão “Para empresas”. Além disso, os assinantes têm acesso a um link personalizável e uma página personalizada para sua empresa. Com essa abordagem, o WhatsApp se tornou uma ferramenta essencial para indivíduos e empresas, permitindo a comunicação rápida, eficiente e segura em todo o mundo. Sua popularidade e sua ampla gama de recursos continuam a torná-lo um dos aplicativos mais utilizados e confiáveis no cenário de troca de mensagens.

4.1.1 COMPARTILHAMENTO DE INFORMAÇÃO

O WhatsApp permite o envio e compartilhamento de diversos tipos de mídia, limitados apenas pelo tamanho e formato do arquivo. Isso torna os usuários suscetíveis a receber informações de natureza variada. Segundo a pesquisa Mensageria no brasil (PANORAMA MOBILE TIME/OPINION BOX, 2023) pelo menos 70% dos usuários utilizam todos os recursos do WhatsApp, o que demonstra um alto engajamento com as ferramentas oferecidas. Além disso, o engajamento com a plataforma é o mais alto do Brasil, com 93% dos usuários utilizando o aplicativo diariamente. Com um grande número de usuários constantemente presentes, o fluxo de informações no WhatsApp é contínuo.

Devido à capacidade dos usuários de encaminhar mensagens para outros contatos, uma mesma informação pode ser multiplicada indefinidamente. Quando uma mensagem é repassada por outra pessoa, é possível direcioná-la para até cinco conversas, sendo permitido incluir apenas um grupo. No entanto, quando uma mensagem é encaminhada para cinco ou mais conversas, ela é marcada com a etiqueta "Encaminhada com frequência", aponta o site oficial do WhatsApp em sua central de ajuda. É importante ressaltar que essas mensagens só podem ser encaminhadas para uma única conversa por vez. Esse mecanismo foi implementado para desencorajar compartilhamentos em massa, mas é válido questionar sua efetividade, uma vez que as mensagens encaminhadas podem ser enviadas indefinidamente para quantos grupos o usuário desejar. Essas características do WhatsApp refletem a importância e a influência do aplicativo como uma fonte significativa de compartilhamento de informações no Brasil, com uma ampla base de usuários e recursos que incentivam a disseminação rápida de mensagens e conteúdo.

4.1.2 CRIPTOGRAFIA

O WhatsApp coloca um grande foco na segurança e privacidade das informações compartilhadas entre os usuários, afirmando que "privacidade e segurança estão em nosso DNA" em seu próprio *site*. Essa preocupação levou a empresa a adotar o modelo de criptografia ponta a ponta para o seu produto. A criptografia ponta a ponta é um conceito em que uma mensagem só pode ser decriptografada pelo destinatário, mesmo que intermediada por um terceiro ou gerenciador. Nesse processo, os intermediários da troca de mensagens não possuem acesso às chaves necessárias para realizar a decodificação das mensagens. A própria WhatsApp Inc. afirma que "O WhatsApp não pode ver o conteúdo de mensagens nem ouvir chamadas feitas no app, porque a criptografia e a descriptografia de mensagens enviadas e recebidas no WhatsApp ocorrem inteiramente no seu aparelho".

A segurança fornecida pela criptografia ponta a ponta é tão forte que até mesmo o supercomputador mais rápido do mundo, o Sunway TaihuLight, levaria uma quantidade inimaginável de tempo para testar todas as possíveis chaves de desbloqueio de uma mensagem enviada pelo aplicativo (TEIXEIRA; SABO; SABO, 2017). De acordo com um artigo publicado na revista da faculdade de direito da UFMG (TEIXEIRA; SABO; SABO, 2017), estimou-se que demoraria cerca de 1,9737 x 10^53 anos para realizar essa tarefa. Isso significa que a interceptação de mensagens criptografadas exigiria tentativas exaustivas para quebrar o sistema de criptografia. Assim, somente os detentores dos aparelhos que enviaram e receberam as mensagens teriam a capacidade de visualizar seu conteúdo. Portanto, a privacidade das mensagens só seria violada se o usuário escolhesse exibir suas mensagens para terceiros diretamente de seu aparelho, pois o sistema de criptografia do WhatsApp garante uma camada adicional de segurança e proteção aos dados dos usuários.

4.2 TELEGRAM

O Telegram é um aplicativo para smartphones e computadores que se concentra no envio e recebimento de mensagens "seguras", além de oferecer recursos de rede social segundo o site da empresa. Foi desenvolvido pelos irmãos russos Pavel e Nikolai Durov e lançado em agosto de 2013 (Maréchal, 2018). Anteriormente, os irmãos Durov eram os proprietários da maior rede social da Rússia, chamada "VK", mas foram obrigados a deixar a administração da empresa pelo Kremlin devido ao uso da plataforma na organização de protestos contra os resultados das eleições legislativas de 2011, que suscitaram suspeitas de fraude em benefício do partido Rússia Unida, liderado por Vladimir Putin (Maréchal, 2018). Atualmente, a sede do Telegram está localizada em Dubai, enquanto os Durov tentam utilizar o aplicativo para

promover uma ideologia chamada Ciberlibertarianismo. O Ciberlibertarianismo é uma ideologia que defende a busca da liberdade individual para perseguir interesses e preferências online, através de soluções voluntárias e acordos baseados em consentimento mútuo, buscando minimizar a coerção estatal na resolução de problemas sociais e econômicos (Thierer; Szoka, 2009). Os Durov buscam promover essa ideologia por meio do Telegram.

Nesse aplicativo, cada usuário pode enviar mensagens, áudios, fotos, vídeos e arquivos de qualquer tipo e, além disso, é possível realizar chamadas de voz e videochamadas. Uma característica distintiva do Telegram é o seu sistema baseado em nuvem, que permite que as mensagens sejam acessadas em qualquer dispositivo conectado pelo usuário, sem a necessidade de conexão por smartphone. Os usuários também podem criar grupos com até 200.000 pessoas ou canais para transmitir mensagens para públicos ilimitados, aproveitando todas as funcionalidades mencionadas. O aplicativo também dá ênfase ao suporte a bots, que são programas de computador que executam ações automatizadas semelhantes às realizadas por humanos, e possui uma API aberta, permitindo a interação controlada entre diferentes programas de software com o Telegram. Todas essas informações estão disponíveis na sessão “faq” do site oficial do Telegram.

O mensageiro tem duas formas de geração de receita: mensagens patrocinadas e assinatura premium. As mensagens patrocinadas oficiais têm um limite de 160 caracteres de texto, excluindo qualquer forma de mídia ou links externos (TELEGRAM). Os usuários só podem visualizar uma mensagem patrocinada por canal após a leitura das novas postagens ser concluída. A assinatura premium oferece benefícios ampliados, incluindo a remoção de limites, permitindo o envio de arquivos de até 4 GB, downloads mais rápidos, acesso a stickers exclusivos, reações personalizadas e recursos avançados de gerenciamento de conversas (TELEGRAM). Segundo informações do site da plataforma, as fontes de receita contribuem para cobrir os custos relacionados à infraestrutura e remuneração dos desenvolvedores. No entanto, é importante ressaltar que a busca por lucro não é o objetivo principal do Telegram (TELEGRAM).

4.2.1 COMPARTILHAMENTO DE INFORMAÇÃO

A plataforma do Telegram permite o encaminhamento ilimitado de mensagens, o que levanta preocupações devido à sua capacidade de agrupar usuários em uma mesma via de envio e recebimento de mensagens (TELEGRAM). Embora os grupos possam ser alarmantes nesse aspecto, é importante prestar atenção especial ao recurso de "canais". Nos grupos, todos os usuários são livres para enviar mensagens de seu interesse, o que pode resultar em um ambiente

caótico quando o limite de 200.000 membros é atingido (TELEGRAM). No entanto, nos canais, apenas os moderadores podem fazer postagens, enquanto outros usuários podem interagir comentando essas postagens, caso seja do desejo dos donos do canal, e não há limite de membros. Segundo uma pesquisa da Panorama (PANORAMA MOBILE TIME/OPINION BOX, 2023), 61% dos usuários do Telegram participam de canais. É importante notar, no entanto, que a taxa de uso frequente do aplicativo é consideravelmente baixa. Apenas cerca de 20% dos usuários utilizam o app diariamente, quase todos os dias ou algumas vezes por semana (PANORAMA MOBILE TIME/OPINION BOX, 2023). Apesar dessas estatísticas, existem canais com milhões de membros, como o canal do ex-presidente Jair Messias Bolsonaro, que possui 2,4 milhões de membros e é estimado como o maior canal do Brasil. O aplicativo desempenha um papel significativo como ferramenta política e foi utilizado durante períodos eleitorais para o envio de informações sobre candidatos, visando favorecer suas campanhas.

4.2.2 CRIPTOGRAFIA

O Telegram utiliza um esquema de criptografia personalizado chamado MTProto, desenvolvido por Nikolai Durov, um dos irmãos fundadores do aplicativo (TELEGRAM). Ele oferece dois tipos de criptografia: para chats privados individuais ou em grupo, os dados são criptografados de forma cliente-servidor. Isso significa que todas as mensagens são armazenadas nos data centers da empresa. Já o outro método é a criptografia cliente-cliente, que é aplicada exclusivamente por meio da funcionalidade "chat secreto". Nesse caso, as mensagens são armazenadas apenas nos dispositivos móveis dos usuários envolvidos no chat secreto, como a criptografia do WhatsApp (TELEGRAM).

Nos chats secretos, as mensagens não podem ser encaminhadas e, quando o usuário exclui as mensagens de sua própria conversa, o aplicativo do outro usuário também é solicitado a excluí-las. Além disso, é possível configurar as mensagens, fotos, vídeos e arquivos para autodestruição, ou seja, eles são automaticamente excluídos após um determinado período de tempo após terem sido lidos ou visualizados pelo destinatário. Isso garante que as mensagens desapareçam tanto no dispositivo do remetente quanto no dispositivo do destinatário. Essas medidas de segurança e privacidade do Telegram visam proteger a confidencialidade das conversas dos usuários e fornecer opções adicionais para controle sobre o conteúdo compartilhado (TELEGRAM).

4.3 FACEBOOK MESSENGER

Ao longo de sua evolução como plataforma de negócios para dispositivos móveis, o Messenger do Facebook se destacou como a primeira instância da plataforma a ser lançada como um aplicativo separado. Embora a troca de mensagens entre usuários já estivesse presente há anos na versão web do Facebook, o Messenger surgiu como uma extensão do Facebook, oferecendo recursos avançados de mensagens em um aplicativo dedicado. Inicialmente chamado de "Facebook Chat" em 2008 (TECHCRUNCH, 2008) e posteriormente renomeado para "Facebook Messages" em 2010, a empresa decidiu separar sua ferramenta de troca de mensagens do aplicativo principal do Facebook (M.G SIEGLER, 2010). Assim, em 2011, o "Facebook Messenger" foi lançado como um aplicativo móvel independente (Nieborg; Helmond, 2019).

O Messenger permite que os usuários enviem mensagens, compartilhem fotos, vídeos, áudio e arquivos entre si. Além disso, oferece suporte para chamadas de voz e vídeo, bem como interações com bots. Para atender ao público mais infantil, o Messenger Kids foi desenvolvido para permitir que as crianças se conectem com segurança a amigos e familiares. Ele oferece recursos como mensagens, videochamadas, jogos e figurinhas. Os pais têm acesso ao Painel para Pais, presente nas contas do Facebook, que lhes permite gerenciar a lista de contatos de seus filhos, monitorar suas atividades e ajustar as configurações da conta, garantindo um ambiente controlado e adequado para as crianças. Todas as informações recém mencionadas foram extraídas do site oficial do Facebook Messenger em sua sessão “central de ajuda”.

Em 2017, o Facebook começou a testar a exibição de anúncios no feed inicial do Messenger como parte de seus esforços para gerar receita com o aplicativo. Inicialmente limitados a usuários na Austrália e Tailândia, esses testes apresentavam anúncios em formato de carrossel. Posteriormente, os testes foram expandidos globalmente, com base em dados e feedback dos usuários, para determinar a melhor forma de exibir anúncios de maneira consistente para a maioria dos usuários (TechCrunch, 2017; JOHNSON, 2017). Dessa forma, o Messenger do Facebook se estabeleceu como uma plataforma versátil para troca de mensagens, interações com bots e até mesmo exibição de anúncios, permitindo que os usuários se conectem e comuniquem de várias maneiras convenientes.

4.3.1 COMPARTILHAMENTO DE INFORMAÇÃO

O Messenger, respaldado pela gigante da tecnologia Facebook, possui vantagens distintas em relação a outros aplicativos de mensagens devido à sua integração com o ecossistema da empresa. O aplicativo de conversas tem a capacidade de sincronizar com

funções como o marketplace e a comunidade, além da sincronia com o Instagram, o que facilita o compartilhamento ágil de informações entre os usuários que utilizam essas funcionalidades. Em relação ao encaminhamento de mensagens, o site oficial do Messenger em sua sessão “central de ajuda”, afirma que é possível enviar mensagens para até 150 pessoas de uma vez. No entanto, o UOL (CARVALHO, 2020) relata que em 2020 o Facebook optou por limitar o encaminhamento para apenas cinco pessoas ou grupos, com a possibilidade de até 250 membros por grupo (YAP, 2022), por vez, e em teste empírico foi confirmado que apenas 5 encaminhamentos por vez foram permitidos. A limitação no encaminhamento de mensagens visa promover um ambiente de comunicação mais controlado e reduzir a disseminação de informações em larga escala. Essas características permitem que os usuários do Messenger aproveitem a conexão com outras funcionalidades do Facebook, para compartilhar informações de forma conveniente e eficiente.

4.3.2 CRIPTOGRAFIA

Assim como os aplicativos mencionados anteriormente, o Facebook Messenger utiliza criptografia ponta a ponta para proteger as mensagens trocadas entre os usuários. Isso significa que as mensagens são protegidas por chaves criptográficas e só podem ser desbloqueadas pelo destinatário da mensagem. Além disso, as mensagens ficam armazenadas apenas nos dispositivos eletrônicos dos usuários, garantindo uma camada adicional de segurança e privacidade, de acordo com o site oficial do Facebook Messenger. No entanto, é importante observar que o Facebook Messenger possui diferenças em relação à sua versão para desktop. A Meta Platforms, Inc., empresa responsável pelo Facebook, destaca em seu site que os dados das conversas no Messenger estão vinculados aos cookies do navegador em uso. Isso significa que se houver uma troca de navegadores ou se o usuário estiver utilizando modos de navegação nos quais os cookies não são salvos, como o modo privado, existe a possibilidade de que as mensagens fiquem inacessíveis ou não sejam sincronizadas corretamente entre os dispositivos. Portanto, é recomendado que os usuários do Facebook Messenger estejam cientes das particularidades relacionadas ao armazenamento e sincronização das mensagens, levando em consideração as configurações do navegador e os modos de navegação utilizados para garantir a disponibilidade e a privacidade das suas conversas.

4.4 INSTAGRAM DIRECT

Segundo uma pesquisa realizada em 2023 pela Panorama (PANORAMA MOBILE TIME/OPINION BOX, 2023), o recurso Instagram Direct, presente na popular rede social

Instagram, alcançou uma taxa impressionante de instalação de 87% em smartphones, posicionando-se como um concorrente forte no mercado de aplicativos de mensagens. Pertencente à empresa norte-americana Meta Platforms, a mesma por trás do Facebook, o Instagram Direct oferece uma ampla gama de recursos, incluindo o envio de mensagens de texto, fotos, vídeos, áudio e a possibilidade de realizar chamadas de áudio e vídeo. Tudo isso de acordo com a sessão "central de ajuda" do seu site oficial.

Lançado em dezembro de 2013, o recurso Instagram Direct trouxe consigo a funcionalidade de interação por meio de mensagens privadas, permitindo que os usuários enviassem mensagens para aqueles que seguem, quebrando a restrição anterior de apenas compartilhamento público (HAMBURGER, 2013). Quando um usuário recebe uma mensagem privada de alguém que não segue, a mensagem é marcada como pendente, exigindo a aceitação do usuário para visualizá-la. Em setembro de 2015, os usuários passaram a ter a capacidade de compartilhar localizações, páginas de hashtags e perfis diretamente por meio de mensagens privadas, facilitando ainda mais a interação com outros usuários a partir do feed de notícias (SETALVAD, 2015).

No entanto, em 2020, o Facebook deu início ao processo de integração entre o Instagram Direct e o Facebook Messenger, unificando as funcionalidades de mensagens entre as duas plataformas (AMADEO, 2020). Essa atualização gradual substituiu o ícone do Instagram Direct pelo ícone do Facebook Messenger, proporcionando uma experiência mais coesa e integrada para os usuários em ambas as plataformas. Essas melhorias constantes no Instagram Direct refletem a busca contínua por oferecer uma experiência completa e atraente de mensagens aos usuários. Com um número crescente de instalações e recursos aprimorados, o Instagram Direct continua a se destacar como uma escolha popular para comunicação privada e interação social na era digital.

4.4.1 COMPARTILHAMENTO DE INFORMAÇÃO

O recurso Instagram Direct segue a mesma abordagem do aplicativo principal de sua empresa controladora. Ao utilizar o Instagram Direct, os usuários têm a capacidade de encaminhar uma mensagem para até cinco grupos ou usuários diferentes por vez. Além disso, existem restrições quanto ao tamanho dos grupos, limitando-os a um máximo de 250 membros. Uma das principais vantagens desse recurso é sua integração com a plataforma Instagram, permitindo que os usuários compartilhem vídeos e imagens de forma rápida e conveniente. Com apenas alguns toques na tela, é possível enviar conteúdos consumidos para outros usuários. Além disso, a integração com o Facebook Messenger facilita a troca de informações entre as

plataformas, permitindo o envio instantâneo de dados de grupos de uma plataforma para outra. Tudo isso de acordo com os dados providos pela “central de ajuda” do site oficial do Instagram

Essas limitações e integrações estratégicas visam proporcionar uma experiência de compartilhamento de conteúdo eficiente e controlada no Instagram Direct. Os usuários podem enviar mensagens para um número limitado de grupos ou usuários, enquanto desfrutam da perfeita integração com a plataforma Instagram e o Facebook Messenger, possibilitando a transferência ágil e conveniente de informações entre as plataformas. Essa abordagem visa equilibrar a praticidade do compartilhamento de conteúdo com a necessidade de controlar a disseminação excessiva de mensagens e manter uma experiência de uso agradável para os usuários do Instagram Direct. Essas restrições visam evitar possíveis abusos e garantir que a plataforma seja utilizada de forma responsável e eficaz, proporcionando um ambiente seguro e controlado para os usuários interagirem e compartilharem conteúdo.

4.4.2 CRIPTOGRAFIA

Recentemente, o Instagram implementou uma atualização significativa no que diz respeito à segurança e privacidade das mensagens, introduzindo a criptografia ponta-a-ponta como parte de suas funcionalidades (SHAUL, 2023). No entanto, é importante ressaltar que essa criptografia ponta-a-ponta necessita ser ativada manualmente pelos usuários antes de iniciar uma conversa com outro usuário ou em grupos. Essa medida permite que os usuários tenham o controle sobre a segurança de suas comunicações, podendo optar por habilitar a criptografia para garantir a confidencialidade de suas mensagens. Ao ativar a criptografia ponta-a-ponta, as mensagens são protegidas por chaves criptográficas, garantindo que apenas os remetentes e destinatários das mensagens possam ter acesso ao seu conteúdo, e as mensagens são armazenadas apenas nos dispositivos dos usuários, não sendo acessíveis pelos servidores do Instagram, segundo o site oficial do aplicativo.

No entanto, é importante destacar que, caso a função de criptografia ponta-a-ponta não seja ativada, as mensagens enviadas serão armazenadas nos servidores do Instagram, pertencentes à Meta. Nesse caso, as mensagens estarão sujeitas à relação tradicional de servidor-cliente, onde a plataforma mantém controle e acesso aos dados enviados. Portanto, é fundamental que os usuários estejam cientes da importância de ativar a criptografia ponta-a-ponta para garantir a máxima segurança e privacidade em suas comunicações no Instagram. Essa medida proporciona uma camada adicional de proteção contra acessos indesejados ou violações de privacidade, assegurando que apenas os participantes da conversa tenham acesso

ao conteúdo das mensagens trocadas. Ao habilitar a criptografia ponta-a-ponta, os usuários podem ter a tranquilidade de que suas comunicações estão protegidas de olhares indesejados.

4.5 SIGNAL

O Signal é um aplicativo que surgiu como sucessor do RedPhone e do TextSecure, desenvolvidos pela startup Whisper Systems em 2010 (WHISPER SYSTEMS, 2010). O RedPhone era focado em chamadas de voz criptografadas, enquanto o TextSecure se dedicava a mensagens de texto criptografadas. Após a aquisição da Whisper Systems pelo Twitter em 2011, o RedPhone foi descontinuado (GREENBERG, 2011), mas o TextSecure foi disponibilizado como software de código aberto. Moxie Marlinspike, um dos fundadores da Whisper Systems, deixou o Twitter e fundou o Open Whisper Systems. Em 2014, o Open Whisper Systems lançou uma nova versão do protocolo do TextSecure, que posteriormente seria chamado de Signal Protocol, essa atualização trouxe novas funcionalidades, como bate-papo em grupo criptografado e mensagens instantâneas, ao TextSecure (DONOHUE, 2014). Combinando o TextSecure e o RedPhone, foi lançado o aplicativo Signal, que se tornou o primeiro aplicativo para iOS a oferecer chamadas de voz com criptografia de ponta a ponta gratuitamente. Em seguida, foram lançadas versões para Android e desktop. Em 2018, Moxie Marlinspike e Brian Acton anunciaram a criação da Signal Technology Foundation, uma organização sem fins lucrativos estabelecida para financiar o desenvolvimento contínuo do Signal (GREENBERG, 2018). Brian Acton, cofundador do WhatsApp, fez um aporte financeiro inicial de 50 milhões de dólares para a fundação. O Signal depende de financiamentos e doações para continuar seu desenvolvimento como uma organização independente sem fins lucrativos, de acordo com dados extraídos de seu site oficial.

O aplicativo móvel Signal oferece aos usuários serviços de envio de mensagens de texto, arquivos, notas de voz, imagens e mensagens de vídeo. Além disso, permite chamadas de voz e vídeo individuais e em grupo com até 40 pessoas. Embora o Signal tenha uma popularidade menor em comparação com outros aplicativos no Brasil, com 13% de adesão entre os entrevistados pela pesquisa da Panorama (PANORAMA MOBILE TIME/OPINION BOX, 2023), é importante observar que apresenta a maior taxa de nunca utilizado, com 17% dos usuários sem interesse no uso do aplicativo.

Nos Estados Unidos, o aumento de adesões ao Signal foi associado a diversos fatores. A CNN ((DUFFY, 2021) destacou a mudança na política de privacidade do WhatsApp como um dos motivos, levando os usuários a procurarem alternativas mais focadas na privacidade. Além disso, o endosso do Signal por figuras proeminentes como Elon Musk e Edward

Snowden, feito por meio do Twitter, também contribuiu para o aumento da popularidade do aplicativo. Outro evento significativo foi o ataque da extrema direita ao Capitólio dos Estados Unidos, que gerou uma preocupação maior com a segurança das comunicações online. A Reuters relatou que mais de 100.000 pessoas instalaram o Signal entre os dias 7 e 8 de janeiro, provavelmente impulsionadas por esses acontecimentos.

No Brasil, a motivação para aderir ao Signal foi um pouco diferente. De acordo com o UOL (DAROS, 2022), após o pedido do atual presidente do STF, Alexandre de Moraes, para o Telegram derrubar cinco grupos que defendiam atos anti-democráticos, os quais agregavam cerca de 560 mil membros, os apoiadores do ex-presidente passaram a considerar o Signal como uma segunda opção para troca de mensagens. Esse episódio específico despertou a atenção dos usuários para a importância da segurança e privacidade nas plataformas de comunicação. Esses eventos destacam a sensibilidade do público em relação à privacidade e à segurança de suas comunicações, impulsionando o aumento no uso do Signal como uma alternativa confiável para troca de mensagens criptografadas.

4.5.1 COMPARTILHAMENTO DE INFORMAÇÃO

O aplicativo Signal é conhecido por suas funcionalidades simples e eficientes, especialmente quando se trata do compartilhamento de informações. Ele adota uma abordagem simplificada para auxiliar os usuários na transferência de mensagens entre si. Os usuários do Signal podem encaminhar uma mesma mensagem para até cinco contatos distintos simultaneamente, seja em conversas individuais ou em grupos. Essa funcionalidade facilita a disseminação rápida de informações importantes. Além disso, o Signal permite a criação de grupos com um grande número de participantes, até mil membros. Isso oferece aos usuários a liberdade de criar grupos para diferentes finalidades, como discussões em equipe, grupos de interesse ou comunidades de compartilhamento de informações. A capacidade de criar e participar de grupos amplos contribui para uma maior interação e colaboração entre os usuários. No geral, o Signal se destaca por oferecer uma experiência de compartilhamento de informações simples, mas poderosa. Suas funcionalidades permitem que os usuários troquem mensagens de forma eficiente, encaminhem conteúdo relevante para múltiplos contatos e criem grupos de diversos tamanhos para interações sociais ou profissionais. Todos esses dados foram coletados da sessão “Suporte do Signal” em seu site oficial.

4.5.2 CRIPTOGRAFIA

A segurança do Signal é garantida por meio de uma criptografia ponta a ponta, que assegura que as mensagens e chamadas só possam ser lidas pelo destinatário e pelo remetente em seus dispositivos eletrônicos. Esse alto nível de segurança é possível graças ao "Signal Protocol", um protocolo de criptografia desenvolvido por Trevor Perrin e Moxie Marlinspike. O Signal Protocol é amplamente reconhecido por sua eficácia na proteção da privacidade das comunicações. Ele oferece aos usuários a capacidade de verificar a integridade da privacidade de suas interações com um contato específico. Isso pode ser feito por meio da comparação de números de segurança ou pelo escaneamento de um código QR exclusivo. Ao verificar os números de segurança ou o código QR, os usuários podem ter a certeza de que suas comunicações estão sendo protegidas e não estão sendo interceptadas ou acessadas por terceiros não autorizados. Essa verificação adiciona uma camada adicional de confiança e segurança aos usuários do Signal. Em resumo, o Signal se destaca por sua segurança robusta, proporcionada pela criptografia ponta a ponta e pelo Signal Protocol. Essas medidas garantem que as comunicações sejam mantidas privadas e protegidas contra acessos indesejados, de acordo com informações de seu site oficial.

5 RESULTADOS E DISCUSSÃO

Com tantas funcionalidades dispostas para todo usuário fazer uso, dentre elas grandes ferramentas para o compartilhamento de informação, é natural que se levante preocupações perante as informações falsas sendo compartilhadas. Em um artigo da revista Ciência & Saúde Coletiva informa-se que 73,7% das notícias falsas sobre a Covid-19 circularam via WhatsApp, entre 17 de março a 10 de abril de 2020. Esses dados foram colhidos durante o primeiro mês que o povo brasileiro teve contato com o vírus, logo 65% das informações foram centradas em como prevenir o contágio e 20% foram sobre como curar a Covid-19 (Galhardi, Freire, N.P, Minayo, M.C.S, Fagundes, M.C.M, 2020). Todo esse fluxo de informações enganosas estava presente em massa em dispositivos eletrônicos de brasileiros, esses que procuravam por alguma solução e acabam por encontrar mentiras que os guiam para caminhos distantes de qualquer solução factível.

Levando em consideração as limitações para membros de grupo de todos os aplicativos, cada aplicativo é capaz de alcançar pelo menos 250 pessoas e são capazes de encaminhar a mesma mensagem para outros grupos 5 grupos simultaneamente. Logo, pode se inferir que uma informação falsa pode atingir até 1250 indivíduos instantaneamente em qualquer aplicativo citado anteriormente, considerando apenas os valores mínimos que cada app consegue alcançar. Se considerarmos a capacidade máxima de membros em grupos de todos os aplicativos somados, os grupos podem aportar um total de 202.524 mil membros, sendo 200 mil membros apenas do Telegram, e com o encaminhamento limitado a 5 grupos diferentes uma mesma informação pode ser compartilhada com até 1.012.620 no mesmo instante. Essa conta foi feita excluindo os canais do aplicativo Telegram, que permitem um número infinito de participantes, e como fora citado antes, existem canais com mais de 2 milhões de usuários. E esses grupos tendem a funcionar como câmaras de eco, reforçando crenças e evitando a exposição a opiniões contrárias ou informações factíveis.

As informações falsas podem ser de teor apelativo que explorem medos e preconceitos, ou através da criação de narrativas convincentes que levem as pessoas a acreditar em informações falsas. Quando ocorrem eventos importantes, como eleições, desastres naturais ou crises, usuários veem como oportunidade para espalhar informações falsas relacionadas a esses eventos. Tudo sustentado por táticas persuasivas e linguagem emocional para enganar os usuários, isso inclui o uso de manchetes sensacionalistas, linguagem apelativa e apelos emocionais que visam provocar reações intensas e impulsionar o compartilhamento da informação falsa. E, além disso, a tendência natural das pessoas em confiar em informações compartilhadas por amigos, familiares e contatos próximos é explorada para disseminar

desinformação. As mensagens falsas são frequentemente enviadas por pessoas que conhecemos e em quem confiamos, o que torna mais provável que acreditemos e compartilhemos o conteúdo sem verificar sua veracidade.

Impulsionados pelo uso de *bots* que podem enviar mensagens em massa, compartilhar *links* ou produzir respostas automatizadas que promovem narrativas falsas. Eles são projetados para amplificar a desinformação e criar a ilusão de que várias pessoas estão compartilhando a mesma informação. A Pesquisa "Bad Bot Report" da Imperva de 2023 estimou que 47.4% do tráfico online foi efetuado por automatizações, demonstrando como os bots estão presentes em quase metade de todo conteúdo presente na internet e com o avanço galopante da inteligência artificial, será cada vez mais comum ver notícias fabricadas e publicadas de forma automática, sem nenhum toque humano. Todo esse fluxo informacional ocasiona a dificuldade na verificação de informações dado a natureza instantânea e privada dos aplicativos de mensagem. Ao contrário das redes sociais, onde as informações podem ser verificadas e contestadas publicamente, nas mensagens privadas a disseminação da desinformação ocorre de forma mais obscura e é difícil rastrear sua origem.

É valido relembrar que cada mensagem com informações questionáveis é protegida por uma criptografia que, além de codificar a mensagem, codifica o destinatário e o remetente da mensagem. Fazendo com que a busca por algum indivíduo que propague informações falsas seja dificultada, a ponto de ser praticamente impossível encontrar qualquer vestígio dele online. A rede de segurança que cada aplicativo de mensagem é capaz de fornecer gratuitamente, pode ser vista como uma resposta a privacidade e liberdade de expressão que alguns donos dos aplicativos estudados fundaram seus serviços. Por mais que a proposta de estar completamente seguro de qualquer pessoa indesejada bisbilhotar suas conversas privadas seja interessante, quando a blindagem contra invasores protege até criminosos, vale a pena questionar se a liberdade de expressão irrestrita se faz importante na luta contra a desinformação.

5.1 LIBERDADE DE EXPRESSÃO

Ao compreender a origem por trás da fundação dos aplicativos mais utilizados no Brasil, pode se notar que existem similaridades. Por um lado, existem mensageiros que são ferramentas que agregam valor ao seu produto final, esses tentam atribuir múltiplas funções sociais para cada plataforma para fins comerciais, os aplicativos pertencentes a Meta Platforms segue esse padrão, como o Whatsapp, Facebook Messenger e o Instagram Direct. Por outro lado, as plataformas Telegram e Signal foram fundadas por diferentes milionários, a fim de cumprir com seus desejos pessoais de obter uma rede de troca de mensagens com liberdade irrestrita de

expressão, e tudo sem fins lucrativos sendo sustentados apenas por doações ou serviços pagos que são utilizados para manutenção do aplicativo. Buscar um produto caro que não obtém lucro em troca de seus serviços é algo que contrapõe o atual sistema econômico que a sociedade contemporânea é submetida, por mais que seus financiadores tenham conseguido arrecadar fundos para sustentar seus projetos seguindo as regras desse sistema.

A liberdade de expressão sem limites é algo tangível dentro de um sistema de troca de mensagens indetectável por terceiros, não é à toa que todos os aplicativos anteriormente citados adotaram a opção de criptografia ponta a ponta. Os próprios desenvolvedores dos aplicativos já utilizaram em propagandas o fato de nem eles próprios têm acesso as suas mensagens. A Constituição Federal de 1988, artigo 5º, parágrafo IV: "É livre a manifestação do pensamento, sendo vedado o anonimato", todavia isso não impede que certas atitudes sejam tomadas. "O limite do direito de liberdade de expressão se dá quando, sob essa pretensa liberdade, atinge-se a honra, a dignidade ou mesmo a democracia", aponta defensor público em matéria da Defensoria pública do estado do Paraná; ele complementa em seguida: "Inclusive existem crimes, previstos no Código Penal, que definem a limitação da chamada liberdade de expressão, como os crimes de injúria, difamação e calúnia". Todas essas violações da lei podem ser cometidas livremente por canais de comunicação em aplicativos de mensagem, desde que não seja apreendido o dispositivo eletrônico usado para envio ou recebimento dessas mensagens.

Isso nos traz ao recente bloqueio do aplicativo Telegram em abril de 2023, onde o aplicativo se recusou a cooperar com a Polícia Federal (PF) e acabou sendo suspenso em território nacional através das provedoras de internet e lojas de aplicativos. Não é a primeira vez que um aplicativo de mensagem foi bloqueado, o WhatsApp e o próprio Telegram já haviam sido suspensos por não cooperarem com investigações da PF. Dessa vez o que motivou a decisão foi o requerimento de informação sobre usuários que estariam incentivando ataques em escolas (G1, 2023), devido ao ataque a uma escola de Aracruz que deixou 4 mortos em novembro de 2022. O aplicativo chegou a ceder informações sobre os envolvidos, mas suspeita-se que entre eles houveram grupos neonazista envolvidos, os quais foram negados a distribuição de dados.

Em outro caso, o Telegram disparou, em maio de 2023, mensagens para seus usuários brasileiros em massa contra a recente PL 2.630/2020, também reconhecida como PL das fake News (UOL, 2023). Essa PL que "Estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções

para o descumprimento da lei", de acordo com a ementa do projeto de lei. Na mensagem que circulava celulares com o aplicativo Telegram baixado, foi dito que a lei vai "acabar com a liberdade de expressão" e "matará a internet moderna" (UOL, 2023).

A dualidade apresentada pela plataforma em suas medidas para apoiar um movimento contrário a um projeto de lei que regula as informações compartilhadas, e a falta de apoio contra grupos neonazista possivelmente envolvidos em um atentado que resultou a morte de 4 pessoas é preocupante. A defesa da liberdade de expressão irrestrita pode viabilizar maiores tragédias caso não sejam monitoradas e cerceadas, a liberdade de poder promover os crimes de injúria, difamação, calúnia, etc. não devem ser defendidos sobre o pretexto de livre pensamento, visto que são atitudes danosas a outros indivíduos.

5.2 ESTUDO DE CASO SOBRE VÍTIMAS DE INFORMAÇÕES FALSAS

A fim de exemplificar o impacto negativo que uma informação falsa pode ter na percepção das pessoas, analisaremos o caso do falso assassino do ex-primeiro ministro japonês Shinzo Abe. Em julho de 2022, circularam informações falsas nas redes sociais de que Abe havia sido assassinado por Tetsuya Yamagami, um ex-oficial da Força Marítima de Autodefesa do Japão (PRESSE, 2022). Segundo os boatos, Yamagami teria utilizado uma arma de fogo caseira durante um discurso público, motivado por ressentimento em relação à Igreja da Unificação, organização na qual a mãe de Yamagami havia feito doações substanciais antes de enfrentar problemas financeiros (JOHNSON; OTAKE, 2022).

Essas informações falsas ganharam ampla circulação devido à combinação de fatores, como a escassez de casos de violência no país e a importância política de Abe para a nação japonesa. No entanto, durante esse período, uma imagem irônica começou a circular nas redes sociais, mostrando o renomado desenvolvedor de jogos eletrônicos Hideo Kojima em situações que aparentavam associá-lo a símbolos comunistas, como a imagem de Che Guevara (O Globo, 2022). Embora as fotos fossem reais, Kojima não possuía nenhuma conexão com o caso de assassinato, e a ironia foi construída pela falta de relação direta entre ele e os eventos mencionados. Hideo Kojima é reconhecido mundialmente por suas contribuições para a indústria de jogos eletrônicos, e sua popularidade nas redes sociais, com mais de 5 milhões de seguidores, é um reflexo desse reconhecimento. No entanto, devido à seleção específica de fotos em que ele aparecia ao lado de imagens e símbolos com conotação esquerdista, algumas pessoas interpretaram erroneamente essas associações como evidências políticas.

Oportunisticamente, oponentes de suas ideologias aproveitaram essa situação para associar o assassinato de Abe às opiniões políticas de Kojima, sem qualquer contexto

humorístico. Essa situação ilustra como uma piada inicialmente compreensível para aqueles familiarizados com a indústria de jogos eletrônicos pode se transformar em uma desinformação disseminada em larga escala. O caso chegou a ser divulgado em um dos canais mais assistidos da Grécia, conforme relatado pelo jornal Globo, com afirmações de que Yamagami estava insatisfeito com Abe e tinha simpatia por Che Guevara. Além disso, o político e militante francês de extrema-direita, Damien Rieu, comentou em seu perfil do Twitter: "a extrema-esquerda mata" (O. GLOBO, 2022). Essa análise destaca a importância de examinar como as notícias falsas podem se espalhar por meio dos aplicativos de mensagem, explorando as nuances dos contextos políticos e sociais que contribuem para a propagação dessas informações enganosas. A compreensão desse fenômeno é fundamental para desenvolver estratégias eficazes de combate à desinformação, promovendo uma sociedade informada e consciente dos riscos associados à propagação de notícias falsas.

O caso mencionado acima ilustra claramente como até mesmo uma piada pode ser distorcida e transformada em uma notícia falsa, com repercussões sérias. É preocupante observar como essa desinformação pode se espalhar rapidamente, alcançando veículos de comunicação e até mesmo sendo repetida por pessoas influentes, com o objetivo de persuadir outras pessoas de seus próprios vieses ideológicos. Embora enganos possam ocorrer em meio ao enorme fluxo de informações, é essencial exercer cautela ao compartilhar qualquer tipo de informação. Uma única notícia falsa divulgada em larga escala pode causar danos irreversíveis. O caso de Hideo Kojima exemplifica que, mesmo com uma repercussão global e a rápida intervenção de seus seguidores para desmentir as informações falsas, os desdobramentos poderiam ter sido diferentes.

No entanto, devemos nos lembrar do trágico caso de Fabiane Maria de Jesus, no Brasil. Ela foi espancada até a morte após uma postagem em uma página do Facebook que divulgou um retrato falado de uma suposta sequestradora de crianças para rituais de magia negra. Esse retrato falado guardava semelhança com Fabiane, o que resultou em sua morte apenas dois dias após o espancamento (ROSSI, 2014). Enquanto o caso de Hideo Kojima foi rapidamente desmentido pelos seus milhares de seguidores ao redor do mundo, Fabiane teve pouco tempo para se defender das acusações e agressões. Esse exemplo chocante revela a gravidade das consequências que uma informação falsa disseminada indiscriminadamente pode acarretar. No caso de Fabiane, ela mal teve a oportunidade de explicar a confusão aos agressores. De acordo com o advogado da vítima, "Fabiane não teve tempo de se defender das acusações e agressões" (ROSSI, 2014). Esses episódios nos levantam questões importantes sobre o papel do jornalista na divulgação de informações corretas, independentemente da situação. No caso de Fabiane, a

informação falsa foi disseminada por uma página de Facebook e prontamente aceita como verdade, sem questionamentos. É possível inferir que o sentimento de revolta levou os cidadãos a agirem daquela forma, mas em nenhum momento as autoridades foram acionadas para iniciar investigações sobre o caso.

Isso demonstra uma confiança significativa em um boato lançado online, sem qualquer embasamento, destacando a periculosidade da propagação de informações falsas. É essencial compreender os perigos e as consequências devastadoras que as notícias falsas podem ter na sociedade. A disseminação irresponsável dessas informações pode levar a atos de violência, injustiças e prejuízos irreparáveis às pessoas envolvidas. Os jornalistas desempenham um papel crucial na verificação dos fatos e na promoção da informação precisa, ajudando a combater a desinformação e a preservar a integridade da sociedade como um todo.

5.3 QUEDA DA CREDIBILIDADE DO JORNALISMO

É inegável que a credibilidade dos veículos jornalísticos tem sido afetada nos últimos anos, o que tem contribuído para o aumento da propagação de informações falsas. A evolução da sociedade contemporânea trouxe consigo transformações estruturais que impactaram significativamente a produção de conteúdo informativo, e essas mudanças têm reflexos nos princípios fundamentais da formação profissional dos jornalistas. Segundo o Centro de Pesquisa Reuters Institute, em seu relatório "Digital News Report" de 2022, o índice geral de confiabilidade na mídia jornalística apresentou uma queda de 6% durante o ano eleitoral, apesar de ter experimentado um crescimento nos dois anos anteriores. Além disso, a dificuldade em distinguir informações verdadeiras de falsas também possui uma dimensão partidária.

Conforme apontado por Levinson (2016), as notícias falsas têm um impacto significativo em virtude de um fenômeno que se desenvolveu com o advento das tecnologias de informação e comunicação: a tendência das pessoas em buscar na internet visões que confirmem suas próprias crenças e convicções. Essa característica humana já existia antes da internet e pode ser relacionada à teoria da dissonância cognitiva de Leon Festinger (FESTINGER, 1962). Além disso, o conceito de "Narciso como narcose", introduzido por McLuhan (MCLUHAN, 1969), destaca nossa apreciação pelos reflexos midiáticos de nossas próprias ideias e emoções. Diante desse cenário, é fundamental compreender os desafios enfrentados pelos veículos jornalísticos na atualidade. A falta de confiança do público nos meios de comunicação tradicionais tem levado as pessoas a procurarem outras fontes de informação, muitas vezes menos confiáveis e sujeitas à propagação de desinformação. Esse contexto exige uma reflexão profunda sobre os processos de produção, verificação e

disseminação de notícias, bem como sobre a necessidade de um jornalismo de qualidade e ético para combater a disseminação de informações falsas.

É essencial que os veículos jornalísticos adotem medidas para fortalecer a confiança do público, como a transparência na divulgação de fontes e métodos de apuração, a busca pela imparcialidade e a verificação rigorosa dos fatos. Além disso, é importante promover a educação midiática e a alfabetização digital, capacitando as pessoas a discernir entre informações verdadeiras e falsas. A luta contra as informações falsas requer esforços conjuntos da sociedade, dos meios de comunicação e das plataformas digitais. Somente com um compromisso coletivo em promover a precisão e a veracidade das informações, aliado a uma postura crítica e responsável por parte dos consumidores de notícias, poderemos enfrentar os desafios trazidos pela disseminação das fake news e preservar a integridade do espaço informacional.

5.4 COMO COMBATER DESINFORMAÇÃO

Diante desse cenário, é necessário compreender e enfrentar os desafios trazidos pela disseminação de informações falsas na era digital. A internet proporciona um ambiente propício para a proliferação de desinformação, exigindo uma abordagem cuidadosa para promover a veracidade, a confiabilidade e o pensamento crítico no consumo de informações online. E os aplicativos de mensagem servem como catalisadores da desinformação, multiplicando exponencialmente a velocidade que uma informação falsa circula pela Internet de forma gratuita e prática, o que torna a situação cada vez mais alarmante. É essencial buscar soluções que permitam filtrar, avaliar e verificar a credibilidade das informações, de modo a preservar a integridade do conhecimento e o bem-estar da sociedade como um todo.

Claire Wardle e Hossein Derakhshan oferecem recomendações para se lidar com desinformações em níveis diferentes da sociedade, foram selecionado as indicações mais relevantes para o objeto de estudo do trabalho. A começar pelas empresas de tecnologia, que deveria “Destacar detalhes contextuais e criar indicadores visuais para conteúdo”. Muita informação pode ser desviada da verdade através da omissão de algum contexto que foi aplicado na situação em destaque, logo criar mecanismos que facilitam o entendimento do momento e situação do qual a informação está inserida se faz necessária. Além disso, “Criar ferramentas de checagem de notícias e de verificação” e “Construir mecanismos de autenticidade"; cada aplicativo visa sempre adicionar funções complementares a fim de enriquecer o valor de seu produto, entretanto nenhum possui uma ferramenta que favoreça a checagem de fatos estruturada dentro de seu próprio aplicativo. Nenhum mecanismo de autenticidade da

informação também se faz presente, permitindo que um usuário possa buscar de forma simples e ágil a veracidade da informação. É importante lembrar que a nossa sociedade teve pouco tempo para se adaptar ao fluxo de informações voraz estabelecido atualmente. Muitos aplicativos citados nesse trabalho têm por volta de 10 anos desde sua criação e o alcance que conseguiram nesse período é algo inédito na história da humanidade, fazendo com que a adaptação do público geral, ao fluxo informacional, fosse algo intangível em tão pouco tempo. É evidente que esses mecanismos possam ser usados de forma partidária ou até favoreça quem pagar mais, entretanto deve-se buscar a máxima neutralidade possível quando se trata de uma ferramenta que pode ser usada para manipular pensamentos de indivíduos.

Seguindo para as recomendações que governos nacionais poderiam seguir para combater a desinformação, “encomendar pesquisas para mapear a desordem da informação” e “Apoiar organizações públicas de mídia e de notícias locais” são bons pontos para se começar. Uma recomendação complementa a outra, a fim de obter resultados relevantes de pesquisas deve-se optar por investimentos em organizações que já trabalham com o assunto. Junto a isso, trabalhar melhor a rede local de informações das cidades do país para que casos como o de Fabiane, que fora antes mencionado, não ocorra novamente por mera falta de informação. “Regular as redes publicitárias” é notoriamente importante devido à imposição de vieses que podem ser veiculados para usuários independente de suas preferências, vale destaque para campanhas eleitorais que fazem uso dos mensageiros para poder se auto promover através de disparos em massa de informações infundadas. E por fim, “Realizar treinamentos avançados de segurança cibernética” é um tópico de suma importância para que cada usuário possa ser independente em sua busca por informação ao utilizar a Internet como um todo, sobretudo em aplicativos de mensagem afim de que se alcance entendimento sobre o conteúdo que recebeu e possa questionar o remetente sobre a veracidade da informação com propriedade.

Os jornais também desempenham função importante na hora de se informar a população, logo recomendações foram feitas sobre o que poderiam fazer para refrear a desinformação. Inicialmente, “Assegurar padrões éticos fortes em todas as mídias” e “Desmascarar fontes, bem como conteúdo” exerceriam um impacto significativo na qualidade das informações distribuídas online. Ao estabelecer esses critérios em cada publicação confeccionada, abandonando qualquer tipo de sensacionalismo barato, podemos alcançar novos padrões para que a credibilidade do jornalismo seja alcançada. Para que isso possa ser concebido, veículos partidários não deveriam ser tidos como fonte de informação segura, visto que, mesmo com uma notícia factível, a manipulação ideológica se faz presente e acaba por reduzir a confiabilidade da matéria. E por fim, deve-se “Produzir reportagens sobre a escala e

a ameaça representadas pela desordem da informação". O assunto desinformação apenas é tratado quando algum evento correlacionado com o tema vem à tona na mídia, e mesmo que seja tratado com atenção, ele permanece relevante durante o tempo que o evento trouxer engajamento para cada jornal. O tema não é amplamente tratado ou discutido com frequência mesmo que o insumo principal dos jornais sejam a informação, os profissionais que trabalham manuseando informação tendem a não demonstrar como o fazem, deixando seu consumidor a parte do mundo informacional.

Em conclusão precisamos pensar como a sociedade vigente deve se portar perante a desinformação, logo recomendações foram sugeridas para o combate das informações falsas. "Educar o público sobre a ameaça da desordem da informação" e "Agir como mediadores honestos" são duas alternativas a serem consideradas por indivíduos de todas as idades. A partir do momento que exista uma relação de confiança entre dois ou mais indivíduos, a persuasão se torna facilitada independente do assunto tratado. A barreira da idade também acaba por ser anulada caso as pessoas envolvidas nessa conversa sejam conectadas pela mesma geração, fazendo algo que propagandas ou apelos públicos não conseguem alcançar. E o compromisso com a honestidade deve ser um padrão a ser adotado para que nossa sociedade evolua como um todo, por mais que a desonestidade possa parecer mais lucrativa, devemos sempre considerar a verdade factível em primeira mão.

6 CONSIDERAÇÕES FINAIS

A disseminação de informações falsas por meio de aplicativos de mensagem representa um desafio significativo para a sociedade contemporânea. Embora os desenvolvedores dessas plataformas possam não ter intenções maliciosas ao criar seus serviços, é inegável que certas ferramentas disponibilizadas nesses aplicativos são frequentemente utilizadas para fins nefastos. Apesar das proporções que tais aplicativos têm alcançado na vida dos usuários, incluindo casos trágicos que resultaram em consequências irreversíveis, parece haver uma falta de esforço significativo para conter a disseminação de informações falsas. É crucial reconhecer que uma única informação falsa pode ter um impacto crucial na vida de um indivíduo, inclusive levando-o à morte, como exemplificado no caso de Fabiane. O compromisso com a privacidade irrestrita, muitas vezes justificado pelo discurso da liberdade de expressão absoluta, acaba por dificultar investigações criminais relacionadas aos agentes divulgadores de informações falsas.

As informações falsas são sempre enviesadas, criadas com o intuito de levar o receptor a acreditar em uma falsa verdade que beneficie o emissor. Os estudos analisados ao longo deste trabalho demonstraram, por meio de casos reais, que lidar com o fluxo de desinformação não pode ser adiado e requer ações imediatas. Embora já existam formas de reprimir o avanço da desinformação, é inegável que os agentes da desinformação evoluem em um ritmo acelerado, superando o desenvolvimento de ferramentas para combatê-los. Nesse contexto, a colaboração entre os setores público e privado desempenha um papel fundamental na luta contra a propagação de informações falsas. Regulamentações que incentivem a implementação de mecanismos de verificação de fatos devem ser consideradas fundamentais para usuários de redes sociais e aplicativos de mensagem. Caso os desenvolvedores de aplicativos não estejam dispostos a criar esses mecanismos, é responsabilidade do Estado fornecer apoio e recursos para iniciativas públicas capacitadas a desenvolvê-los.

Não obstante a isto, regulamentações como as que forma promovidas pelo projeto de lei número 2630, se fazem urgentes para cumprimento da vigente constituição brasileira em território online. Por muito tempo a Internet fora intitulada como “terra sem lei”, o que viabilizou a execução de crimes que violam o código penal do país sem quaisquer fiscalização e punição; por isso que o controle sobre os aplicativos de mensagem se faz importante para nosso país. Existem atualmente duas leis marcantes na história da regulamentação online, a lei Carolina Dieckmann e o Marco civil da internet, ambos trazendo grandes avanços para a segurança online; entretanto essas não se fazem suficiente perante aos avanços demonstrados

pelos meios de comunicações digitais, pois apenas duas regulamentações em 10 anos não são compatíveis com os avanços tecnológicos ocorridos durante esse período.

Contudo, a valorização de profissionais que trabalham com o manuseio da informação deverá ser aumentada em períodos de caos informacional online. Bibliotecários formados são lecionados em disciplinas diversas sobre como extrair uma informação, tratá-la e entregá-la para seu público de acordo com sua demanda. As próprias bibliotecas são organismos em constante adaptação para a demanda informacional que seu público almeja, fazendo com que informações de qualidade e com maior veracidade sejam entregues a quem precisa delas. É evidente que o fluxo informacional hoje é praticamente instantâneo através de smartphones, mas as bibliotecas, com bibliotecários capacitados, podem oferecer serviços que fundamentem muitos contextos expostos ao público através de informações falsas. O fluxo de informacional falso pode ser combatido através de um contra fluxo informacional com maior credibilidade, um fluxo que possa ir contra a desinformação para que se viabilize desconstrução do conteúdo enganoso através de fontes robustas e confiáveis. No entanto, mesmo que as ferramentas para combater a desinformação sejam implementadas, sua eficácia será limitada se os usuários não estiverem cientes da veracidade das informações verificadas. A politização da informação e o alinhamento partidário dos veículos de mídia contribuem para uma polarização que prejudica a credibilidade do jornalismo e perpetua a alienação dos usuários. Em última análise, enfrentar a questão das informações falsas nos aplicativos de mensagem requer uma abordagem equilibrada, que leve em consideração tanto os aspectos tecnológicos quanto os aspectos sociais envolvidos.

Em suma, a humanidade enfrenta um longo caminho no que diz respeito ao tratamento adequado da informação. Se, em uma década, testemunhamos um avanço desenfreado dos aplicativos de mensagem, não seria surpreendente esperar o surgimento de novas tecnologias que tornem as anteriores obsoletas. Esse é o grande desafio da contemporaneidade: lidar com os problemas que nós mesmos criamos, que em uma escala massiva e a uma velocidade nunca antes vista são permeadas para todo o mundo. É alarmante reconhecer que a humanidade pode estar entrando em um ciclo no qual cada nova tecnologia inventada será utilizada para disseminar ainda mais informações falsas.

Por outro lado, é esperançoso ver esforços voluntários de muitos agentes nas plataformas digitais para o combate a desinformação, perfis independentes que se movem para procurar fontes e desmentir informações falsas podem ser um pilar para a reversão do quadro que nos encontramos. Com a credibilidade dos jornais sendo constantemente questionada, talvez contarmos com pequenos portais sem alinhamentos políticos rígidos possa ser uma

resposta ao imenso indicie de desconfiança online. E caso os usuários digitais procurem por portais de notícias administrados por profissionais independentes e capacitados, além de possuir fontes fidedignas, esse usuário deve fazer uso dela sempre que algum indivíduo próximo lhe compartilhar alguma informação falsa. Tudo isso para que gradativamente possamos aumentar a qualidade e credibilidade das informações compartilhadas online.

REFERÊNCIAS

AMADEO, Ron. Facebook Messenger starts taking over Instagram Direct messages. **Ars Technica**, 17 ago. 2020. Disponível em: https://arstechnica.com/gadgets/2020/08/facebook-starts-merging-instagram-direct-and-facebook-messenger/. Acesso em: 29 jun. 2023.

BOCCATO, V. R. C. Metodologia da pesquisa bibliográfica na área odontológica e o artigo científico como forma de comunicação. **Rev. Odontol**. Univ. Cidade São Paulo, São Paulo, v. 18, n. 3, p. 265-274, 2006.

BRASIL. **Projeto de Lei n° 2630**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 26 jun. 2023.

CARVALHO, Caio. Facebook Messenger limita o encaminhamento massivo de mensagens no app. **UOL**, 3 set. 2020. Disponível em: https://gizmodo.uol.com.br/facebook-messenger-encaminhamento-mensagens/. Acesso em: 28 jun. 2023.

CETIC.BR. **TIC domicílios 2022**. 16 maio 2023. Disponível em: https://cetic.br/media/analises/tic_domicilios_2022_coletiva_imprensa.pdf. Acesso em: 29 maio 2023.

CHAVES, Mônica; BRAGA, Adriana. **A pauta da desinformação**: "fake news" e análise de categorizações de pertencimento na eleição presidencial brasileira em 2018. Brazilian Journalism Research, Brasília, DF, v. 15, n. 3, p. 498-523, dez. 2019.

DAROS, Gabriel. O que são CloutHub e Signal, novas redes procuradas por bolsonaristas. **UOL**, 1 nov. 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/11/01/o-que-sao-clouthub-e-signal-novas-redes-procuradas-por-bolsonaristas.htm. Acesso em: 29 jun. 2023.

DEFENSORIA PÚBLICA DO ESTADO DO PARANÁ. **Quais são os limites da liberdade de expressão?**. 23 mar. 2023. Disponível em: https://www.defensoriapublica.pr.def.br/Noticia/Quais-sao-os-limites-da-Liberdade-de-Expressao#:~:text=Constituição%20Federal%20de%201988,%20artigo,sociedade%20brasileira%20nos%20últimos%20anos. Acesso em: 24 jun. 2023.

DONOHUE, Brian. TextSecure sheds SMS in latest version. **Threat Post**, 24 fev. 2014. Disponível em: https://threatpost.com/textsecure-sheds-sms-in-latest-version/104456/. Acesso em: 29 jun. 2023.

DUFFY, Clare. Why messaging app Signal is surging in popularity right now. **CNN**, 13 jan. 2021. Disponível em: https://edition.cnn.com/2021/01/12/tech/signal-growth-whatsapp-confusion/index.html. Acesso em: 29 jun. 2023.

FESTINGER, Leon. **A theory of cognitive dissonance**. [S. l.]: Stanford University Press, 1962. 291 p. ISBN 0804709114.

FGVCIA. **Uso de TI no Brasil**: país tem mais de dois dispositivos digitais por habitante, revela pesquisa. 3 maio 2023. Disponível em: https://portal.fgv.br/noticias/uso-ti-brasil-pais-tem-mais-dois-dispositivos-digitais-habitante-revela-pesquisa. Acesso em: 29 maio 2023.

G1. **Quem executa o bloqueio do Telegram? Veja perguntas e respostas**. Globo, 26 abr. 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/04/26/quem-deve-executar-o-bloqueio-do-telegram-veja-perguntas-e-respostas.ghtml. Acesso em: 24 jun. 2023.

Galhardi, C.P., Freire, N.P, Minayo,M.C.S., Fagundes, M.C.M. **Fato ou Fake? Uma análise da desinformação frente à pandemia da Covid-19 no Brasil**. Cien Saude Colet [periódico na internet] (2020/Ago). [Citado em 25/06/2023]. Está disponível em: http://cienciaesaudecoletiva.com.br/artigos/fato-ou-fake-uma-analise-da-desinformacao-frente-a-pandemia-da-covid19-no-brasil/17733?id=17733&id=17733. Acesso em: 25 jun. 2023.

GREENBERG, Andy. Twitter acquires moxie marlinspike's encryption startup whisper systems. **Forbes**, 28 nov. 2011. Disponível em: https://www.forbes.com/sites/andygreenberg/2011/11/28/twitter-acquires-moxie-marlinspikes-encryption-startup-whisper-systems/?sh=3fd3644c30b9. Acesso em: 29 jun. 2023.

GREENBERG, Andy. WhatsApp co-founder puts $50M into signal to supercharge encrypted messaging. **Wired**, 21 fev. 2018. Disponível em: https://www.wired.com/story/signal-foundation-whatsapp-brian-acton/. Acesso em: 29 jun. 2023.

HAMBURGER, Ellis. Instagram announces Instagram Direct for private photo, video, and text messaging. **The Verge**, 12 dez. 2013. Disponível em: https://www.theverge.com/2013/12/12/5203302/instagram-direct-photo-text-messaging. Acesso em: 29 jun. 2023.

IMPERVA. **2023 imperva bad bot report**. 2023. Disponível em: https://www.imperva.com/resources/resource-library/reports/2023-imperva-bad-bot-report/. Acesso em: 25 jun. 2023.

INSTAGRAM. **Centro de ajuda**. Disponível em: https://help.instagram.com/1245691589716869/?helpref=hc_fnav. Acesso em: 29 jul. 2022.
JOHNSON, Jesse; OTAKE, Tomoko. **Unification Church says Abe shooting suspect's mother is follower**. The Japan Times, 11 jul. 2022. Disponível em: https://www.japantimes.co.jp/news/2022/07/11/national/crime-legal/abe-assassination-unification-church/. Acesso em: 1 jun. 2023.

JOHNSON, Khari. Facebook to expand Messenger home screen ads beta worldwide. **VentureBeat**, 11 jul. 2017. Disponível em: https://venturebeat.com/ai/facebook-to-expand-messenger-home-screen-ads-beta-worldwide/. Acesso em: 28 jun. 2023.

LE COADIC, Yves-François. **A ciência da Informação**. Brasília - DF: Briquet de Lemos, 1996. E-book 124 p. ISBN 85-85637-08-0. Disponível em: https://bibliotextos.files.wordpress.com/2012/07/a-cic3aancia-da-informac3a7c3a3o-le-coadic.pdf. Acesso em: 21 jun. 2023.

LEVINSON, Paul. **Fake news in real context**. [S. l.]: Connected Editions, 2016. 78 p. ISBN 1561780545.

M.G SIEGLER. Facebook's modern messaging system: seamless, history, and A social inbox. **Techcrunch**, 15 nov. 2010. Disponível em: http://tcrn.ch/cSIU7E. Acesso em: 28 jun. 2023.

MARÉCHAL, Nathalie. **From russia with crypto**: a political history of telegram. 2018. Disponível em: https://www.usenix.org/system/files/conference/foci18/foci18-paper-marchal.pdf. Acesso em: 25 jun. 2023.

MCLUHAN, Marshall. **Os meios de comunicação como extensões do homem: understanding media**. [S. l.]: Cultrix, 1969. 408 p. ISBN 8531602580.

MDN WEB DOCS. **Arpanet**. 6 nov. 2022. Disponível em: https://developer.mozilla.org/pt-BR/docs/Glossary/Arpanet#saiba_mais. Acesso em: 29 maio 2023.

META PLATFORMS INC. **Messenger centro de ajuda**. Disponível em: https://web.facebook.com/help/messenger-app. Acesso em: 28 jun. 2023.

MIRANDA, R. C. DA R.. **O uso da informação na formulação de ações estratégicas pelas empresas**. Ciência da Informação, v. 28, n. 3, p. 286–292, set. 1999.

NIEBORG, David B.; HELMOND, Anne. The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance. Media, Culture & Society, v. 41, n. 2, p. 196-218, 2019.

O GLOBO. **Designer de jogos Hideo Kojima é confundido com assassino de Shinzo Abe nas redes sociais; entenda**. O Globo, 7 ago. 2022. Disponível em: https://oglobo.globo.com/mundo/noticia/2022/07/designer-de-jogos-hideo-kojima-e-confundido-com-assassino-de-shinzo-abe-nas-redes-sociais.ghtml. Acesso em: 1 jun. 2023.
PANORAMA MOBILE TIME/OPINION BOX. **Mensageria no brasil**. Jan. 2023. Disponível em: https://www.mobiletime.com.br/pesquisas/mensageria-no-brasil-fevereiro-de-2023/. Acesso em: 1 jul. 2023.

PEREZ, Sarah. Facebook Messenger begins testing ads…and they're big. **Techcrunch**, 25 jan. 2017. Disponível em: http://tcrn.ch/2k4GGDN. Acesso em: 28 jun. 2023.

PRESSE, France. **O que se sabe sobre o suspeito do assassinato de Shinzo Abe, ex-primeiro-ministro do Japão**. Globo, 9 jul. 2022. Disponível em: https://g1.globo.com/mundo/noticia/2022/07/09/o-que-se-sabe-sobre-o-suspeito-do-assassinato-de-shinzo-abe-ex-primeiro-ministro-do-japao.ghtml. Acesso em: 1 jun. 2023.

REUTERS INSTITUTE FOR THE STUDY OF JOURNALISM. **Reuters institute digital news report 2022**. 2022. Disponível em: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-06/Digital_News-Report_2022.pdf. Acesso em: 6 jun. 2023.

ROSSI, Mariane. **Mulher espancada após boatos em rede social morre em Guarujá, SP**. G1 Santos, 5 maio 2014. Disponível em: https://g1.globo.com/sp/santos-regiao/noticia/2014/05/mulher-espancada-apos-boatos-em-rede-social-morre-em-guaruja-sp.html. Acesso em: 1 jun. 2023.

SETALVAD, Ariha. Instagram Direct gets a huge update focused on messaging your friends. **The Verge**, 1 set. 2015. Disponível em: https://www.theverge.com/2015/9/1/9236553/instagram-direct-messaging-update. Acesso em: 29 jun. 2023.

SHAUL, Brandy. Instagram: how to use end-to-end encryption in chats. **ADWEEK**, 16 fev. 2023. Disponível em: https://www.adweek.com/social-marketing/instagram-how-to-use-end-to-end-encryption-in-chats/. Acesso em: 29 jun. 2023.

SINGAL. **Suporte do signal**. Disponível em: https://support.signal.org/hc/pt-br. Acesso em: 29 jun. 2023.

TECHCRUNCH. Facebook chat launches, for some. **Techcrunch**, 6 abr. 2008. Disponível em: http://tcrn.ch/1Gabbe0. Acesso em: 28 jun. 2023.

TEIXEIRA, Tarcisio; SABO, Paulo Henrique; SABO, Isabela Cristina. **Whatsapp e a criptografia ponto-a-ponto**: tendência jurídica e o conflito privacidade vs. interesse público - 10.12818/p.0304-2340.2017v71p607. Revista da Faculdade de Direito da UFMG, v. 71, 29 dez. 2017. Disponível em: https://doi.org/10.12818/p.0304-2340.2017v71p607. Acesso em: 2 jul. 2023.

TELEGRAM. **Telegram FAQ**. Disponível em: https://telegram.org/faq. Acesso em: 25 jun. 2023.

TELEGRAM. **Telegram**. Disponível em: https://telegram.org. Acesso em: 25 jun. 2023.
THIERER, Adam; SZOKA, Berin. **Cyber-Libertarianism**: the case for real internet freedom. [S. l.]: The Technology Liberation Front, 2009. E-book (10 p.). Disponível em: https://pt.scribd.com/document/18490847/Cyber-Libertarianism-The-Case-for-Real-Internet-Freedom-Ver-1-0-Thierer-Szoka. Acesso em: 1 jul. 2023.

UOL. **Telegram manda mensagem em massa ligando PL das Fake News à censura**. UOL, 9 maio 2023. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2023/05/09/telegram-manda-mensagem-a-usuarios-criticando-pl-das-fake-news.htm. Acesso em: 25 jun. 2023.

WARDLE, Claire; DERAKHSHAN, Hossein. **A desordem da informação**. Disponível em: https://www.manualdacredibilidade.com.br/desinformacao. Acesso em: 26 jun. 2023.
WHATSAPP. **About us**. Disponível em: https://www.whatsapp.com/about. Acesso em: 14 jun. 2023.

WHATSAPP. **WhatsApp business**. Disponível em: https://business.whatsapp.com. Acesso em: 24 jun. 2023.

WHATSAPP. **WhatsApp centro de ajuda**. Disponível em: https://faq.whatsapp.com. Acesso em: 24 jun. 2023.

WHISPER SYSTEMS, Time de Desenvolvedores. **Announcing the public beta**. 25 maio 2010. Disponível em: https://web.archive.org/web/20100530011131/http://www.whispersys.com/updates.html. Acesso em: 29 jun. 2023.

YAP, Stephanie. Messenger group chat: how to create group chat in messenger. **Respond.io**, 25 nov. 2022. Disponível em: https://respond.io/blog/facebook-messenger-group-chat. Acesso em: 28 jun. 2023.