HACKERS EM PAUTA? ABORDAGENS JORNALÍSTICAS DURANTE O PERÍODO DE ATAQUE CIBERNÉTICO

HACKERS IN THE NEWS? JOURNALISTIC APPROACHES DURING THE CYBER ATTACK PERIOD

¿HACKERS EN LA AGENDA? ENFOQUES PERIODÍSTICOS DURANTE EL PERÍODO DE ATAQUE CIBERNÉTICO

Fernanda Shelda de Andrade Melo[1]

Resumo

Os ataques cibernéticos, também conhecidos como ataques *hackers*, são ameaças iminentes no contexto digital. Todavia, o tema continua centralizado em estudos específicos da computação e pouco abordado em uma lente comunicacional. Defendemos especialmente que o processo informativo pode ajudar na minimização de vulnerabilidades dos sujeitos durante as invasões. Por isso, neste trabalho, trazemos o objetivo de analisar as principais lógicas aplicadas nas coberturas jornalísticas durante o período de ataque cibernético, considerando o caso das Lojas Americanas em 2022. Os principais resultados apontam que os veículos focam na preocupação com os prejuízos monetários e nas afetações das organizações, com poucas investigações que considerem vulnerabilidades dos cidadãos acerca do caso.

Palavras-chave: ataques cibernéticos; hackers; jornalismo; vulnerabilidades; públicos.

Abstract

Cyberattacks, also known as hacker attacks, are imminent threats in the digital context. However, the topic remains centered on specific computer studies and is rarely addressed from a communication perspective. We specifically argue that the information process can help minimize citizens' vulnerabilities during invasions. Therefore, in this work, we aim to analyze the main logic applied in journalistic coverage during the period of cyberattacks, considering the case of Lojas Americanas in 2022. The main results indicate that the media outlets focus on the concern with monetary losses and the impact on organizations, with few investigations considering citizens' vulnerabilities regarding the case.

Keywords: cyber attacks; hackers; journalism; vulnerabilities; publics.

Resumen

Los ataques cibernéticos, también conocidos como ataques de *hackers*, son amenazas inminentes en el contexto digital. Sin embargo, el tema sigue centrado en estudios específicos de la computación y poco abordado en una lente comunicacional. Defiende especialmente que el proceso informativo puede ayudar en la minimización de vulnerabilidades de los sujetos durante las invasiones. Por eso, en ese trabajo, se trae el objetivo de analizar las principales lógicas aplicadas en las coberturas periodísticas durante el período de ataque cibernético, considerando el caso de las tiendas americanas en 2022. Los principales resultados indican que los vehículos se centran en la preocupación por los daños monetarios y las afectaciones de las organizaciones, con pocas investigaciones que consideren vulnerabilidades de los ciudadanos sobre el caso.

Palabras clave: ataques cibernéticos; *hackers*; periodismo; vulnerabilidades; públicos.

[1] Doutoranda em Comunicação Social pelo Programa de Pós-Graduação da Universidade Federal de Minas Gerais (UFMG). Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes). E-mail: fernandashelda@ufmg.br.

DOI: https://doi.org/10.21882/ruc.v12i20.986

1 Introdução

Em uma lógica rotineira que nos leva ao uso diário de *smartphones* e computadores, os registros por meio de dados são cada vez mais utilizados já que contém todos os passos *online*, desde simples curtidas até informações importantes sobre saúde – cenário este que é chamado de ambiente datificado por teóricos que abordam a interação de plataformas digitais com o cenário social (Dijck, 2014). Entendê-los dessa forma não significa ceder poder total aos dados sob a vida humana, mas verificá-los enquanto agentes potenciais de infraestruturas que coordenam ações diárias é indispensável para verificar vulnerabilidades dos públicos (D'Andrea, 2020; Marres, 2007).

Uma ameaça que cerca esse contexto e vem se tornando perigosa em disputas no ciberespaço, uma vez que atinge não só indivíduos específicos, mas também grandes organizações – sejam estas privados ou governamentais – são os ataques cibernéticos, também conhecidos popularmente como ataques *hackers*. De acordo com uma pesquisa da Check Point, compartilhada pelo portal IT Forum (2024), o Brasil registrou aumento de 67% no número de ataques cibernéticos, totalizando 2.754 invasões às organizações nacionais por semana somente em 2024. Essa realidade ainda é abordada na academia de forma tímida, especialmente por autores que procuram enfatizar lógicas de criminalidade para os *hackers* ou em setores específicos da computação, ao trabalharem com demandas de segurança cibernética (Greenberg, 2021; Schneier, 2020).

Nesta pesquisa, verificamos a necessidade de aplicar uma lente comunicacional para o tema. Dada a dimensão desses acontecimentos, podemos enxergá-los enquanto um campo de disputas de sentido, sendo possível afirmar que a comunicação também está imbricada nessas ações. No caso deste trabalho, abordamos principalmente as características presentes durante o processo de repasse de informações para a população, que pode objetivar a diminuição de boatos e incertezas sobre os casos. Essa busca procura contribuir com a forma que olhamos para esse acontecimento, considerando que as estratégias comunicacionais podem demonstrar cenários ainda desconhecidos. Além disso, mostra-se relevante ao unir conceitos que, até então, continuam afastados da comunicação e podem ser integrados em perspectivas inéditas.

Nesse sentido, entendemos que diversas vulnerabilidades dos públicos podem ser contornadas durante o processo de acesso à informação. Um simples exemplo é que no caso de um ataque cibernético direcionado à uma instituição financeira, a informação levada aos usuários daquela plataforma pode atentar que os serviços do banco estão comprometidos, incluindo sua própria segurança ao realizar transações. Isso significa que comunicar esse acontecimento é indispensável para a minimização de mais estragos durante a atuação dos invasores.

O formato mais utilizado para considerar esse tipo de repasse informativo é a imprensa. Logo, é preciso entender como essa esfera vem lidando com esses casos, considerando que sua abordagem pode modular a recepção desse tipo de conteúdo, além de verificar se ele está sendo trabalhado de forma especializada ou não. Por isso, o presente artigo traz como objetivo analisar as principais lógicas aplicadas nas coberturas jornalísticas durante o período de ataque cibernético, considerando o caso das Lojas Americanas[2]. O objeto empírico escolhido para a análise desse trabalho está centrado em um caso real que impactou uma das maiores organizações privadas do país.

Para tanto, iniciamos o artigo entendendo um pouco mais sobre o que são ataques cibernéticos, também conhecidos como ataques *hackers*, buscando acionar teorias indispensáveis para essa discussão (Araujo; Rossi, 2020; Silva, 2019; Evangelista, 2018). Em seguida, discutimos a necessidade de informar esse acontecimento e como isso pode ajudar a contornar as vulnerabilidades dos públicos, problematizando as assimetrias de poder, encarando essa temática em uma lente pragmatista da comunicação (Henriques; Silva, 2014; Dewey, 1954). Por fim, aplicamos uma metodologia exploratória para investigar o caso escolhido com resultados iniciais que apontam para a preferência por notícias ao invés de reportagens, com focos centrados em setores econômicos e abordagem de prejuízos financeiros da empresa e pouca observação de afetações aos sujeitos

2 Por que precisamos estudar ataques cibernéticos?

À priori, concentraremos nossos esforços em explicar o que são ataques cibernéticos. Nesse sentido, precisamos resgatar teorias da área computacional, entendendo que os estudos sobre esse tipo de invasão surgem de pesquisas envolvendo o arcabouço teórico de Tecnologia da Informação (TI). Em primeiro lugar, é preciso entender que um ataque cibernético nada mais é que uma invasão de um sistema, podendo afetar diversas estruturas a depender de seu objetivo (Gomes; Cordeiro; Pinheiro, 2016).

Para além disso, a categorização desses ataques possui diversas variáveis. Por exemplo, Araujo e Rossi (2020) enfatizam que os *malwares* – arquivos contaminados – podem ser espalhados de múltiplas formas com duas atuações principais: *Distributed Denial of Service* (DDoS) e *ransomware*. No primeiro caso, há uma tentativa de atacar a continuidade dos serviços, fazendo com que sites e aplicações fiquem travados. Isso pode ser direcionado a gerar danos à imagem de organizações, especialmente em momentos cruciais para estas, como o enfrentamento de outras crises. Um exemplo está no ataque de DDoS sofrido pelos Órgãos

[2] O ataque que atingiu as Lojas Americanas ocorreu em 2022, com uma nova tentativa de invasão em 2024. Os sistemas foram paralisados e o aplicativo comercial ficou inacessível por cerca de três dias.

estaduais de Roraima, em que 30 sites foram alvos de instabilidades no sistema e na pausa do funcionamento de serviços em janeiro de 2024[3]. Por vezes, esses prejuízos também são direcionados a figuras políticas, gerando desgastes à sua credibilidade enquanto governantes, por isso podem possuir maior foco em organizações públicas.

Em seguida, o *ransomware* tem um conteúdo mais profundo e seus danos também são mais graves. Em resumo, esse tipo de ataque pode ser considerado uma espécie de sequestro dos dados e pode ter influência até mesmo em guerras políticas, como discutido por Greenberg (2021) nas disputas entre a Rússia e a Ucrânia. O autor também demonstra a utilização dessa categoria de invasão para roubar dados do país oposto; bem como a intenção de extorquir valores monetários de indivíduos ou empresas. Essa classificação de ataque acontece muito no Brasil, como no caso das Lojas Renner que admitiu ter sofrido um ataque de *ransomware* em 2021, tendo dados roubados pelos criminosos que exigiram 20 milhões de dólares para retorno dessas informações[4].

É claro que essas invasões, independentemente de seu tipo, podem ser contornadas. Uma das primeiras medidas é a própria criptografia, assim, mesmo que os *hackers* consigam acesso aos dados, eles precisarão dedicar um tempo maior para descriptografá-los e, às vezes, podem nem obter sucesso nessa jornada (Silva, 2019). Em outra medida, o *backup* dessas informações também pode ajudar as empresas que enfrentam essa dinâmica, já que como explicado no exemplo anterior, esse tipo de invasão quando não obtém sucesso pelo resgate cobrado pode levar embora documentos que são cruciais e muito importantes para a organização.

Fato é que a figura central desses ataques, comumente chamada de *hacker*, também está posicionada em uma questão polêmica. Em primeiro lugar, o próprio termo *hacker* – bastante utilizado no linguajar informal para se referir aos ataques – é criticado na academia por diferentes vieses. Em um deles, Lemos, Seara e Pérsio (2002) explicam que *hacker* não necessariamente é uma figura que atua para danificar sistemas e que esse indivíduo, na verdade, seria um *cracker*. Para os autores: "a diferença entre um *hacker* e um *cracker* são cruciais. Um *cracker* é uma pessoa que invade e 'danifica' sistemas, causando danos pelo simples prazer de fazê-lo. Um *hacker* digamos, é um *cracker light*. Ele somente mostra que esteve ali" (Lemos; Seara; Pérsio, 2002, p. 30).

Enquanto isso, Malaguti (2022) afirma que a tipologia adotada na mídia e na sociedade pode afetar a criminalização dessas ações, já que *hacker* é um termo muito variável. Pensando nisso, optamos por utilizar o termo ataque cibernético para especificar a ação na maior parte das abordagens, porém, não deixamos de problematizar que esse tipo de debate, por vezes, pode

[3] Governo teria sofrido tentativa de ataque de mesmo hacker que invadiu sites de universidades em Roraima. Folha BV, 17 de janeiro de 2024. Disponível em: https://www.folhabv.com.br/politica/governo-sofre-ataque-de-mesmo-hacker-que-invadiu-sites-de-universidades-em-roraima/. Acesso em 18 setembro 2024.

[4] Após ataque hacker, Renner nega que pagou US$ 20 milhões aos criminosos. Revista Exame, 2021. Disponível em: https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/. Acesso em 18 setembro 2024.

estar centrado na academia e não atingir o ambiente social, em que os termos mais "fáceis" e "simples" já estão no linguajar popular.

Em seguida, problematizamos também a ideia utilizada no imaginário social sobre os *hackers* que, geralmente, é atravessada por uma dualidade do bem e do mal: poderia então um *hacker* ser bonzinho, enquanto o *cracker* é o que atua para o mal? Entendemos que outras perspectivas atingem a comunidade *hacker*, como é o caso do hackerativismo. Evangelista (2018) retoma os exemplos em que os *hackers* invadem sistemas para democratizar o acesso à leitura ou disponibilizar materiais culturais para acesso geral, por exemplo. Nestes casos, torna-se ainda mais difícil separar a figura do invasor do que é bom e o que é ruim – já que a situação possui um contraste importante, o cometimento de crimes cibernéticos para disponibilização de acesso livre.

Além disso, *hackers* também são contratados no mercado para trabalhar justamente com segurança cibernética no cenário atual de TI. Isso porque, essas invasões podem ser feitas em grandes empresas a nível de teste – entendendo quais falhas de segurança podem ser corrigidas caso o sistema permita uma invasão simulada. Nesse sentido, é preciso tomar cuidado com o que se enxerga enquanto ataque e quem é a figura central desse movimento.

Os exemplos citados demonstram que as disputas de sentido que envolvem esses casos – como na situação discursiva que perpassa a própria nomeação do acontecimento, além do seu risco iminente para qualquer indivíduo com acesso à internet, uma vez que empresas enormes também já foram alvos como a Microsoft (Walters, 2014), é uma realidade cada vez mais preocupante. Assim, entendemos que outras áreas, além das computacionais, podem e devem estudar os ataques cibernéticos mais de perto, compreendendo seus possíveis danos e afetações em estruturas sociais. Neste artigo, procuramos entender tais casos em uma lente comunicacional, abordando na próxima seção como a dinâmica informacional pode ser uma aliada neste contexto.

3 Informação e minimização de vulnerabilidades

Entendendo a gravidade desses ataques, é possível enxergar diversas classificações de vulnerabilidades que podem cercar os públicos neste momento. Quando direcionamos a ideia de que grandes invasões são voltadas às organizações privadas e governamentais, não podemos esquecer que estas lidam diretamente com dados de sujeitos. No caso da esfera pública, por exemplo, há um recorte de *backups* de Registros Gerais (RGs) e Cadastros de Pessoas Físicas (CPFs) de todos os cidadãos do país, incluindo a documentação para continuidade de projetos de políticas públicas e auxílios sociais. Enquanto isso, os públicos também estão incluídos na prestação de serviços de empresas privadas, como é o caso do setor comercial que pode coletar dados sensíveis e informações financeiras, como registros de cartões de crédito.

Para além disso, alguns outros danos são ainda mais severos. Greenberg (2021), ao retomar o maior ataque cibernético do planeta conhecido como Sandworm, retoma exemplos ao redor da história das invasões online. Em um desses casos, um vírus que foi batizado de *WannaCry*[5] atingiu serviços prestados em hospitais do Reino Unido, fazendo com que consultas e cirurgias fossem desmarcadas. Ademais, os ataques também podem ter danos físicos que ultrapassam o mundo virtual, como no caso do corte de energia e da aceleração de máquinas a ponto até de elas poderem vir a implodir.

Com isso posto, verificamos que a ideia de "saber o que está acontecendo" é fundamental para se proteger em tais momentos. Desde os estudos pragmatistas da comunicação, Dewey (1954) defendia que o público funcionava em duas medidas: o sofrer e o agir. Em primeiro lugar, era preciso entender que estava sendo afetado para, em seguida, reagir. Entretanto, o que o autor pontuava desde aquela época era uma preocupação crescente com o que ele chamou de eclipse dos públicos, quando os sujeitos não conseguem saber o que lhes afeta por diversos motivos, um deles quando a informação não é compartilhada de forma a deixá-los no escuro.

Em outra medida, consideramos fundamental entender que a desinformação e, nesse caso, não estamos lidando exatamente com a ideia de informações falsas, mas sim com a ideia de que alguns conteúdos podem propagar ainda mais dúvidas sobre os casos como os boatos, além da própria falta de informação – é um tipo de assimetria de poder. Isso significa que ela pode ser usada para esconder a real situação em contextos específicos, uma estratégia utilizada principalmente por organizações privadas para que o acontecimento não gere danos à sua imagem enquanto empresa. Esse entendimento também é utilizado na área da saúde, em que a falta de informações afeta o preparo para promoção da saúde, indo além do que é entendido enquanto desinformação apenas na esfera de *fake news* (Dornelas; Giannini; Ferreira, 2015).

Esse fenômeno não é somente comunicacional, mas tem um profundo caráter político, especialmente porque deixar os públicos no eclipse utilizando desta assimetria de poder pode resultar em dificuldades para que a sociedade faça as cobranças corretas (Cotrim Junior; Silva; Cotrim, 2022). Por exemplo, citamos anteriormente o caso do ataque cibernético às Lojas Renner. Após dias de silêncio sobre os sistemas fora do ar, a empresa foi acionada pelo Procon para dar esclarecimentos sobre o caso[6]. Essa cobrança em peso também veio da imprensa, figurando uma pressão para que os sujeitos possam cobrar por seus direitos corretamente. Se os

[5] O nome foi colocado pelos próprios criadores do vírus, fazendo um jogo de palavras – uma vez que o termo pode significar "Quer chorar?" em inglês. Uma frase comumente usada ao se referir sobre afetações a outras pessoas.

[6] Procon-SP notifica Lojas Renner sobre ataque cibernético. Procon São Paulo, 2021. Disponível em: https://www.procon.sp.gov.br/procon-sp-notifica-lojas-renner-sobre-ataque-cibernetico/. Acesso em 18 setembro 2024.

públicos não soubessem que um ataque aconteceu, como foi feito ou se suas informações podem ter sido roubadas, não há sequer uma possibilidade de que cobrem por demandas de segurança.

É fato que tanto nesse exemplo, como em outros casos, a imprensa pode funcionar em uma metáfora de *watch-dog*, o cão de guarda, como defendido por autores que estudam vulnerabilidades dos públicos. Isso porque, os veículos jornalísticos podem constituir um corpo sólido de denúncia, unindo sua credibilidade e visibilidade – além de quesitos monetários como infraestrutura e profissionais qualificados – para relatar tais acontecimentos (Henriques; Silva, 2014). Acontece que alguns entraves são enfrentados nesse panorama. Antes de mais nada, a associação do jornalismo com a lógica empresarial pode constituir interesses privados que afastem a tentativa de investigações com caráter mais escandaloso, principalmente quando se referem às grandes empresas associadas (Moraes, 2021).

Em seguida, os próprios cortes nas esferas jornalísticas – como *layoff* de profissionais, corte de gastos e afins – podem prejudicar investigações mais profundas. Essa condição também aproxima uma busca incessante por cliques, o que acaba dando preferência à escolha editorial por notícias ao invés de reportagens. Para Lage, a diferença está na estrutura narrativa, uma vez que a notícia trata os fatos de forma mais crua e expositiva. Enquanto isso, a reportagem adiciona técnicas mais subjetivas na narrativa apresentada, tentando explicar os fenômenos mais a fundo (Lage, 1993).

Dessa forma, apesar de ser um caminho indispensável para denunciar condutas que prejudiquem os públicos nestes contextos, além de possibilitar o acompanhamento cada caso de forma mais próxima, os desafios que perpassam a produção atual do jornalismo podem ser entraves problemáticos na tentativa de minimizar vulnerabilidades por meio da informação. Nesta pesquisa, acreditamos que visualizar como essa produção vem sendo feita, especificamente nos casos de ataques cibernéticos, é fundamental para contrastar como esse debate vem sendo efetivado na prática. Por isso, na próxima seção, abordamos um caso real de forma exploratória.

4 Fase analítica

Em fevereiro de 2022, quem tentava acessar o site e os serviços oferecidos pelas Lojas Americanas se deparava com uma falha no sistema. O caso começou a ser comentado nas redes sociais, principalmente porque, na época, a empresa era uma das principais patrocinadoras da 22ª edição do Big Brother Brasil e as instabilidades começaram a ocorrer justamente no período em que o *reality show* produzia mais um evento mediado pela empresa. A organização

continuou com os serviços fora do ar por cerca de três dias, até que os sistemas fossem gradativamente retomados.

Um fato curioso é que dois anos depois, em 2024, as Lojas Americanas foram alvo, mais uma vez, de um novo ataque. Neste trabalho, porém, selecionamos o primeiro caso por dois motivos: em primeiro lugar, o segundo ataque foi mais rápido e aparentemente mais superficial que o primeiro. Uma outra questão é que com o início das discussões relacionadas às fraudes fiscais da empresa, ex-executivos admitiram que utilizariam deste exemplo de ataque cibernético para justificar os rombos financeiros que estavam acontecendo na organização[7]. Dessa forma, entendemos que o primeiro caso poderia fornecer informações mais voltadas para o ataque cibernético que o segundo, já que este foi permeado de disputas de sentido envolvendo polêmicas da empresa – reflexo que seria encontrado nas publicações jornalísticas da época.

Selecionamos como método de pesquisa uma vertente exploratória, iniciando a investigação a partir de uma aba anônima do Google, na tentativa de burlar possíveis algoritmos de indicação no caso da utilização de perfis específicos. Realizamos uma pesquisa com os seguintes termos: "lojas americanas"; "ataque cibernético" e "*hacker*", justificando essa busca pelas discussões primárias neste artigo, que verificaram o uso de ambos os termos para se referir a estes casos. Filtramos, também, o prazo de publicações. As primeiras publicações sobre o ataque iniciam no dia 19 de fevereiro, com o pico de publicações até o dia 23, quando o sistema já havia retornado. Para tanto, concentramos nossos esforços na análise de publicações apenas no mês de fevereiro.

Aplicamos lógicas de navegação exploratória, excluindo publicações jornalísticas que citassem os termos envolvidos, mas não necessariamente o caso abordado. Após o filtro, o resultado foi de 17 publicações. Após isso, iniciamos uma análise mais cuidadosa das matérias, verificando artifícios como as abordagens mais comuns, os temas mais comentados sobre o caso e, também, os veículos que mais aparecem – destacando de forma discursiva nesta etapa os casos que mais se destacaram sobre o tema. Lembramos que o trabalho não possui a intenção de trazer uma abordagem quantitativa, por isso, a análise flutuante foi suficiente para entender qualitativamente as publicações alcançadas.

A primeira menção ao ataque ocorre no portal Poder360[8], indicando que o site das Americanas e sua subsidiária Submarino teriam sofrido ataque e saído do ar. A notícia é

[7] Ex-executivos da Americanas cogitaram até ataque hacker para escamotear rombo de R$ 25 bi, diz MPF. Estadão, 2024. Disponível em: https://www.estadao.com.br/politica/blog-do-fausto-macedo/ex-executivos-da-americanas-cogitaram-ate-ataque-hacker-para-escamotear-rombo-de-r-25-bi-diz-mpf/. Acesso em 18 setembro 2024.

[8] Submarino e Americanas sofrem ataque hacker e saem do ar. Poder360, 2022. Disponível em: https://www.poder360.com.br/poder-tech/tecnologia/submarino-e-americanas-sofrem-ataque-hacker-e-saem-do-ar/. Acesso em 18 setembro 2024.

previamente simplória, com um conteúdo de atualização sobre o caso. Um ponto importante é que a primeira matéria foi alocada no setor de tecnologia. As publicações que seguem essa prática são semelhantes, com informações mais iniciais sobre o ataque e sugerindo possíveis responsáveis, como é o caso de *hackers* "famosos" no país.

É importante mencionar que durante este primeiro período, a assessoria das lojas Americanas divulgou que ainda não se manifestaria sobre o caso, justificando que os colaboradores estavam focados em resolver o problema. Durante à noite, a Revista Oeste lança uma matéria[9] mais descritiva, publicando como a instabilidade começou e comparando a invasão com outros ataques cibernéticos recentes. Neste momento, a revista também caracteriza a publicação na pasta tecnologia.

É então no dia seguinte que o assunto começa a surgir em veículos maiores, como é o caso do G1[10]. A publicação também segue uma lógica semelhante à da Revista Oeste, procurando explicar o que é um ataque *hacker*, como ele acontece e as tentativas falhas da empresa de retornar os serviços ao ar. O que verificamos em seguida são abordagens divergentes que começam a surgir na imprensa. É aí que aparece o portal Mercado & Consumo, destacando possíveis afetações econômicas do caso e da própria Folha de S. Paulo que setoriza a matéria na seção econômica e destaca a manchete[11]: "Americanas perde mais de R$100 milhões por dia com ataque *hacker*", dando ênfase às perdas monetárias. Logo em seguida, destacamos um levantamento feito pelo portal NeoFeed[12]. Nele, o texto discute a perda monetária por dias que estão deixando de vender.

Enquanto isso, a CNN Brasil traz uma reportagem, também setorizada na pasta econômica, com um especialista que procura afirmar que o ataque afeta diversas dimensões organizacionais da empresa, como é o caso do setor financeiro e da própria imagem e credibilidade[13]. Até o momento, verificamos que todas as publicações são voltadas para

[9] Hackers atacam sites das lojas do Submarino e Americanas. Revista Oeste, 2022. Disponível em: https://revistaoeste.com/tecnologia/hackers-atacam-sites-das-lojas-do-submarino-e-americanas/. Acesso em 18 setembro 2024.

[10] Americanas e Submarino voltam a tirar sites do ar após suspeita de ataque hacker. G1, 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/02/20/americanas-e-submarino-tiram-sites-do-ar-apos-identificarem-acesso-nao-autorizado.ghtml. Acesso em 18 setembro 2024.

[11] Americanas perde mais de R$100 milhões por dia com ataque hacker. Folha de S. Paulo, 2022. Disponível em: https://www1.folha.uol.com.br/mercado/2022/02/americanas-perde-mais-de-r-100-milhoes-por-dia-com-ataque-hacker.shtml. Acesso em 18 setembro 2024.

[12] Com sites fora do ar, Americanas deixa de vender cerca de R$ 100 milhões por dia. NeoFeed, 2022. Disponível em: https://neofeed.com.br/blog/home/com-sites-fora-do-ar-americanas-deixar-de-vender-cerca-de-r-100-milhoes-por-dia/. Acesso em 18 setembro 2024.

[13] Queda de sites traz danos financeiros e de imagem às Americanas, dizem analistas. CNN Brasil, 2022. Disponível em: https://www.cnnbrasil.com.br/economia/investimentos/queda-de-sites-traz-danos-financeiros-e-de-imagem-a-americanas-dizem-analistas/. Acesso em 18 setembro 2024.

entender as dinâmicas empresariais e qual seria o futuro das Lojas Americanas, em uma espécie de padrão (Figura 1).

Figura 1: publicação da CNN Brasil, evocando a estrutura padronizada

Fonte: Captura de tela realizada a partir do portal CNN Brasil. Disponível em: https://www.cnnbrasil.com.br/economia/investimentos/queda-de-sites-traz-danos-financeiros-e-de-imagem-a-americanas-dizem-analistas/. Acesso em: 07 novembro 2024.

Assim, é apenas com uma publicação do portal InfoMoney, de forma inédita, que finalmente verificamos uma vertente diferente, um olhar mais voltado para os públicos. Isso porque, a notícia traz como manchete a notificação que o Procon faz para que as Lojas Americanas forneçam explicações sobre o caso, especialmente se o ataque poderia afetar algum cliente ou dados dos consumidores. Mesmo assim, a matéria[14] continua sendo classificada no setor econômico.

No prazo de dois e três dias após o ataque, o coro sobre o prejuízo empresarial continua. Esse é o caso da CNN Brasil que evoca[15] o mesmo tema com uma classificação específica na pasta "Investimentos"; também do portal Mais Retorno que retoma a queda de ações da empresa

[14] Procon-SP notifica Americanas e Submarino por derrubada de sites após suposto ataque hacker. InfoMoney, 2022. Disponível em: https://www.infomoney.com.br/minhas-financas/procon-sp-notifica-americanas-e-submarino-por-derrubada-de-sites-apos-suposto-ataque-hacker/. Acesso em 18 setembro 2024.

[15] Americanas perde mais de R$ 2 bilhões em valor de mercado com sites fora do ar. CNN Brasil, 2022. Disponível em: https://www.cnnbrasil.com.br/economia/investimentos/americanas-perde-mais-de-r-2-bilhoes-em-valor-de-mercado-com-sites-fora-do-ar/. Acesso em 18 setembro 2024.

após divulgação do ataque[16]; da Revista Exame[17] que enseja que o prejuízo poderia ultrapassar mais de R$325 milhões, no setor "Negócios"; e, também, da Forbes Brasil[18], dessa vez na pasta chamada de "Money" – principal pauta das publicações.

Finalmente, no dia 23 de fevereiro, as matérias voltam o foco para o retorno da loja, dessa vez, sem categorizações em pastas específicas – apenas com demandas noticiosas mais superficiais, como é o caso do Poder360[19], da Forbes[20] e do Meio & Mensagem[21]. Nos três casos, porém, a menção da perda monetária ainda existe, mesmo que de forma simbólica.

Como finalização do caso, destacamos O Globo[22], sendo o primeiro a mencionar que a comunicação em relação aos possíveis prejuízos ao consumidor era fundamental, citando inclusive a Agência Nacional de Proteção de Dados (ANPD). Apesar desse passo, a separação editorial continua centrada na esfera econômica, bem como as menções de prejuízo financeiro no título. Por fim, resgates do caso são feitos no final do mês com o resumo do acontecimento e a indicação de prevenção para futuras invasões semelhantes, como matéria sugestiva do Meio & Mensagem[23].

5 Resultados

Alguns pontos que apareceram na fase analítica são indispensáveis para destacar a discussão presente neste artigo. Sabemos que há uma evidente limitação em lidar com todas as abordagens feitas, principalmente porque neste trabalho analisamos matérias publicadas *online* e, dessa forma, há um destaque evidente para meios que se repetem nesta estrutura. Enquanto

16 Americanas perde R$ 3,5 bi em valor de mercado, em dois pregões, após ataque hacker. Mais Retorno, 2022. Disponível em: https://maisretorno.com/portal/americanas-perdeu-r-35-bi-em-valor-de-mercado-em-dois-pregoes-apos-ataque-hacker. Acesso em 18 setembro 2024.

17 72h fora do ar: Prejuízo da Americanas pode ultrapassar R$ 325 milhões. Exame, 2022. Disponível em: https://exame.com/negocios/72h-fora-do-ar-prejuizo-da-americanas-pode-ultrapassar-r-325-milhoes/. Acesso em 18 setembro 2024.

18 Americanas perde mais de R$ 2 bilhões em valor de mercado com sites fora do ar. Forbes, 2022. Disponível em: https://forbes.com.br/forbes-money/2022/02/americanas-perde-mais-de-r-2-bilhoes-em-valor-de-mercado-com-sites-fora-do-ar/. Acesso em 18 setembro 2024.

19 Americanas restabelece sites depois de 3 dias fora do ar. Poder360, 2022. Disponível em: https://www.poder360.com.br/brasil/americanas-restabelece-sites-depois-de-3-dias-fora-do-ar/. Acesso em 18 setembro 2024.

20 Americanas.com volta a funcionar parcialmente após três dias fora do ar. Forbes, 2022. Disponível em: https://forbes.com.br/sem-categoria/2022/02/americanas-com-volta-a-funcionar-parcialmente-apos-tres-dias-fora-do-ar/. Acesso em 18 setembro 2024.

21 Após dias fora do ar, Americanas restabelece e-commerce. Meio & Mensagem, 2022. Disponível em: https://www.meioemensagem.com.br/marketing/apos-dias-fora-do-ar-americanas-restabelece-e-commerce. Acesso em 18 setembro 2024.

22 Americanas: Com suspensão das vendas on-line, empresa já perdeu quase R$ 3,5 bi em valor de mercado. O Globo, 2022. Disponível em: https://oglobo.globo.com/economia/negocios/americanas-com-suspensao-das-vendas-on-line-empresa-ja-perdeu-quase-35-bi-em-valor-de-mercado-25405818. Acesso em 18 setembro 2024.

23 Caso Americanas: como os marketplaces podem prevenir ataques. Meio & Mensagem, 2022. Disponível em: https://www.meioemensagem.com.br/marketing/caso-americanas-como-as-redes-podem-prevenir-ataques. Acesso em 18 setembro 2024.

isso, a esfera que trata do caso no telejornalismo ou no jornalismo de revista pode abordar táticas diferentes sobre a invasão, que neste momento é observada em um ambiente específico do digital, tratando também de uma temática de tecnologia.

Uma condição que apareceu de forma constante nesta pesquisa foi o fato de os veículos sempre conduzirem as matérias relacionadas ao ataque cibernético para as pastas econômicas, com evidente inquietação de afetação monetária. Isso significa que o destaque do prejuízo financeiro para o acontecimento estava muito mais centrado em como isso afetaria a organização e, consequentemente, seus reflexos na bolsa de valores e outras demandas econômicas nacionais, uma vez que se trata de uma grande empresa brasileira.

Se pontuamos no início deste trabalho a esperança de as notícias estarem centradas em um modelo especializado voltado para o ambiente datificado, há uma clara reversão dessa ideia como comentado anteriormente. Apenas alguns portais que cuidaram da pauta em seu início, como é o caso da primeira publicação no Poder360, trazem a notícia para a pasta tecnológica, e – considerando que as invasões fazem parte de uma lógica digital – entendemos a presença dessas notícias neste setor específico. No entanto, a forte separação em um quesito econômico exibe uma aproximação do jornalismo empresarial. Isso nos mostra que a preocupação com os sujeitos ficou em segundo plano, evidentemente esquecida ou propositalmente ignorada. Nas únicas duas publicações em que há uma breve menção sobre as vulnerabilidades dos públicos nesse acontecimento, ainda há a continuidade da estratégia de setorização das matérias em uma pasta de economia.

Para além disso, a escolha por constantes modelos de notícia, sem grandes preferências pela estrutura de reportagem, também nos exibe uma baixa apreensão com a invasão, perpassando uma sensação de que é algo rapidamente resolvível e pouco alarmante para os clientes. Isso também é refletido nas explicações superficiais sobre o caso, uma vez que pessoas leigas na temática pouco se aprofundam sobre possíveis cobranças ou danos, quando há somente uma ênfase no acontecimento de forma superficial e pouca preocupação narrativa em explicar as camadas que envolvem um ataque cibernético.

O que a pesquisa empírica parece evocar é um modelo semelhante ao discutido anteriormente. A dinâmica de necessidade por cliques deixa de lado um trabalho mais cuidadoso e investigativo nos portais digitais em relação ao acontecimento e claramente dá pouca ênfase aos possíveis danos aos clientes, sendo a empresa o único pilar preocupante deste contexto. Não há, por exemplo, nenhum tipo de cobrança pelo posicionamento da organização para relatar essa preocupação com os sujeitos. Na verdade, citamos que um dia após o caso, a publicação evoca o discurso da assessoria da empresa de que ela ainda não se posicionaria.

Por último, um destaque importante está na utilização do termo *hacker*. Discutimos na primeira fase teórica a problematização feita em torno dessa nomeação, especialmente na dualidade do bem e do mal – considerando que a atuação *hacker* pode ir muito além disso. Entretanto, o debate acadêmico não parece alcançar a realidade social, refletida nas matérias analisadas. Em todas elas, sem exceção, há a menção ao termo *hacker* como agente principal da invasão. Neste sentido, é indispensável refletir se as argumentações acadêmicas podem alcançar a prática e, consequentemente, saírem do âmbito exclusivamente teórico.

6 Considerações finais

O presente artigo trouxe como objetivo analisar as principais lógicas aplicadas nas coberturas jornalísticas durante o período de ataque cibernético, considerando o caso das Lojas Americanas. Dessa forma, observou as principais teorias voltadas para a explicação das invasões *hackers*, além de discutir como o processo informacional pode ajudar na minimização de vulnerabilidades dos sujeitos em momentos críticos como nos casos exemplificados anteriormente.

Aplicamos também uma pesquisa empírica que buscou analisar qualitativamente em uma navegação flutuante as matérias publicadas durante o mês de fevereiro de 2022, período em que as Lojas Americanas sofreram um ataque cibernético. Notamos que há um cenário aflitivo na abordagem jornalística em relação às invasões, considerando que em apenas duas matérias há uma breve citação às vulnerabilidades dos públicos. Para além disso, a setorização focada na perspectiva econômica ainda preocupa em relação aos objetivos e aos interesses privados que podem estar por trás dessas publicações, uma vez que apenas a perda monetária das Lojas Americanas é abordada, com pouca responsabilização para o ataque e muito destaque à possibilidade (ou impossibilidade) de recuperação econômica da empresa.

Além disso, as menções que evidenciam o uso recorrente do termo *hacker* exibem um cenário divergente daquele discutido na academia. É interessante entender que o uso no jornalismo pode surgir justamente da utilização social da palavra que é comumente relacionada aos ataques cibernéticos. Nesse sentido, vale considerar que, frequentemente, os debates acadêmicos não alcançam a realidade dos cidadãos ou, até mesmo, a realidade da produção jornalística. Considerar se isso é um ponto positivo ou negativo acerca desse tema é uma possibilidade para futuros estudos.

Em segundo plano, é evidente que este trabalho possui limitações à medida que foca na análise de publicações em portais *online*. Isso significa que tentamos abrir espaço para pesquisas que relacionem à prática jornalística com a temática dos ataques cibernéticos, tão

atual e relevante para a sociedade contemporânea. Assim, pesquisas futuras podem abordar diferentes plataformas, além de considerar casos ainda maiores de invasão que podem demonstrar resultados complementares.

Compreendemos que a junção dessas temáticas é indispensável para entender o cenário informativo quanto aos ataques cibernéticos no Brasil. Nesse sentido, procuramos contribuir com o campo comunicacional ao observar características jornalísticas imbricadas em um acontecimento que é centralizado em demandas de segurança cibernética. Esse deslocamento pode ajudar na abertura de novas discussões sobre a atuação da comunicação nesta esfera.

Referências

ARAUJO, F.; ROSSI, J. **A evolução dos ataques cibernéticos**. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Segurança da Informação) — Faculdade de Tecnologia de Americana "Miniostro Ralph Biasi", Americana, 2020. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/5272. Acesso em: 18 set. 2024.

COTRIM JUNIOR, D.; SILVA, J.; COTRIM, A. Fake News como estrutura de poder: uma questão de assimetria de poder e desigualdade. **Informação em Saúde**, Rio de Janeiro, v. 1, n. 2, p. 17-31, 2022. DOI: https://doi.org/10.21728/asklepion.2021v1n2.p17-31. Disponível em: https://asklepionrevista.info/asklepion/article/view/31. Acesso em: 18 set. 2024.

D'ANDRÉA, C. **Pesquisando plataformas online**: conceitos e métodos. Salvador: EDUFBA, 2020.

DEWEY, J. **The public and its problems**. Ohio: Swallow Press Books, 1954.

DIJCK, J. Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. **Surveillance & Society**, [*s. l.*], v. 12, n. 2, p. 197-208, 2014. DOI: https://doi.org/10.24908/ss.v12i2.4776. Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication. Acesso em: 18 set. 2024.

DORNELAS, R.; GIANNINI, S.; FERREIRA, L. Dia Mundial da Voz em notícia: análise das reportagens sobre a Campanha da Voz no Brasil. **CoDAS**, [*s. l.*], v. 27, n. 5, p. 492-497, 2015. DOI: https://doi.org/10.1590/2317-1782/20152014204. Disponível em: https://www.scielo.br/j/codas/a/KcXXQykn8qK7gqcS9CCtpxL/abstract/?lang=pt. Acesso em: 18 set. 2024.

EVANGELISTA, R. **Para além das máquinas de adorável graça**: cultura hacker, cibernética e democracia. São Paulo: Edições Sesc São Paulo, 2018.

GOMES, M.; CORDEIRO, S.; PINHEIRO, W. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). **Revista Militar de Ciência e Tecnologia**, [*s. l.*], v. 33, n. 2, p. 11-18, 2016. Disponível em: https://rmct.ime.eb.br/arquivos/RMCT_3_tri_2016_web/RMCT_275.pdf. Acesso em 18 setembro 2024.

GREENBERG, A. **Sandworm**: uma nova era na guerra cibernética e a caça pelos hackers mais perigosos do Kremlin. Rio de Janeiro: Alta Books, 2021.

HENRIQUES, M.; SILVA, D. Vulnerabilidade dos públicos frente a práticas abusivas de comunicação empregadas por organizações: limitações para o monitoramento civil. **Comunicação e Sociedade**, [*s. l.*], v. 26, p. 162-176, 2014. DOI: https://doi.org/10.17231/comsoc.26(2014).2031. Disponível em: https://revistacomsoc.pt/article/view/1152. Acesso em: 18 set. 2024.

IT FÓRUM. **Ataques cibernéticos crescem 67% no Brasil no 2º trimestre de 2024**. IT Fórum, 19 de julho de 2024. Disponível em: https://itforum.com.br/noticias/ataques-ciberneticos-crescem-67-brasil-2-tri-2024/. Acesso em: 18 set. 2024.

LAGE, N. **Estrutura da Notícia**. São Paulo: Ática, 1993.

LEMOS, A.; SEARA, S.; PÉRSIO, W. Hackers no Brasil. Dossiê Imagens: **Múltiplos sentidos**, [*s. l.*], n. 6, p. 21-42, 2002. DOI: https://doi.org/10.22409/contracampo.v0i06.463. Disponível em: https://periodicos.uff.br/contracampo/article/view/17322. Acesso em: 18 set. 2024.

MALAGUTI, B. **A utilização inadequada do termo hacker na mídia e implicações no ordenamento jurídico**. JusBrasil, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/a-utilizacao-inadequada-do-termo-hacker-na-midia-e-implicacoes-no-ordenamento-juridico/1743565231. Acesso em: 18 set. 2024.

MARRES, N. The issue deserve more credit: pragmatist contributions to the study of public involvement in controversy. **Social Studies of Science**, v. 37, n. 5, 2007. DOI: https://doi.org/10.1177/0306312706077367. Disponível em: http://sss.sagepub.com/content/37/5/759. Acesso em: 18 set. 2024.

MORAES, F. Jornalismo, ativismo e sensibilidade hacker: por uma prática situada que ousa dizer o nome. **Revista Alceu**, [*s. l.*], v. 21, n. 44, p. 115-131, 2021. DOI: https://doi.org/10.46391/ALCEU.v21.ed44.2021.244. Disponível em: https://revistaalceu.com.puc-rio.br/alceu/article/view/244. Acesso em: 18 set. 2024.

SCHNEIER, B. **Clique aqui para matar todo mundo**: como sobreviver em um mundo hiperconectado. Rio de Janeiro: Alta Books, 2020.

SILVA, W. **A evolução da criptografia e suas técnicas ao longo da história**. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) — Instituto Federal Goiano, Ceres, 2019. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1/tcc_Willian_Wallace_de_Matteus_Silva.pdf. Acesso em: 18 set. 2024.

WALTERS, R. **Cyber Attacks on U.S**. Companies Since November 2014. Report Cybersecurity, The Heritage Foundation, 2015. Disponível em: https://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014. Acesso em: 18 set. 2024.

Data de submissão: 18 de setembro de 2024
Data de aceite: 24 de outubro de 2024