SEMIÓTICA EM APLICATIVOS MENSAGEIROS ANCORADA PELA LGPD COMO ESTRATÉGIA DE INTELIGÊNCIA COMPETITIVA

SEMIOTICS IN MESSENGER APPLICATIONS ANCHORED BY THE LGPD AS A COMPETITIVE INTELLIGENCE STRATEGY

Eunice Ribeiro Moreira[1]
Lucas de Castro Carvalho[2]
Jurema Suely de Araújo Nery Ribeiro[3]
Fábio Corrêa[4]
José Maurício Costa[5]

RESUMO
Esta pesquisa teve como objetivos identificar a maneira com que a adoção de políticas de segurança, à luz da semiótica, pode contribuir com o processo de inteligência competitiva nos aplicativos de mensageiros. O tema foi escolhido devido ao aumento dos ataques cibernéticos no Brasil, que foi o segundo país mais afetado na América Latina. A incompreensão e o desinteresse dos usuários quanto aos termos de política de privacidade fazem com que os dados fiquem vulneráveis. Neste caso, a aplicação da LGPD, de forma clara e criativa, é uma vantagem competitiva em aplicativos mensageiros. Para abordar o tema, analisou-se a política de privacidade do WhatsApp e Telegram. Como resultado, identificou-se a clareza na aplicação do *compliace* da LGPD nos dois aplicativo; o impacto da política de privacidade segurança dos dados dos usuários e o conhecimento relativo a estes, além da paridade entre os aplicativos; a Inteligência Competitiva em interação com a LGPD e a Semiótica na clareza das informações aos usuários e proteção de dados. A criptografia de ponta a ponta no WhatsApp teve destaque, por se estender a todas as interações. Em suma, a Inteligência Competitiva estabelece interação com a LGPD e a Semiótica na clareza das informações direcionadas aos usuários de aplicativos mensageiros. Tornando possíveis medidas necessárias para a proteção de dados.
PALAVRAS-CHAVE: LGPD, Inteligência Competitiva, Contrainteligência, Aplicativos mensageiros, Semiótica.

ABSTRACT
This research aimed to identify how the adoption of security policies, in the light of semiotics, can contribute to the process of competitive intelligence in messenger applications. The theme was chosen due to the increase in cyber-attacks in Brazil, placing it in second place among countries in Latin America. Users' lack of understanding and lack of interest in the terms of the privacy policy make your data stay vulnerable. In this case, the application of the LGPD, in a clear and creative way, is an advantage competitive in messenger apps. To address the topic, the privacy policy of WhatsApp and Telegram was analyzed. As a result, clarity was identified in the application of LGPD compliance in both applications; the impact of the privacy policy on the security of users' data and their knowledge, in addition to the parity between applications; Competitive Intelligence in interaction with the LGPD and Semiotics in the clarity of information to users and data protection. End-to-end encryption on WhatsApp was highlighted, as it extends to all interactions. In short, Competitive Intelligence establishes interaction with LGPD and Semiotics in the clarity of information directed to users of messenger applications. Making necessary measures for data protection possible.
KEYWORDS: LGPD, Competitive Intelligence, Counterintelligence, Messenger Apps, Semiotics.

[1] Mestranda em Sistemas de Informação e Gestão do Conhecimento – Universidade FUMEC, Brasil. *https://orcid.org/0000-0001-8470-3376*
[2] Mestrando em Sistemas de Informação e Gestão do Conhecimento – Universidade FUMEC, Brasil. https://orcid.org/0009-0000-2789-5340
[3] Doutora em Sistemas de Informação e Gestão do Conhecimento – Universidade FUMEC, Brasil. https://orcid.org/0000-0002-6465-6020
[4] Doutor em Sistemas de Informação e Gestão do Conhecimento – Universidade FUMEC, Brasil. E-mail: fabiocontact@gmail.com. https://orcid.org/0000-0002-2346-0187
[5] Doutorado em Ciências da Computação – UFMG, Brasil. https://orcid.org/0000-0002-0313-1335

1. INTRODUÇÃO

O crescimento do uso da Internet e os perigos da exposição dos dados, que circulam no ambiente cibernético, propiciaram a criação da Lei Geral de Proteção de Dados. A Lei nº 13.709, criada em 14 de agosto de 2018, torna-se cada dia mais relevante no Brasil, já que em 2022, ocorreram 88,5 bilhões de tentativas de ataques cibernéticos no país (FORTINET, 2023).

Os longos Termos de Políticas de Privacidade de aplicativos, somados a informações pouco claras, ou chamativas, aos olhos dos usuários proporcionam um ambiente mais oportuno para esses ataques. O que desafia as empresas de aplicativos mensageiros a aplicarem a Inteligência Competitiva, e assim passam a obter vantagens sobre o concorrente, na utilização de mecanismos que garantam a proteção dos dados de seus clientes/usuários.

A semiótica como estudo das linguagens, pode se destacar na contribuição da aplicação da Inteligência emocional, uma vez que estabelece a relação de entendimento entre o signo, objeto e interpretante. Enquanto a Inteligência Competitiva e a Contrainteligência se valem de unir dados espalhados entre os indivíduos, interpretá-los como informação e os transforma em conhecimentos a serem geridos para tomadas de decisões e proteção das informações organizacionais, a semiótica analisa se a entrega é compreensível ao seu cliente final, o usuário. Diante deste cenário, a pesquisa propõe responder a seguinte questão: de que maneira a adoção de políticas de segurança, à luz da semiótica, pode contribuir com o processo de inteligência competitiva nos aplicativos mensageiros?

Para responder a esta questão de pesquisa, este estudo tem como objetivo geral identificar a maneira com que a adoção de políticas de segurança, à luz da semiótica, pode contribuir com o processo de inteligência competitiva nos aplicativos de mensageiros. Para isto, foram estabelecidos três objetivos específicos: i) analisar a aplicação da *compliance* da LGPD em aplicativos mensageiros, ii) apontar o impacto da adoção de políticas de segurança em aplicativos mensageiros, iii) compreender o efeito semiótico da informação na aplicação de segurança como Inteligência Competitiva em aplicativos mensageiros.

A presente pesquisa se justifica devido ao crescimento do acesso à internet no Brasil, que já chegou a 152 milhões de usuários em 2020 (ICT HOUSEHOLDS, 2021). Tal crescimento impulsionou as tentativas de ataques cibernéticos no Brasil, colocando o país na segunda posição de ocorrência na América Latina (FORTINET, 2023). Poucos usuários de aplicativos, em geral, sabem como se proteger, não leem todo o termo da política de privacidade, e os que leem não têm as informações como claras. Ferreira, Pinheiro e Marques (2021), em sua pesquisa, identificaram em quatro estudos pesquisados a necessidade de alertar

os usuários sobre a preservação de dados íntimos. A análise das informações acessíveis ao usuário se faz necessária no apontamento das vantagens e desvantagens dos aplicativos mensageiros, sob a ótica da Inteligência Competitiva.

Diante disso, a pesquisa se subdivide em seções, em que a primeira sustenta três fundamentos teóricos em que a investigação é baseada. Em sequência, segue a metodologia utilizada, delineando os passos adotados, seguido pelas análises e resultados. Por fim, as conclusões são apresentadas, mostrando a relação dos resultados com as bases teóricas.

2. REFERENCIAL TEÓRICO

2.1. Lei Geral de Proteção de Dados

O abuso criativo das formas de se coletar dados, sem o expresso consentimento do usuário e a alta do mercado de informações, motivou em 2018 a aprovação, pelo legislativo brasileiro da Lei nº 13.709, da Lei Geral de Proteção de Dados (LGPD), com o intuito de garantir direitos individuais de cada usuário. A necessidade da aplicação da LGPD se dá aos recorrentes ataques cibernéticos. O Brasil foi o segundo país mais atingido da América Latina em 2022, expressando um aumento de 16% ao ano anterior. Das 360 bilhões de tentativas na América Latina e Caribe, pelo menos 88,5 bilhões ocorreram no Brasil em 2022, perdendo apenas para o México com 187 bilhões (FORTINET, 2023). Estes dados podem estar relacionados ao crescimento de acesso à Internet, quando passou de 74% em 2019, para 81% em 2020, chegando a 152 milhões de usuários (ICT HOUSEHOLDS, 2021).

> Ao ligar o GPS, pedir uma pizza, procurar um emprego ou mesmo transitar pelas ruas da cidade, as pessoas produzem informações que são coletadas e armazenadas em equipamentos eletrônicos, permitindo a quem colheu usá-las conforme seus interesses. Isso se torna um problema para os titulares dos dados e para a sociedade, quando essas informações são compartilhadas e disponibilizadas a terceiros. O que acaba transformando a vida particular em um *Reality Show*, tornando o indivíduo um objeto em constante vigilância" (RODOTÁ, 2008, p.19).

Segundo Harari (2019), o futuro dos dados é, talvez, uma das mais relevantes questões políticas atuais, uma vez que estes estão se tornando o capital mais importante do mundo. Por isso, entre os direitos garantidos pela LGPD destaca-se o fato de que os dados coletados pertencem ao usuário, porém garantindo o usufruto das companhias sobre eles. Caso o consentimento de manipulação destes dados seja dado pelo usuário, é necessário re-solicitar o consentimento a cada nova estratégia de manipulação que a empresa for adotar. Este consentimento poderá ser coletado por qualquer meio, desde que sejam apresentadas as

finalidades. Devendo ser disponível ao titular das informações a possibilidade de revogá-lo a qualquer momento, sendo vedado o tratamento sob qualquer forma de vício deste (MAGALHÃES; OLIVEIRA, 2021).

No entanto, a lei autoriza o uso de dados pessoais pelas empresas e entidades públicas, mas limita esse uso, estabelecendo garantias específicas para os titulares. Como o direito de acesso livre e facilitado aos dados tratados, direito de saber quais são eles, garantia de que a coleta e tratamento sejam realizados sob o mínimo necessário e, se possível, com o emprego das técnicas de anonimização, bem como o direito de retificação e de portabilidade, entre outros constantes nos artigos 17 a 22 da LGPD (MAGALHÃES; OLIVEIRA, 2021).

A Lei Geral Proteção de Dados (LGPD) impõe sanções variadas a quem infringir as regras. Inicialmente é dada uma advertência simples, que determina uma data para correção da irregularidade. Multas de até 2% do faturamento líquido da empresa também podem ser aplicadas, não chegando a mais de R$50 milhões, havendo a possibilidade também de aplicação de multa diária (BRASIL, 2018). Para que a empresa tenha longevidade e reputação é necessária a responsabilidade na manipulação dos dados dos clientes. Além de usar os dados como informações e conhecimento nas tomadas de decisões, a preservação dos usuários torna-se vital para sua fidelização.

2.2. Os aplicativos mensageiros

As mídias sociais se destacam como rica fonte de dados. Uma vez que os dados são a forma bruta da informação, quando deixados pelos usuários no ato das interações no ambiente digital, são captados para monitoramento das preferências dos consumidores e ofertas de produtos e serviços (OTTONICAR *et al.*, 2021). Entendendo seus últimos rastros digitais e seu perfil de uso no momento, gerado pelas identidades e comportamentos dos indivíduos e suas ações em redes digitais, estes se tornam moeda paga pelo uso gratuito de plataformas, *sites* e serviços *online*. O que fez com que o mercado de dados pessoais se tornasse uma forte fonte de renda para a economia brasileira. O cenário atual permite afirmar que o mercado de dados dará maior poder às corporações do que aos cidadãos em relação às trocas realizadas (SILVEIRA; AVELINO; SOUZA, 2016).

Contudo o volume de dados compartilhados neste ambiente, frente aos frequentes *cibercrimes*, traz a necessidade de medidas de segurança estabelecidas pelos donos desses aplicativos. Em resposta a essas necessidades, as empresas criadoras de aplicativos mensageiros, a fim de garantir a troca de mensagens mais seguras, implementaram recursos

como criptografia de ponta a ponta e verificação em duas etapas (o que protege a conta pessoal de invasão por *hackers*).

Conforme Kamara et al. (2021), a criptografia se destaca como elemento primordial na proteção e segurança do usuário, assim como sua liberdade de expressão no ambiente digital. Porém, nem todos os usuários têm conhecimento do que é criptografia de ponta a ponta. A criptografia se caracteriza pela encriptação, que pode ser comparada a uma assinatura ou cifra. Esta cifragem ocorre quando uma mensagem é criada e o usuário utiliza uma chave para acondicionar os dados da mensagem garantindo sua integridade, autenticidade e confidencialidade. O que antes escrito de forma lógica, ganha um código através da chave do emissor, que será decodificado, através da chave do remetente desta mensagem.

Os termos de políticas de privacidade das redes sociais online são fundamentais para a segurança do usuário. Mas se torna um risco quando o usuário não lê os termos e desconhece o quanto seus dados estão expostos. Outro problema está na falta de padronização dos termos, textos longos e linguagem de difícil compreensão dos usuários (FERREIRA; PINHEIRO; MARQUES, 2021). Problemas como esses podem ser minimizados com informações claras, textos curtos ou fragmentados em tópicos e uso de recursos que facilitam as informações pertinentes ao acordo feito entre empresa e usuário, quando preenchido na adesão do serviço por um simples clique.

O aplicativo WhatsApp surge dentro desta perspectiva. Criado pelo ucraniano Jan Koum e o americano Brian Acton, em 2009, o aplicativo começou com uma proposta de mensagem, modelo SMS, foi se adaptando às necessidades e desejos do usuário, agregando diversas mídias como: texto, fotos, vídeos, documentos, localização e chamadas de voz. Para oferecer maior segurança do usuário a empresa implementou a garantia de trocas de mensagens mais seguras com criptografia de ponta a ponta. Em 2014, a empresa foi vendida ao Facebook, possibilitando o compartilhamento de conteúdo entre as plataformas. Atualmente, o WhatsApp possui mais de dois bilhões de usuários em mais de 180 países (WHATSAPP LLC, 2023).

O Telegram sucedeu ao WhatsApp. Lançado em 14 de agosto de 2013, o aplicativo, num primeiro momento, foi direcionado para IOS, se estendendo para Android no dia 20 de outubro do mesmo ano. Pavel foi quem idealizou o Telegram e hoje é o apoiador financeiro. Nikolay Durov foi o mentor no campo da tecnologia, a partir de um protocolo com dados exclusivos. Tais dados são abertos, porém, seguros podendo otimizar o trabalho com diversos centros de dados. Este tem como foco a velocidade e segurança, dispondo de criptografia de ponta a ponta, com aplicação diferenciada de seu concorrente. A popularidade do Telegram já soma mais de

700 milhões de usuários ativos, sendo um dos 10 aplicativos mais baixados em todo o mundo (TELEGRAM, 2023).

Ambos investem em seu potencial focando em seu nicho e suas necessidades, buscando atualizações e soluções mais efetivas para sua consolidação no mercado de aplicativos mensageiros.

2.3. Inteligência Competitiva e Contra Inteligência

A inteligência, propriamente dita, pode ser compreendida a partir de três vertentes. Como atividade, no que tange à produção da inteligência, como produto dessa atividade e como organização que exerce a atividade produtora da inteligência (RIBEIRO; CARDOSO-JUNIOR, 2021). Já a Inteligência Competitiva tem por propósito contribuir nas tomadas de decisões antecipadas frente aos agentes do macroambiente (RIBEIRO; CARDOSO-JUNIOR, 2021; OTTONICAR *et al*., 2021).

Para a garantia de sua aplicação, a inteligência competitiva passa por quatro fases, sendo elas: planejamento, coleta, análise e difusão que requerem procedimentos, políticas e infraestruturas adequadas (RIBEIRO; CARDOSO-JUNIOR, 2021). Ferro (2019) corrobora apresentando o papel da Inteligência Competitiva como facilitadora dos processos de análise do mercado e mensuração do desenvolvimento da concorrência, por meio de dados balizadores que possam levar a organização a um desempenho superior ao de seu oponente. Segundo Cardoso-Júnior (2008), uma empresa só se torna competitiva quando consegue reduzir as ameaças diante de novas empresas concorrentes, vencer as rivalidades através do posicionamento no mercado e, consequentemente, a pressão dos consumidores e fornecedores.

Para isso, a Inteligência Competitiva envolve pessoas na seleção de informação, treinamento e gestão de conhecimento, além de informações como elemento necessário à empresa e na capacitação de seus membros, quando o conhecimento extraído tende a trazer um reflexo positivo aos negócios da empresa (RODRIGUES; RISCAROLLI; ALMEIDA, 2011).

O processo começa na identificação da informação, passando pela seleção, captação, depuração e distribuição da mesma, até que seja sociabilizada em todas as áreas, agregando novos elementos que consolidaram a gestão do conhecimento nas organizações. A cada socialização, outros elementos vão sendo agregados ao conhecimento primário na formação do espiral do conhecimento (RODRIGUES; RISCAROLLI; ALMEIDA, 2011; TAKEUCHI, NONAKA, 2008). Este é transformado em inteligência competitiva, quando bem empregado pelos executivos nas tomadas de decisão (RODRIGUES; RISCAROLLI; ALMEIDA, 2011).

Considerando as mudanças imprevisíveis que ocorrem no ambiente organizacional, a contrainteligência se faz necessário como barreira de proteção frente à inteligência competitiva da concorrência. Esta barreira utiliza medidas que previne e impede o avanço dos concorrentes, detectando e neutralizando estratégias, por eles utilizadas, fundamentadas em coletas de informações importantes. Enquanto a inteligência competitiva foca em conhecer a concorrência, a contrainteligência centra-se em proteger informações organizacionais, das quais se baseiam o seu diferencial (CARDOSO-JÚNIOR, 2008).

2.4. Semiótica das interfaces

A Semiótica é compreendida como a ciência que estuda todas as expressões linguísticas. O teórico Charles Peirce pauta a semiótica na tríade objeto – signo – interpretante, na qual deriva a semiose. A semiose, por sua vez, ocorre na interpretação do significado do signo (que representa o objeto), pelo seu interpretante. O que começa pela percepção da qualidade do signo, evolui para uma reação racional, na compreensão do que é percebido e culmina na comprovação dos dados apresentados que leva a interpretação do objeto. Nesse processo os cinco sentidos são empregados na formulação da linguagem (SANTAELLA, 1983).

Peirce categoriza os signos em três tricotomias. Na Primeiridade o signo se relaciona com ele mesmo. Quando relacionado a uma qualidade, é chamado de quali-signo, quando há uma referência, sin-signo, e quando há algo legalmente reconhecido é chamado de legi-signo. Na Secundidade, o signo se relaciona com o objeto sendo chamado de quali-signo-icônico, quando relacionado à sua semelhança. É considerado legi-signo-indicativo quando a referência do signo indica possibilidade de ser determinado objeto. Quando aponta para algo determinado por lei, considera-se um legi-signo-simbólico. Na Terceiridade o símbolo se relaciona com seu interpretante, quando o signo representa uma única coisa é chamado de legi-signo indicativo dicente. Quando representa um ou duas coisas semelhantes, é chamado de simbólico remático e é chamado de simbólico dicente quando relacionado a proposição ordinária, em uma sentença que pode ser verdadeira ou falsa (SANTAELLA, 1983).

Com base na compreensão das categorias tricotômicas da Semiótica, a Ciência da Computação se vale da Engenharia Semiótica na construção de interfaces respondendo às necessidades e desejos do usuário. A Engenharia Semiótica se preocupa com a comunicação humana por meio de sistemas computacionais. Entre o sistema e o usuário está o *designer*, que comunica com o usuário por meio de interfaces (CARVALHO *et al*., 2010). Pela ótica de Peirce, a interface é o universo dos signos, o objeto é o *designer*, representado pelas propostas

comunicacionais, enquanto o interpretante é o usuário que interpreta os signos a partir de suas percepções (CORTEZ, 2012). A semiose ocorre quando o usuário transforma a mensagem do designer em metamensagem, através da interface, chegando ao objetivo de comunicabilidade do sistema, na qual é testada e comprovada as limitações e potencialidade do *hardware* e *software* (CARVALHO *et al*., 2010; BARBOSA *et. al.*, 2021; ARAMUNI; MAIA, 2018).

3. METODOLOGIA

Por ter como objetivo gerar conhecimento científico a presente pesquisa se caracteriza como básica (MENEZES *et al,* 2019). Por estar fundamentada no tema e suas variáveis, apresenta com a abordagem qualitativa e exploratória por aprofundar a investigação sobre algum tipo de fenômeno (BARDIN, 1977; MARCONI; LAKATOS, 2003). Para responder à questão de pesquisa, foi realizada uma análise comparativa entre as interfaces das principais plataformas, sendo elas Telegram e WhatsApp. As coletas de dados foram feitas a partir dos aplicativos citados. Como base teórica para analisar os dados, empregou-se uma revisão bibliográfica com a temática abordada (MENEZES, 2019).

4. RESULTADOS E DISCUSSÃO

Com o intuito de chegar na resposta da pergunta de pesquisa, os dados foram analisados a partir dos objetivos específicos. Sendo necessário analisar a aplicação da *compliance* da LGPD em aplicativos mensageiros, apontar o impacto da adoção de políticas de segurança em aplicativos mensageiros, compreender o efeito semiótico da informação na aplicação de segurança como Inteligência Competitiva em aplicativos mensageiros. Entendendo o nível de clareza das informações disponíveis aos usuários convencionais, confrontando-as com a políticas de segurança, com a interface ofertada por cada uma.

4.1. Aplicação da Compliance da LGPD em aplicativos mensageiros

Os prints desta seção busca analisar os textos relativos ao *compliace* da LGPD nos aplicativos pesquisados, quanto à forma como é exposta ao usuário, a clareza das informações usadas pelas empresas concorrentes e o cumprimento da LGPD.

Ao observar a Figura 1, dentro dos termos da política de privacidade das plataformas, identificou-se que ambas coletam dados dos usuários, porém com finalidades diferentes. Para o Telegram dois princípios fundamentais são aplicados, quando se trata da coleta e tratamento de dados pessoais. O aplicativo informa não usar dados pessoais de seus usuários para mostrar

anúncios e, simplesmente, armazena os dados que esta precisa para funcionar como um serviço de mensagens seguro. Tendo assim seu escopo de coleta bem reduzido a funcionalidades ofertadas.

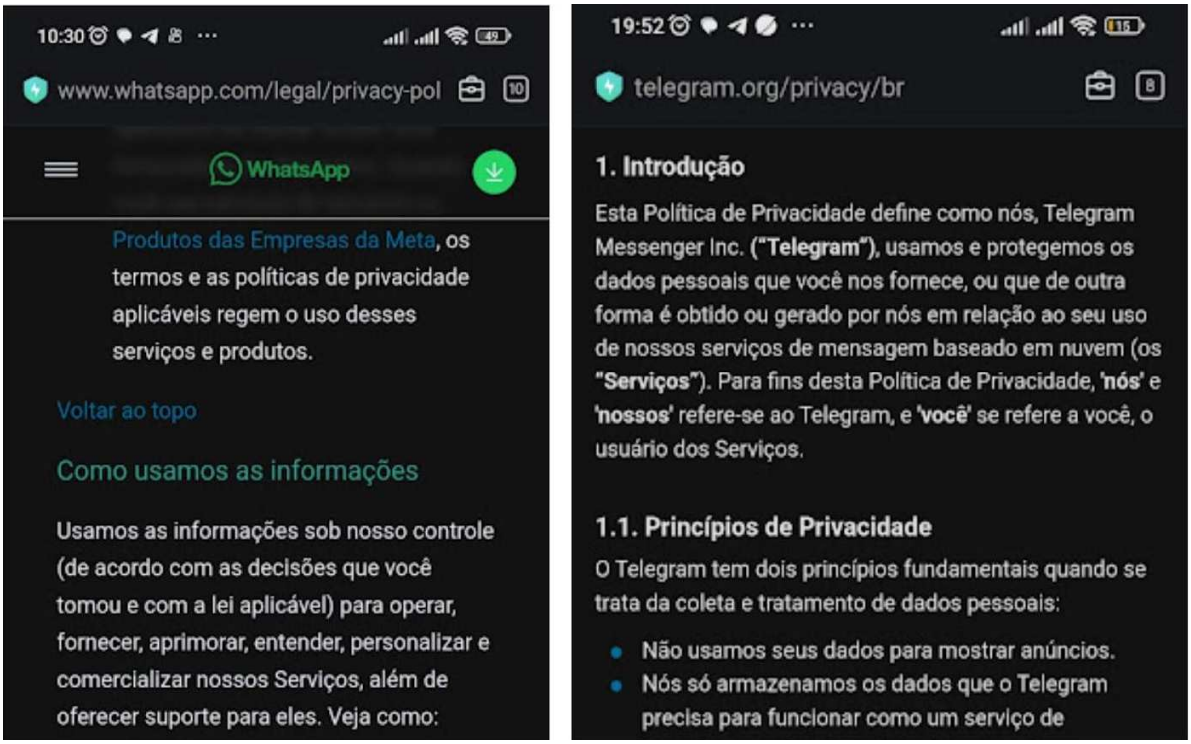

Figura 1 - Informação sobre coleta de dados do Telegram e WhatsApp
Fonte: Telegram e WhatsApp (2023)

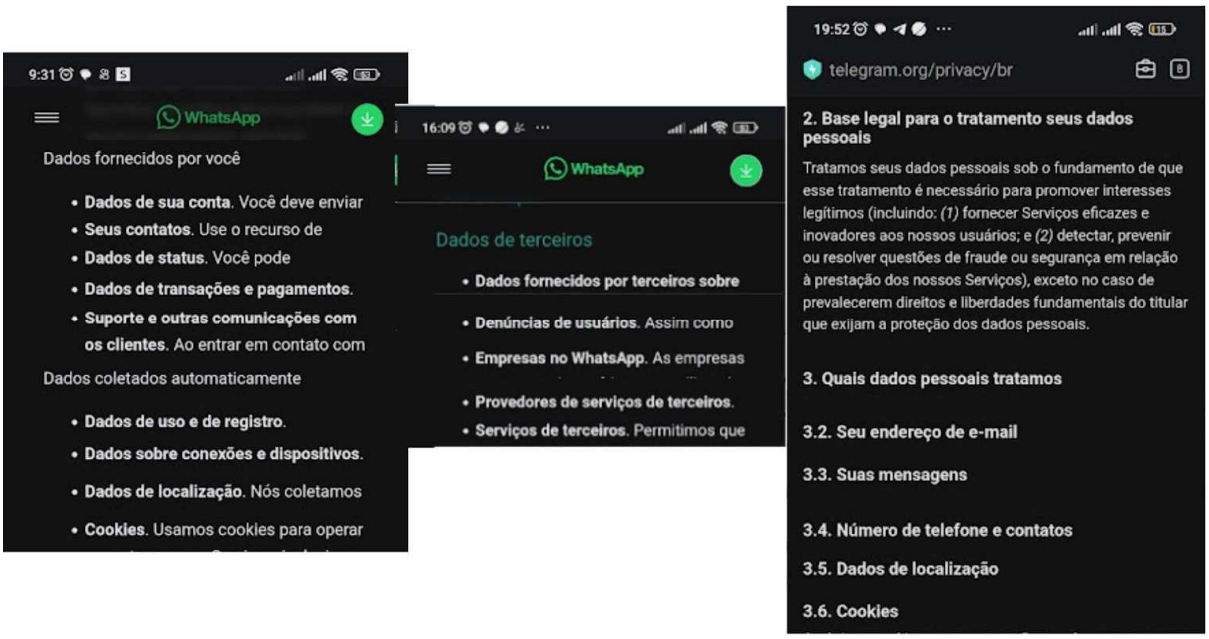

Figura 2 - Dados coletados no WhatsApp e Telegram
Fonte: WhatsApp e Telegram (figura adaptada ressaltando os tópicos principais, 2023)

A Figura 2 mostra que no Whatsapp a coleta de dados pessoais, descrita nas políticas de privacidade, demonstra ser mais intensa. O número de informações coletadas é significativamente maior que a do Telegram, fazendo parte de um ecossistema de coleta e disponibilização de informações do usuário ligados ao grupo Meta. Assim, são cruzadas com informações fornecidas por terceiros e com as geradas, através da coleta via uso da plataforma.

Ambas trazem a coleta de dados pessoais descritas em seus contratos de uso, mas não notificam o usuário visualmente quando as informações estão sendo coletadas. Resguardam o momento que o sistema operacional pede permissão para utilização de recursos, como geolocalização. Também, não se mostrou possível, através dos menus recusar, o compartilhamento dos dados ou visualizar as coletas já feitas.

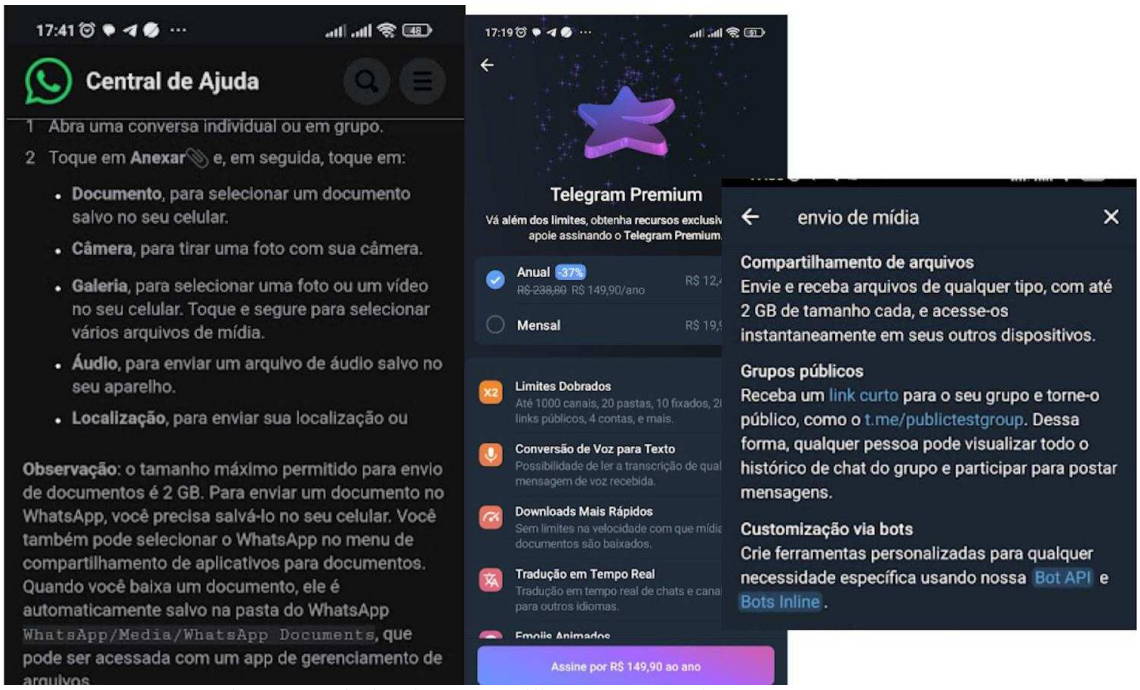

Figura 3 - Limite de compartilhamento no Telegram (2023)
Fonte: Telegram (2023)

Conforme mostra a Figura 3, o envio de mídias no Telegram é de até 2GB, seja arquivos ou áudios. É permitido que o chat por voz tenha um número ilimitado de pessoas, é permitido que assim como vídeo de chamadas ter no máximo 30 pessoas e a cada grupo possua até 200.000 integrantes. Permite-se que o usuário assine a plataforma para obter recursos extras, como transcrição de áudio e remoção de anúncios. No Whatsapp, o envio de mídias, também, é de 2GB, quando enviado pelo menu anexar, sendo que os vídeos gravados pelo aplicativo são liberados em até 16MG. É permitido que o chat por voz tenha até 32 pessoas. Permite-se que

vídeo de chamadas tenham no máximo 8 pessoas, e cada grupo 1.024 integrantes, não tendo plano de assinatura para vantagens extras.

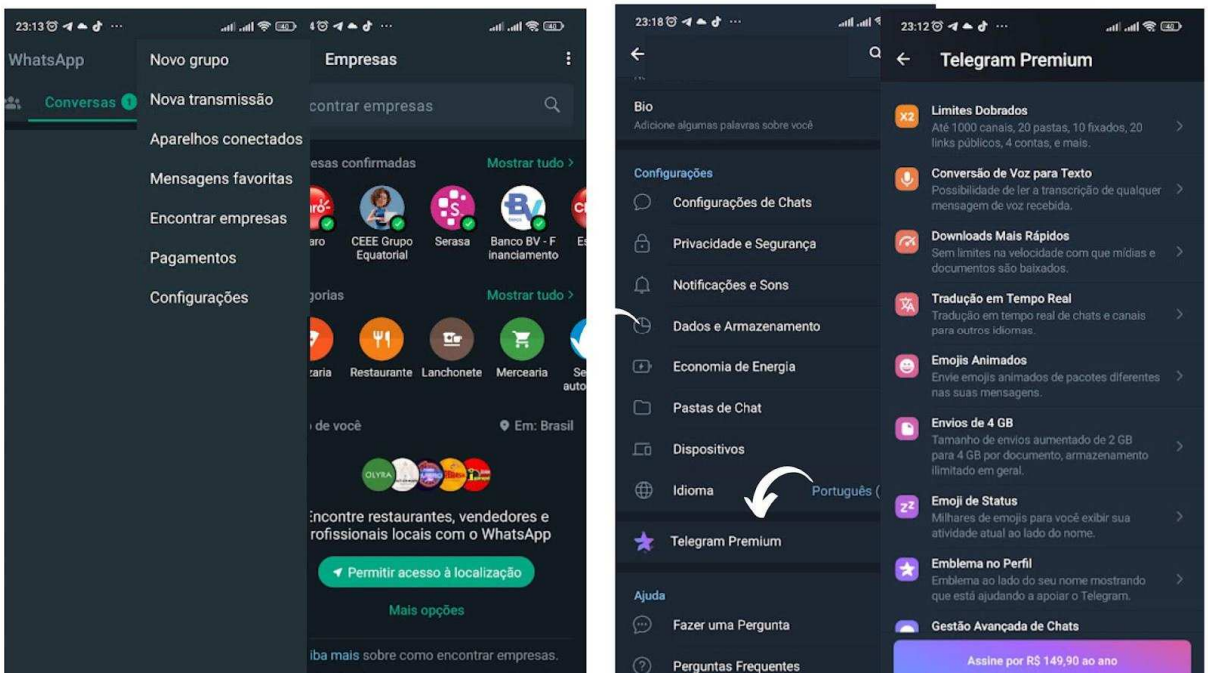

Figura 4 - Como se dá os códigos das empresas no WhatsApp e Telegram
Fonte: Telegram e WhatsApp (2023)

Na Figura 4, nota-se que mesmo sendo aplicativos de um mesmo nicho, o direcionamento do Telegram demonstra ser para um público mais específico. Pois possibilita a criação de grupos com capacidade elevada de pessoas, envio de arquivo consideravelmente grandes e a possibilidade de elevar esses números com o recurso premium, alinhados à construção de *Bots*. O Telegram aparenta para atingir nichos de mercado específicos, como grandes empresas, criadores de conteúdo e até perfis técnicos.

A construção dos *Bots* é um recurso explorado pela plataforma por permitir desenvolvedores a criarem recursos adicionais para acoplar ao código da empresa, não existindo a necessidade de ser descrita dentro do próprio Telegram. Pois o público de desenvolvedores naturalmente procuraria conteúdo relacionado na documentação da plataforma. Já o WhatsApp expõe seus clientes business, e seus respectivos serviços, de uma forma pré-estabelecida.

Os resultados mostraram que as plataformas seguiram a aplicação da *compliance* da LGPD, agrupando e compartilhando informações claras aos usuários, conforme a prática da gestão do conhecimento (RODRIGUES; RISCAROLLI; ALMEIDA, 2011). Ambas demonstraram clareza documental da coleta, tratativa dos dados e recursos disponíveis para segurança de seus usuários. Os textos utilizados foram organizados por temas, facilitando o

acesso. Porém as informações não dão ao usuário a opção de recusar qualquer parte do termo que seja. O entendimento de cada item analisado por este artigo, partiu da construção de um conhecimento prévio para ser entendido. Construção essa que não acontecerá no uso cotidiano dessas plataformas.

4.2. O impacto da adoção de Políticas de Segurança em aplicativos mensageiros

A partir dos conjuntos que compõe a política de segurança, resumidos no Quadro 1, observou-se o que se pode caracterizar como força ou fraqueza de cada plataforma.

Quadro 1 - Critérios de Análise da Pesquisa

	Telegram	Whatsapp
1) Coleta de dados pessoais		
1.1) Coleta dados do usuário	✓	✓
1.2) Tipos de dados coletados	Endereço de email, Contatos da lista telefônica	Contatos da lista telefônica, Informações financeiras, Localização, Informações de contato, Conteúdo do usuário, Dados de uso e Dados de diagnóstico
2) Disponibilidade das informações geradas pelo usuário para terceiros		
2.1) Permite envio de mídias	✓	✓
2.2) Tamanho máximo para envio de mídias	2GB	16MB
2.3) Mídias podem ser lidas pela empresa do aplicativo	✓	✗
2.4) Chat de voz	✓	✓
2.5) Quantidade de pessoas por chat de voz	Ilimitado	32
2.6) Video chamadas	✓	✓
2.7) Capacidade de pessoas video chamada	30	8
2.8) Permite criar grupos	✓	✓
2.9) Quantidade de pessoas por grupo	200.000	1.024
2.10) Permite usar Bots	✓	✗
2.11) Modo premium	✓	✗
3) Politicas de segurança		
3.1) Permite usar verificação em duas etapas	✓	✓
3.2) Criptografia ponta a ponta ativa por padrão	✗	✓
3.3) Permite chat secretos	✓	✓
3.4) Código aberto	✓	✗

Fonte: elaborada pelos autores (2023)

A luz dos dados citados no Quadro 1, notou-se que a competitividade entre as plataformas as tornou praticamente niveladas em recursos disponíveis. Observa-se uma diferenciação, quanto a disponibilidade de uso desses recursos e a abordagem sobre assinantes da plataforma chamada de modo premium, que se destaca como diferencial, dependendo do público-alvo escolhido por cada uma. É permitido, em ambas as partes, que o usuário envie mídias digitais, faça chamadas de voz, crie grupos e faça vídeo chamadas.

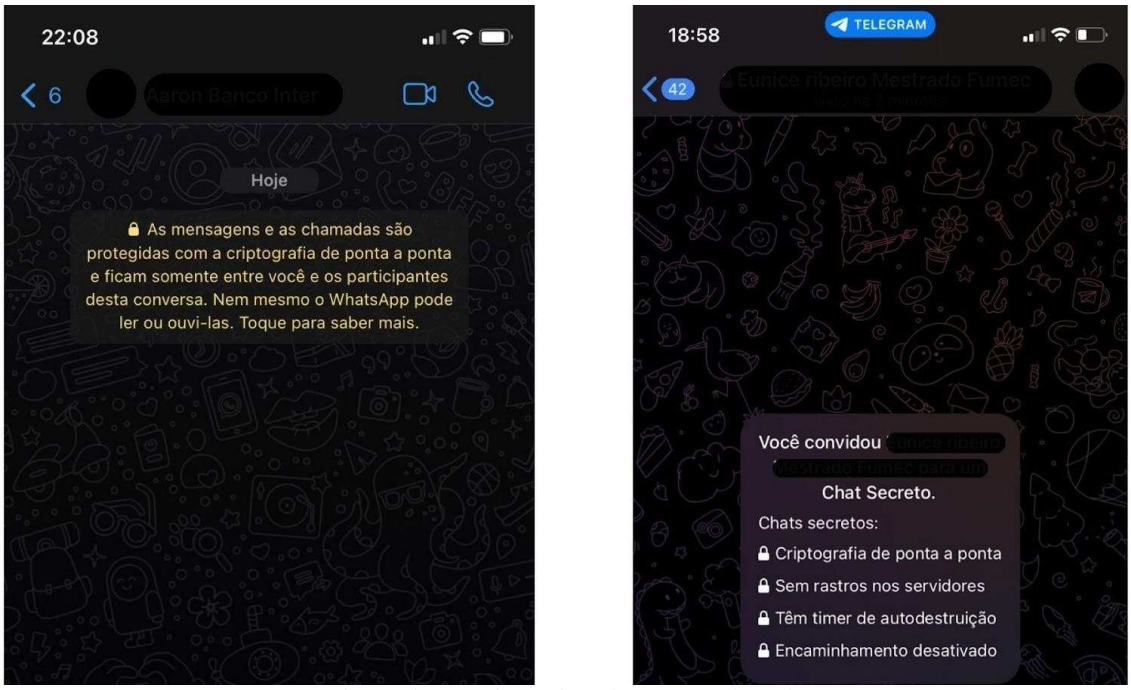

Figura 5 - Interfaces do WhatsApp e do Telegram
Fonte: WhatsApp e Telegram (2023)

Foi encontrado o diferencial nas plataformas ao analisar as políticas de segurança de cada uma. A confirmação em duas etapas, como uma camada a mais de proteção conta de invasão de Hacker, é uma opcional, no qual é criada uma senha e de segurança e um cadastro de e-mail, como forma de recuperação de senha. Sem esta ninguém poderá acessar a conta. Uma vez aplicada a confirmação, todas as interações, sejam troca de mensagens por texto ou áudio, ou mesmo vídeos e áudio chamadas são protegidas, como mostra a Figura 5. Observa-se também, que no Telegram, a criptografia de ponta a ponta é ativada facultativamente. Porém, a ativação da mesma não garante a segurança de todas as trocas de dados, mas somente do contato selecionado para “chat secreto”. Quando não ativado este recurso, os conteúdos gerados são considerados como conversas "públicas” pela plataforma. Podendo ser lidas pela empresa. O que não significa que sejam, mas que tecnicamente é possível.

Como resultado desta análise, é visto que a política de privacidade dos aplicativos impactam na segurança dos dados do usuário, assim como no conhecimento relacionados aos

dados coletados pelas empresas e de como são usados. No que tange a disponibilidade de recursos de *cibersegurança*, notou-se uma paridade entre ambas, tendo basicamente os mesmos recursos disponíveis. Contudo, como descrito na Figura 5, o Whatsapp demonstra superioridade no fator criptografia ponta a ponta, por todos seus *chats* serem criptografados por padrão e pela falta de exploração desses recursos de forma visual na plataforma Telegram.

O Telegram demonstra força, quando analisamos o fato dele não fazer parte de um grande grupo que coleta inúmeras informações do usuário, tendo seu código aberto, permitindo assim auditoria externa, o que se torna um grande diferencial competitivo para usuários mais especializados e preocupados com a segurança de seus dados. A LGPD sugere que conteúdos compartilhados pelo usuário mesmo em redes sociais e de mensagerias podem estar isentos sob a análise de alguns critérios da mesma, uma vez que foi decisão do usuário compartilhá-las (BRASIL, 2018).

4.3. O efeito semiótico da informação na aplicação de segurança como Inteligência Competitiva em aplicativos mensageiros

Os prints apresentados nesta seção apresentam o efeito semiótico na transmissão das informações, conforme o contexto do usuário como inteligência competitiva.

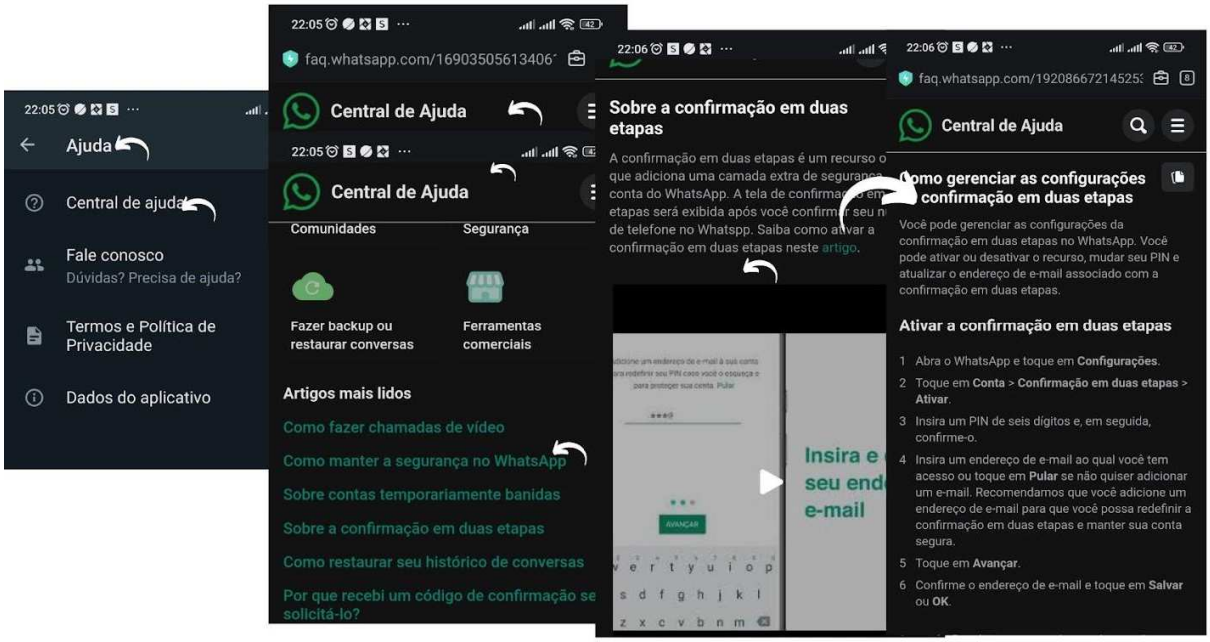

Figura 6 - Acesso às informações de Confirmação em Duas Etapas no WhatsApp
Fonte: WhatsApp (2023)

No quesito segurança, conforme mostra a Figura 6, o WhatsApp se destaca nas informações sobre confirmação/ou verificação em duas etapas, explorando signos e

significados para garantir a compreensão do usuário. O Aplicativo, também, explora visualmente o fato de ter a criptografia de ponta a ponta por padrão em sua plataforma, direcionando este conhecimento para seu público e expondo para seus usuários a mensagem. Por sua vez, o Telegram também possui criptografia ponta a ponta dispondo dos signos e significados, como o do concorrente, mas o usuário precisa optar por ativá-la, diferente do Whatsapp que é um recurso ativo por padrão.

Ao analisar as políticas de privacidade da plataforma Telegram confrontando o fato de que a criptografia ponta a ponta, não existe, por padrão, nos *chats*. As informações sobre a aplicação da confirmação em duas etapas no WhatsApp são praticadas de forma clara e didática, fazendo usos de texto tutorial e vídeo, conforme mostra a Figura 6.

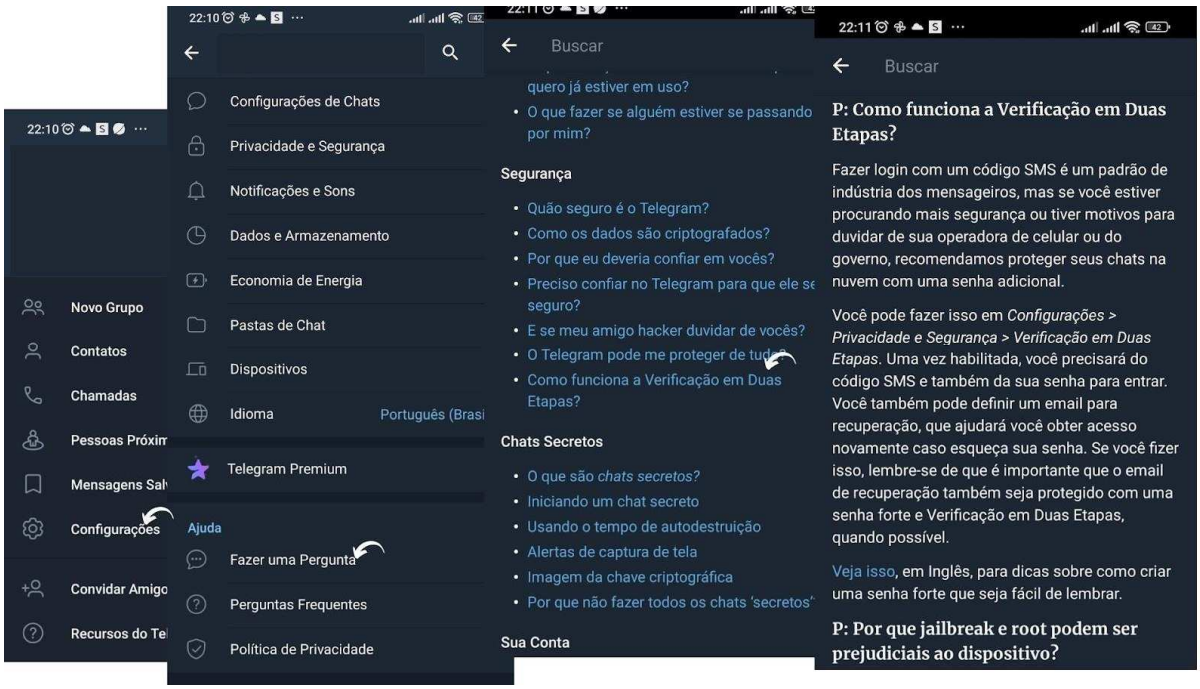

Figura 7 - Acesso às informações de Verificação em Duas Etapas no Telegram
Fonte: Telegram (2023)

No Telegram, como mostra a Figura 7, a aplicação é feita com clareza, com textos curtos, sem emprego de imagem e sem tutorial em vídeo. Neste caso, os textos são subdivididos em tópico, utilizando mensagens claras.

A leitura, à luz da semiótica, apresenta maior clareza da linguagem entregue ao usuário, quando os signos/palavras representados são de fácil compreensão para quem o interpreta. Uma mensagem com utilização imagética traz uma melhor compreensão, conforme menciona Cortez (2012). A aplicação de imagens, no direcionamento deste conhecimento ao público, deixa mais

evidente a mensagem, possibilitando uma escolha mais assertiva para o usuário. Levando, assim, conhecimento ao usuário de que seus dados estão sendo coletados e oferecendo recursos para o auxílio no *compliance* com a LGPD. A disponibilização e manipulação de seus dados é um direito garantido por lei e poderia ser apoiada pela semiótica nestes contextos. Desta forma o WhatsApp reconhece sua força diante de seu concorrente, aumentando a segurança contra os ataques cibernéticos, o que estabelece uma relação de confiança entre empresa e usuário.

Observou-se a aplicação da Inteligência competitiva em elementos utilizados por uma plataforma ou outra. No processo da gestão do conhecimento, notou-se a organização das informações por tema e conforme as dúvidas mais frequentes, quanto a aplicações de medidas de segurança. No caso da verificação em duas etapas no Whatsapp, a disponibilidade da informação se valeu do recurso áudio visual. A criptografia e a confirmação ou verificação de ponta a ponta se destacaram como contrainteligência, quando propõe evitar ataques cibernéticos contra o perfil do usuário. As informações trazidas de forma clara e ilustrativa, mostra a importância da semiótica, quando a mensagem transmitida é construída por meio de signos cujos usuários conhecem o significado. Assim a aplicação da LGPD se torna clara quando explicada através dos recursos da semiótica. No contexto dos aplicativos mensageiros a Inteligência competitiva, a LGPD e a Semiótica interagem, uma colaborando com a outra.

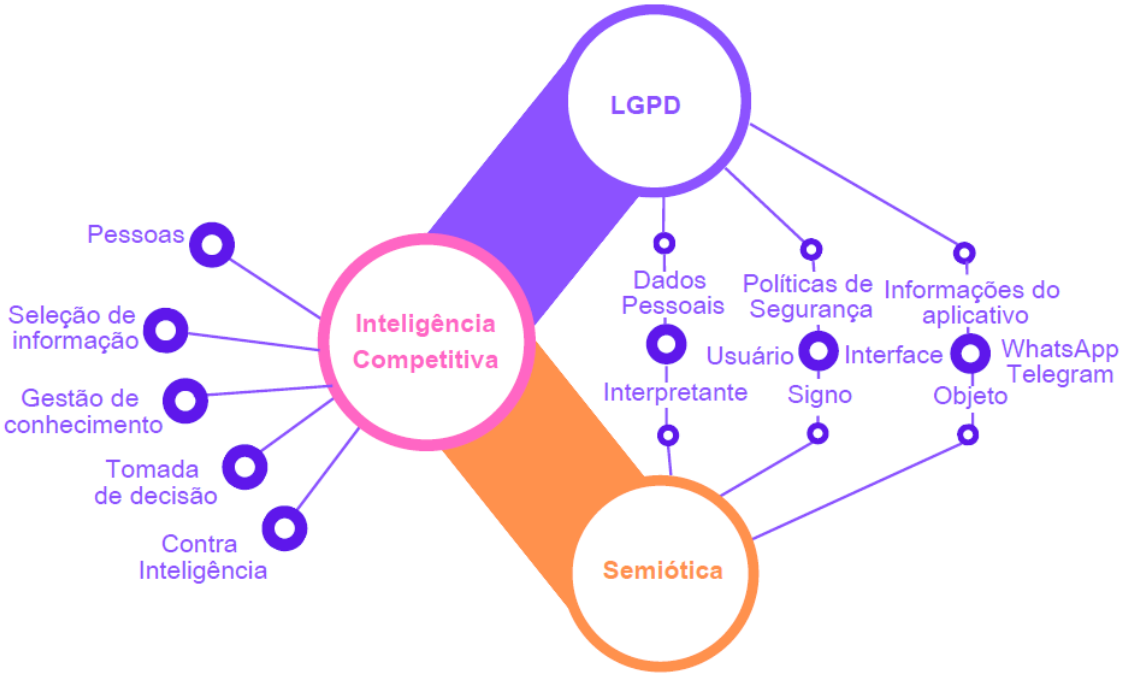

Figura 8 - Interação entre a Inteligência Competitiva, LGPD e Semiótica
Fonte: Autores 2023

Como mostra a Figura 8, a Inteligência Competitiva pode estabelecer interação com a LGPD e a Semiótica na clareza das informações direcionadas aos usuários de aplicativos mensageiros. Os dados são coletados dos usuários (pessoas), tornando-se em informações dentro do aplicativo. A política de Segurança é criada a partir das informações e como forma de garantir a segurança dessas informações. As medidas utilizadas para esta segurança efetiva se dão pela gestão do conhecimento, organizada nos aplicativos. A tomada de decisão em disponibilizar mecanismos que facilitem a vida do usuário, conquistando sua confiança, caracteriza-se como inteligência competitiva. E quando usada como forma de se antecipar frente à concorrência e agir de forma preventiva, esta se estabelece como Contra Inteligência. Na tríade da semiótica, a política de segurança é apresentada por meio dos signos na interface do aplicativo. O interpretante que a interpreta está relacionado a LGPB mediante seus dados coletados. O objeto a ser compreendido por meio dos signos são as informações transmitidas pelos aplicativos WhatsApp e Telegram. Neste contexto, Todas as informações, quando disponível de forma clara, dentro do contexto do usuário, se valendo de signos cujo significados são acessíveis, são usadas à luz da semiótica contribuindo com o sucesso da organização.

A inteligência competitiva de uma empresa deve contar com um bom suporte de Tecnologia da Informação e a aplicação da gestão da informação e do conhecimento tornando as funções e informações acessíveis ao usuário (CARDOSO-JUNIOR, 2008).

5. CONSIDERAÇÕES FINAIS E IMPLICAÇÕES

Este estudo descreveu a importância dos termos da política de privacidade, nos aplicativos mensageiros, descrito de forma clara sob a perspectiva semiótica. A clareza das informações, com recursos imagéticos e linguagem acessível, podem assegurar os usuários de possíveis ataques cibernéticos. Isto é, quando a empresa de aplicativos mensageiros utiliza de estratégias diferenciadas, esta aplica a inteligência competitiva tendo ganho sobre a concorrência. Mas quando estas estratégias se destacam, como conhecimento capaz de impedir ataques e prejuízos contra os dados trabalhados por ela, a inteligência competitiva avança para a prática de contrainteligência.

5.1. Contribuição da pesquisa

Considerando o contexto, este estudo trouxe esclarecimento sobre a eficácia da aplicação da Lei de Proteção de dados, dentro da prerrogativa da semiótica, com vantagem competitiva de empresas de aplicativos mensageiros. Assim, compreendida com estratégias da Inteligência Competitiva e contrainteligência, na utilização da Gestão do Conhecimento.

5.2. Implicações teóricas e práticas

Tendo como objetivo identificar de que maneira a adoção de políticas de segurança, à luz da semiótica, pode contribuir com o processo de inteligência competitiva nos aplicativos mensageiros, observado sob a base teórica a prática da Lei Geral de Proteção de Dados praticadas nos aplicativos mensageiros – WhatsApp e Telegram – notou-se a aplicação da *compliace* da Lei Geral de Proteção de Dado, com clareza das informações em ambos os aplicativos. Foram notados os textos informativos organizados tematicamente, com fácil acesso. Porém, o usuário não tem a opção de recusar qualquer parte do termo.

Sob o amparo da inteligência e contrainteligência, utilizada a partir da gestão do conhecimento, observou-se o impacto da política de privacidade na segurança dos dados dos usuários e o conhecimento relativo a estes. Foi percebida, também, uma paridade entre os aplicativos, porém, com destaque no fator confirmação em duas etapas no WhatsApp, em que a proteção de dados é estendida a todas as interações. Em contrapartida, por ter seu código aberto, o Telegram permite auditoria externa como diferencial.

Sob o olhar semiótico, verificou-se que, referente à segurança, o WhatsApp se destaca por ter recursos imagéticos na explicação de como aplicar a confirmação em duas etapas. Além de um tutorial em formato de texto simplificado, também dispõe de um vídeo com passo a passo. Os dois aplicativos se valem da figura de um cadeado, indicando a aplicação da criptografia de ponta a ponta na proteção das mensagens.

Por fim, ficou nítido que a Inteligência Competitiva estabelece interação com a LGPD e a Semiótica, na clareza das informações direcionadas aos usuários de aplicativos mensageiros, tornando possível medidas necessárias para a proteção de dados.

5.3. Implicações gerenciais

A pesquisa trouxe a temática para o contexto dos aplicativos mensageiros, explorando o WhatsApp e o Telegram. Por meio do conceito da inteligência competitiva, na prática da gestão do conhecimento para a contrainteligência frente a concorrência, foi demonstrado o processo que inicia na coleta de dados, passando pela seleção da informação até chegar ao conhecimento demanda estratégias. Deste processo que é gerado o conhecimento, e sua gestão, utilizado pela inteligência competitiva e contrainteligência. Para isso, o conhecimento deve ser explicitado com clareza, dentro dos preceitos da semiótica, cujo uso de recursos facilite a compreensão de quem o recebe.

Cabe questionar se só a riqueza documental por parte das plataformas é o suficiente para a transmissão da informação. Se através da semiótica não é possível adicionar formas menos

técnicas de gerenciar o conhecimento, existentes nas políticas de privacidade de cada uma, demonstrando aos usuários de forma mais populista os recursos existentes nas políticas de privacidade e a importância de usá-los.

5.4. Limitações da pesquisa e estudos futuros

O presente artigo se limitou à observabilidade das informações dispostas nas telas das plataformas e na análise comparativa, entre os dados disponibilizados via políticas de segurança de cada uma.

Para pesquisas futuras, sugere-se uma análise aprofundada, com o intuito de compreender as disponibilidades das informações. Sugere-se observar os princípios da gestão do conhecimento, dispostos em cada plataforma, na busca pela otimização da redistribuição das informações para alcançar uma vantagem competitiva.

REFERÊNCIAS

ÂNGELO, Kedson. **A História da Criação do WhatsApp.** Artigos Linkedin, 3 de nov., 2006. Disponível em: <https://www.linkedin.com/pulse/hist%25C3%25B3ria-da-cria%25C3%25A7%25C3%25A3o-do-whatsapp-kedson-angelo/?trackingId=0%2Bbm2tYET1SRkwHYJdYOfg%3D%3D>. Acesso em: 19 jun 2023.

ARAMUNI, João Paulo; MAIA, Luiz Cláudio Gomes. **A Influência da Engenharia Semiótica na Experiência de Aplicativos Mobile.** Acta Semiótica et Lingvistica, 2018. p.44-53. Disponível em: <https://periodicos.ufpb.br/index.php/actas/article/view/43701/0>. Acesso em 21 de jun 2023.

AVELINO, R., MACHADO, D, F., (2017) **Big Data, Vigilância e o Mercado de Dados Pessoais na Saúde** https://www.academia.edu/36830813/BIG_DATA_VIGIL%C3%82NCIA_E_O_MERCADO_DE_DADOS_PESSOAIS_NA_SA%C3%9ADE Acesso em 20 de março de 2023.

BARBOSA, Simone Diniz Junqueira; SILVA, Bruno Santana. **Interação Humano-Computador.** Rio de Janeiro: Elsevier, 2010.

BARDIN, Laurence. **Análise de Conteúdo.** Lisboa. Edições 70, 1977.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei Nº 13.709, de 14 de Agosto de 2018. Brasília, 18 março. 2023 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em 02 jul 2023.

CARDOSO-JUNIOR, Walter Felix Cardoso. **Inteligência Competitiva.** 2ª Edição Revista e Atualizada.Palhoça: UNISULVIRTUAL, 2008.

CARVALHO, Dárlinton. Barbosa. Feres de. *et al*. **Um Estudo Sobre a Utilização de Programas com Interface Baseada em Mapas.** Monografias em Ciência da Computação Nº 17/10. Pontifícia Universidade Católica do Rio de Janeiro, 2010. disponível em: <http://bib-di.inf.puc-rio.br/ftp/pub/docs/techreports/10_17_carvalho.pdf>. Acesso em 20 de jun 2023

CORTEZ, Natália Moura *P*. ***Umwelts*** **e Nichos Ecológicos:** Melodias e Comunicabilidade de Interfaces segundo a Engenharia Semiótica. E-xacta. Belo Horizonte: Editora UniBH. v. 5, n. 2, 2012. p. 139-148. Disponível em: <www.unibh.br/revistas/exacta/>. Acesso em: 19 jun 2023.

CUNHA, Yuri Lázaro de Oliveira; SANTOS, Teresa Rachael Rodrigues; CARVALHO, Mateus Espindola. **Impactos da Transformação Digital no Modelo de Negócios**. Congresso Transformação Digital, 2019. Disponível em: <http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2019/paper/viewFile/7341/2123>. acesso em 02 de jun 2023.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr Pinheiro; MARQUES, Rodrigo Moreno Marques. **Termos de Uso e Políticas de Privacidade das Redes Sociais On-Line.** Informação & Informação, Londrina, v. 26, n. 4, out./dez. 2021. p. 550 – 574. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/51720/2/Termos%20de%20uso%20e%20pol%C3%ADticas%20de%20privacidade%20das%20redes%20sociais%20on-line.pdf>. Acesso em 02 de jul 2023.

FORTINET. **Relatório de Cenário de Ameaças Global: Um Relatório Semestral da FortiGuard Labs.** Fevereiro de 2023.Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/pt_br/report-2023-threat-landscape.pdf>. Acesso em 02 jul 2023.

ICT Households. **TIC Domicílios:** Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros/2020. São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em: <https://cgi.br/media/docs/publicacoes/2/20211124201233/tic_domicilios_2020_livro_eletronico.pdf>. Acesso em: 02 jul 2023.

KAMARA, Seny et al. **Olhando de Fora Para Dentro:** Abordagens para a moderação de conteúdo em Sistemas com Criptografia de Ponta a Ponta. Center for Democracy e Technology. Tradução: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: <https://irisbh.com.br/wp-content/uploads/2022/02/Olhando-de-fora-para-dentro-Abordagens-para-a-moderacao-de-conteudo-em-Sistemas-com-Criptografia-de-Ponta-a-Ponta.pdf>. Acesso em 01 de julho de 2023.

MAGALHÃES, Rodrigo Almeida.; OLIVEIRA, Érika Cristina Rodrigues Nardoni. **O Direito à Privacidade na Era Digital.** Revista Jurídica Da FA7**,** *18*(1), 2021. p.55-70. Disponível em: <https://doi.org/10.24067/rjfa7;18.1:1173>. acesso em 19 jun 2023.

MENEZES, Afonso Henrique. Novaes *et al*. **Metodologia Científica**: teoria e aplicação na Educação a Distância. Petrolina: Universidade Federal do Vale do São Francisco. 2019.

RIBEIRO, Anna Carolina Mendonça Lemos; OLIVEIRA-JUNIOR, Almir de. **Inteligência Competitiva**: Revisão Sistemática da Produção Nacional. Perspectivas em Ciência da Informação, v.26, número 3, set., 2021. p. 74-95. Disponível em:

<https://www.scielo.br/j/pci/a/gBM5chKS7QHqRhmQxhLwWqP/?format=pdf&lang=pt>. Acesso em 21 de jun 2023

RODOTÁ, Stefano. **A vida na Sociedade de Vigilância: A Privacidade Hoje**. Org. Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Leonel Cezar; RISCAROLLI, Valéria; ALMEIDA, Martinho Isnard Ribeiro De. **Inteligência Competitiva No Brasil:** Um Panorama do Status e Função Organizacional. São Paulo: Revista Inteligência Competitiva. v. 1, n. 1, abr./jun., 2011. p. 63-85. Disponível em: <https://ric.emnuvens.com.br/rev/article/view/4/13>. Acesso em 19 jun 2023.

SABADIN, Neli Miglioli. **Interação Humano-Computador**. UNIASSELVI, 2016.

SANTAELLA, Lúcia. **O Que é Semiótica**. Volume 103. Coleção Primeiros Passos. São Paulo: Editora Brasilense, 1983.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. (2016). **A Privacidade e o Mercado de Dados Pessoais | Privacy and the Market of Personal Data.** Liinc Em Revista, *12*(2). Disponível em:<https://doi.org/10.18617/liinc.v12i2.902>. Acesso em 01 de jul 2023.

TAKEUCHI, Hirotaka; NONAKA. Ikujiro. **Gestão do Conhecimento.** Porto Alegre: Bookman, 2008.

TELEGRAM. **FAQ**. 2023. Disponível: < https://telegram.org/faq#p-o-que-e-telegram-o-que-faco-aqui>. Acesso em 12 jul 2023.

WHATSAPP LLC. **Sobre o WhatsApp**. Site do WhatsApp, 2023. Disponível em: < https://www.whatsapp.com/about?lang=pt_BR#:~:text=O%20WhatsApp%20foi%20fundado%20por,em%20qualquer%20lugar%20do%20mundo>. Acesso em: 19 jun 2023.