LUMINA
Revista do Programa de Pós-graduação em Comunicação
Universidade Federal de Juiz de Fora / UFJF
e-ISSN 1981-4070

Imaginários dos públicos sob a ótica dos ataques cibernéticos:

caso das Lojas Renner

Fernanda Shelda de Andrade Melo[1]

Resumo

Este trabalho tem como objetivo refletir sobre os imaginários que cercam o acontecimento de um ataque cibernético. Conhecidos popularmente como "ataques *hackers*", esses episódios envolvem o acionamento de ideias e de cobranças dos públicos a partir de possíveis vazamentos de dados, que colocam à prova diversas vulnerabilidades – tanto dos clientes, como das próprias organizações afetadas. A intenção foi compreender este cenário permeado por questionamentos utilizando um estudo focado no caso das Lojas Renner, que sofreu um desses ataques em 2021. A primeira etapa aplicou uma revisão bibliográfica, discutindo os principais temas que envolvem a lógica dos ciberataques e entendendo como eles acontecem. Em seguida, a metodologia exploratória foi colocada em prática a partir de uma análise sob a perspectiva qualitativa de comentários coletados em uma das publicações no perfil do Instagram da empresa no dia do incidente. Reunimos os termos mais mencionados em uma *word cloud*, investigando em seguida as cobranças mais latentes advindas na enunciação dos sujeitos. Os resultados iniciais apontam para imaginários sociodiscursivos centrados em uma ideia catastrófica dos ataques, com preocupações mais voltadas para as instabilidades de acesso e uso do que para a segurança digital.

Palavras-chave

Ataques cibernéticos; imaginários; públicos; *hackers*; comunicação organizacional.

[1] Doutoranda em Comunicação Social do 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.

LUMINA
Revista do Programa de Pós-graduação em Comunicação
Universidade Federal de Juiz de Fora / UFJF
e-ISSN 1981-4070

Public imaginaries through the lens of cyberattacks:

the case of Lojas Renner

Fernanda Shelda de Andrade Melo[1]

Abstract

This study aims to reflect on the imaginaries surrounding the occurrence of a cyberattack. Popularly known as "hacker attacks", these events trigger public perceptions and demands from the public based on possible data leaks, which expose various vulnerabilities – both for customers and the affected organizations. The intention was to understand this scenario, marked by uncertainty and questioning, through a case study of Lojas Renner, which suffered such an attack in 2021. The first stage applied a bibliographic review discussing the key themes involving the logic of cyberattacks and understanding how they happen. Then, the exploratory methodology was put into practice based on a qualitative analysis of comments collected from one of the company's Instagram posts on the day of the incident. We gathered the most mentioned terms in a word cloud, investigating the most latent demands arising from the subjects' statements in a second stage. Initial results point to socio-discursive imaginaries centered on a catastrophic idea of attacks, with greater concern over access and usability issues than over digital security itself.

Keywords

Cyberattacks; imaginaries; publics; hackers; organizational communication.

[1]Doutoranda em Comunicação Social do 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.

Introdução

Último mês do período de inverno e próximo à comemoração nacional do Dia dos Pais, agosto costuma ser importante para pequenos e grandes comércios. Porém, para as Lojas Renner, esse cenário aconteceu fora da normalidade no ano de 2021. Qualquer cliente que tentasse acessar os serviços dos sites ou, até mesmo, realizar pagamentos nos locais físicos das Lojas Renner com cartões da empresa, encontrava falhas nos serviços. Os boatos começaram a circular, afinal, como pagar o boleto do cartão de crédito sem as funcionalidades ativas? Ou pior: como garantir que os erros de conexão não respingariam na segurança das próprias contas? Diversas indagações dos clientes começaram a surgir nas redes sociais da organização, que confirmou para a imprensa, na noite de 19 de agosto de 2021, que havia sofrido um ataque cibernético (Site [...], 2021).

Anteriormente conhecidos como ataques *hackers*, essas ações invasoras no ambiente digital prejudicam empresas e indivíduos que se tornam vulneráveis à exposição de dados on-line. Para os públicos, surge o receio de estar em um eclipse – termo utilizado por Dewey (1954) para indicar o momento em que os sujeitos estão na opacidade sem saberem o que está acontecendo e, consequentemente, não preverem uma ação para o problema. Nesses casos, informações pessoais podem ser vazadas sem o conhecimento dos próprios clientes. Já para as organizações, as vulnerabilidades não são menores: de acordo com a empresa britânica de segurança de *software* Sophos, das 75 empresas que sofreram esse tipo de ataque no Brasil em 2023, 83% desembolsaram altos valores para recuperar os dados. A quantia de resgate (valor pago para acabar com o "sequestro" de dados) chega a totalizar cerca de R$6,2 milhões (Sutto, 2024).

Todo esse contexto precisa ser integrado a uma discussão que retoma as lógicas de segurança digital e a interação entre atores humanos e não humanos durante um acontecimento. Nesse sentido, a relação dos sujeitos com pequenos números registrados em um banco de dados se torna um ponto de partida, já que na contemporaneidade os dados determinam algumas condições digitais e o que podemos ou não acessar e fazer. Essa visão não pretende ceder total "poder" aos dados, mas reconhecer que eles fazem parte das relações interpessoais e dos cotidianos dos indivíduos (D'Andréa, 2020). E no caso dos ataques exemplificados anteriormente, esse cenário é extremamente pontual: sistemas como o das Lojas Renner registram e salvam informações pessoais, além das integrações com meios de pagamento que coletam dados financeiros – como cartões de crédito.

Esse debate também reflete um ponto fundamental: os imaginários, já que a relação com a tecnologia é colocada à prova na perspectiva do que é factível e quais ideias se destacam sobre os ataques. O conceito de imaginários pode ser abordado em diversas dinâmicas, mas é importante estabelecer que eles são usualmente mantidos

coletivamente, múltiplos e podem evocar noções desejáveis ou distópicas de um cenário (Mager; Katzenbach, 2021). Uma outra ideia destacada nesta discussão é a de imaginários algorítmicos. Essa concepção reúne esforços acadêmicos que visam discutir como a população percebe e lida com o cenário marcado pela plataformização (Winques, 2022). Além disso, quando discutidos a partir da lente sociodiscursiva, os imaginários são fundamentais para compreender "um modo de tomar conhecimento do mundo socialmente partilhado" (Charaudeau, 2017, p. 575).

Dessa forma, o objetivo desta pesquisa está centrado em refletir, a partir do caso das Lojas Renner, sobre os imaginários que cercam o acontecimento de um ataque cibernético. A fase analítica deste trabalho selecionou a metodologia exploratória para coletar comentários de clientes em uma das publicações no perfil do Instagram da empresa durante o período do ataque. A partir dos 3.851 comentários obtidos, realizamos uma análise qualitativa das indagações, dúvidas e incertezas, inspirando-se nas perspectivas do mapeamento de controvérsias de Venturini e Munk (2021), adaptando as sugestões para a observação dos imaginários. O trabalho foi dividido em duas seções teóricas que abordam os contrastes dos ataques cibernéticos e como acionamos essa perspectiva na esfera dos imaginários, posteriormente trazendo a análise empírica. Um ponto que chama a atenção nos resultados iniciais é a preocupação mais destacada em relação à falta de acesso e pouco voltada para lógicas de segurança digital – como o vazamento de dados.

Ataques cibernéticos: o que são e como acontecem?

A ameaça de uma figura que se aproxima dos contos míticos é aplicada no entendimento do que é um *hacker*. No começo dos anos 2000, os estudos acadêmicos reuniam esforços para explicar o que exatamente era essa *persona*, bem como a necessidade de diferenciá-la a partir de suas atividades. Lemos, Seara e Pérsio (2002) chegam a inferir duas categorias: o *cracker*, alguém que invade e danifica sistemas, e o *hacker*, que apenas apareceria no ciberespaço em testes de segurança, exibindo a invasão como uma conquista. Evangelista (2018) ainda destaca o termo *hackerismo*, perspectiva de ativismo democrático ligado às invasões de sistemas privados. Nesse sentido, jogos, filmes ou até livros pagos poderiam ser acessados a partir de vazamentos causados por esses grupos. É a partir daí que o autor também pontua que a perspectiva *hacker* tem uma cultura e até regras de colaboração em meio a algumas vertentes de programadores.

Há alguns anos, esforços acadêmicos vêm sendo feitos para deixar de lado o termo *hacker*, principalmente devido à conotação negativa e ao estigma que ele carrega, passando a utilizar termos como “ciberataques” ou “ataques cibernéticos”. Em algumas vertentes, como no caso dos estudos ligados à criminologia, a crítica é em relação à grande variedade de nomeações e à imensa abrangência

do termo *hacker* (Nunes Sobrinho; Scott, 2022). As invasões danosas e com objetivo de prejudicar, ou seja, fora do espectro de colaboração mencionado anteriormente, também passaram por tipificações de crime cibernético, que é definido como: "Todo delito praticado utilizando a tecnologia da informação como ferramenta a fim de causar dano a outrem" (Araújo; Rossi, 2020, p. 15).

Independentemente de como sejam chamados, uma coisa é certa: os danos acarretados durante esses ataques são enormes e atingem uma diversidade de empresas. Esse é o caso da Windows, atacada em 2017, e do restaurante Chick-Fil-A, em 2014. Segmentos extremamente variados e distintos, mas que acabam com os mesmos problemas: a preocupação com o vazamento de dados que podem gerar tanto perdas monetárias quanto prejuízos jurídicos em relação à proteção ao consumidor (Lima, 2018; Walters, 2014).

Uma reflexão importante está no entendimento sobre como ocorre um ataque cibernético. Em primeiro lugar, precisamos considerar que as infraestruturas digitais estão todas configuradas a partir de *softwares*, que podem ser entendidos como "qualquer programa de computador capaz de comandar o funcionamento de um sistema com base em computador, executando tarefas específicas" (Amorim, 2015, p. 3). Dessa forma, um *software* nada mais é do que o programa em sua versão *backstage*, um ponto fundamental que, configurado da maneira correta, desenvolverá as requisições para um sistema específico, seja um programa ou aplicativo. Há, ainda, a presença dos *hardwares*, que se encontram em uma condição mais física – como é o caso de fios, placas e da estrutura responsável por fazer os *softwares* funcionarem.

Durante um cibercrime, o alvo pode ser uma ou mais redes ligadas a um *software* ou *hardware*. Por exemplo, o ataque pode tentar invadir a seção onde estão elencadas as principais informações de um banco de dados e alcançar somente parte delas. Em algumas empresas, principalmente aquelas ligadas ao setor bancário, o armazenamento de dados é guardado a sete chaves – ou melhor que chaves, criptografias. Nesse sentido, mesmo quando há um vazamento, o criminoso precisaria descriptografar todas as informações para ter algo útil. É como tentar enxergar a expressão “Oi”, mas apenas ler o código 01001111 01101001 [1]. Assim, a criptografia é uma estratégia desenvolvida ao longo dos anos justamente para lidar com questões de segurança, principalmente no sentido de acessos não autorizados (Silva, 2019).

Além disso, existem diferentes tipos de ataques. As duas categorias mais conhecidas são separadas como *Distributed Denial-of-Service* (DDoS) e *ransomware*. Araújo e Rossi (2020) explicam que o DDoS prevê apenas aquilo que está intrínseco na tradução de seu nome: uma interrupção do sistema. Nesses casos, geralmente os usuários presenciam travamentos nos aplicativos ou sites que carregam com lentidão. Por isso, esse ataque é visto como algo mais superficial, apesar de Greenberg (2021) pontuar que são importantes ferramentas em guerras políticas, pois alguns tipos de DDoS podem ser usados para espionagem.

Enquanto isso, os ataques que utilizam *ransomware* podem tentar invadir sistemas ou posicionar *malwares* – arquivos "contaminados" – nos computadores do alvo. Nesses casos, há a possibilidade de um roubo de dados, acessando informações indevidas. Essa foi justamente a categoria do ataque às Lojas Renner, como declarado pela própria empresa, que relatou ainda que os criminosos solicitaram 20 milhões de dólares para restabelecer os sistemas após os danos (Lopes, 2021). Geralmente, as táticas de extorsão do alvo também são comuns para persuadir as empresas a não deixarem que documentos sigilosos sejam vazados.

Apesar dos exemplos explicitados estarem ligados às organizações, é importante ponderar que esses crimes também podem acontecer com indivíduos comuns, principalmente aqueles mais vulneráveis on-line. Dessa forma, fica claro reparar como os ataques cibernéticos são perigosos e estudá-los se torna indispensável no contexto permeado pela plataformização. Essas infraestruturas podem guiar lógicas cotidianas, como dados bancários para uma simples transação, informações de registro em um clube ou até fotografias guardadas no modo privacidade em uma rede social. Todos esses exemplos são datificados em sistemas digitais (Poell; Nieborg; Dijck, 2020) e estão sujeitos a invasões. Estudar aspectos e fragilidades desse acontecimento pode dar ênfase à necessidade de expandir entendimentos sobre segurança digital, entendendo o que os públicos pensam e como lidam com esse cenário, adquirindo conhecimento sobre ele a partir da tentativa de escapar das assimetrias de acesso e poder que cercam esses acontecimentos enraizados nas materialidades digitais (Guerra; D'Andréa, 2023).

Imaginários na lógica digital

Durante o processo de crescimento, nossa consciência utiliza dos imaginários para condicionar uma noção de mundo. É nessa lógica que, quando crianças, começamos a fazer perguntas sobre tudo e todos, pretendendo alcançar a superfície do conceito das coisas. No estudo de públicos, alguns teóricos se esforçam para explicar o entendimento social. Lippmann (2008) chega a utilizar a ideia dos estereótipos: longe do estigma negativo, essa perspectiva defende que cada indivíduo se aproxima e concorda com conceitos que estão mais próximos de suas realidades. Esse sentido é ainda mais prolongado com a aceleração do tempo no cenário digital, já que pegaríamos atalhos cognitivos para entender aquilo que nos cerca.

Quando voltamos o debate para os ataques cibernéticos, essa ideia também pode fazer sentido, principalmente no caso das vulnerabilidades dos públicos. Um exemplo simples está na própria concepção do que é um *hacker*: como explicado anteriormente, a imagem negativa da palavra foi construída ao longo dos anos e pode carregar a imagem de um "terrorista digital" que atacaria sistemas apenas para o "mal", segundo uma ideia determinista de bom e ruim. Essa ideia é contornada

pelo surgimento dos *hackers* "do bem", que são profissionais da Tecnologia da Informação (TI). Esses indivíduos atuam na direção contrária: atacam as instituições que trabalham justamente para identificar possíveis fragilidades e onde pode estar a melhor solução de segurança (Nunes, 2025). Além, é claro, das perspectivas de *hackativismo* (Evangelista, 2018).

É válido lembrar que os dispositivos presentes nesse contexto ainda são permeados por interações de agentes humanos (nós, enquanto sujeitos) e os agentes não humanos – no caso dos ataques, os sistemas que são invadidos, os dados roubados e a própria infraestrutura voltada para a segurança digital. Essas lógicas não são pré-definidas apenas pela possibilidade de ataque, mas também pela participação que os agentes humanos têm neste processo, o que também conta com os imaginários do que é ou não possível durante esse acontecimento (Braga, 2020). É relevante visualizar essa discussão com ajuda da perspectiva neomaterialista, que enfatiza a importância de entender as peças da infraestrutura digital que permeiam esses fenômenos. Por isso, neste trabalho, refletimos sobre essa interação entre ambos agentes elencados nas possibilidades dos imaginários (Lemos, 2020).

De acordo com Silva (2020, p. 40), "imaginários tratam tanto das lentes usadas para interpretar fenômenos e ações presentes – considerando interpretações do passado – quanto na definição de horizontes de possibilidades". Logo, as ideias que são construídas por nós, socialmente imbricados, fazem parte do que entendemos diante da vivência humana. Uma outra concepção importante para a discussão apresentada está baseada no imaginário algorítmico. Apesar dos esforços acadêmicos dessa perspectiva se basearem de forma mais enfática nas teorias dos algoritmos e suas recomendações de uso, podemos resgatar a análise da percepção dos usuários no mesmo caso dos ataques. Isto é, "o imaginário algorítmico não deve ser entendido como uma crença falsa ou uma espécie de fetiche, mas, antes, como a maneira que as pessoas imaginam, percebem e experimentam algoritmos e o que essas imaginações tornam possível" (Bucher, 2017, p. 11) (Tradução nossa) [2].

Destacamos, também, a expressão "imaginários sociodiscursivos", especialmente por estar ligada aos debates que defendem a dinâmica que é apresentada durante a fala e a enunciação. Considerando que o presente trabalho pretende analisar a perspectiva dos públicos durante o acontecimento de um ataque cibernético, essas manifestações também refletem a construção dos imaginários, uma vez que estes são "engendrados pelos discursos que circulam nos grupos sociais, se organizando em sistemas de pensamento coerentes, criadores de valores, desempenhando o papel de justificação da ação social e se depositando na memória coletiva" (Charaudeau, 2017, p. 578).

Ainda quando falamos sobre os ataques, é importante destacar que um ator central nessa esfera são os dados. Nos principais casos de *malwares*, a intenção está no roubo desta "matéria-prima", visando às informações que estão elencadas nessa

estrutura datificada. Isso nos leva a pensar sobre as implicações dos imaginários nessa dinâmica. O fluxo de alimentação dos dados em relação à concentração de poder se tornou uma possível forma de colonização e de quantificação da vida (Ricaurte, 2023). Essa concepção abre reflexões sobre uma outra vulnerabilidade dos públicos durante tal acontecimento: a assimetria de conhecimento em relação aos próprios dados. Dessa forma, sem sequer entender o que pode ter sido roubado durante os momentos de ataques *ransomware*, é ainda mais desafiador para os sujeitos considerarem se estão ou como estão vulneráveis. Assim, é indispensável entender que essa assimetria também pode elencar uma nova condição de poder neste contexto.

O acontecimento do ataque também é permeado de dúvidas e receios, algo comum na disputa de sentidos protagonizada pelos públicos e pelas organizações – fluxo de discussões que acaba constituindo possíveis controvérsias acerca do acontecimento. O imaginário é necessário tanto para elaborar um entendimento (mesmo que primário) do que está acontecendo quanto pode ser crucial para o momento de ação. Isso significa que, mesmo quando é fantasiada, a ideia do que é um ataque cibernético pode ajudar durante o contorno das vulnerabilidades, como iniciativas que vão do bloqueio de cartões até a cobrança por mais informações da instituição que foi atacada.

Partindo desse ponto, Maffesoli (2001) nos lembra que é preciso quebrar a ideia de que os imaginários estão sempre distantes da realidade, intangíveis. Na verdade, é preciso entender essa concepção como elemento de ensejo, advindos de "algo que ultrapassa o indivíduo, que impregna o coletivo ou, ao menos, parte do coletivo" (Maffesoli, 2001, p. 76). Ao unir esse conceito com possíveis análises que podem respingar no estudo dos acontecimentos dos ataques cibernéticos, propomos na seção seguinte um estudo que permite um vislumbre dessa perspectiva em um caso real.

Fase analítica

De acordo com os estudos de Dewey (1954), os públicos partem para a ação em uma sequência: após repararem que estão sofrendo, afetados por alguma coisa, agem. Essa teoria, pautada no sofrer e no agir, ilustra um cenário interessante na perspectiva dos ataques cibernéticos, principalmente porque é fundamental para os indivíduos saberem que podem estar vulneráveis. Na contramão desse pensamento, as organizações, durante os momentos de ataque, também estão vulneráveis – são diretamente atacadas e alvos da situação. Durante esse contexto, é notório que há a presença de boatos e dúvidas em relação ao ataque: o que aconteceu? Como aconteceu? Quem foi atingido? São inúmeras as perguntas (e respostas) que exibem as publicações no perfil das empresas durante o período de ataque aos sistemas.

Entretanto, para além da controvérsia e da disputa de sentidos na tentativa

de liderar o discurso em uma argumentação entre públicos e organizações, o presente trabalho destaca um quesito importante: os imaginários. É a partir dos imaginários que os discursos dos públicos se manifestam na cobrança dessas empresas e do que, especialmente, esses sujeitos entendem sobre o acontecimento e percebem os efeitos dele sobre si. Permeado de termos técnicos e projeções distópicas, os ataques cibernéticos podem causar o compartilhamento de rumores e até uma crescente mistificação do que de fato ocorreu. Logo, os esforços munidos neste artigo se inspiram em Marres (2007) na junção do pragmatismo de Dewey com a perspectiva dos Estudos Sociais da Ciência e da Tecnologia (STS) para compreender a dinâmica do envolvimento dos públicos com a mobilização de atores não humanos que constituem um papel fundamental nesse acontecimento.

Ainda considerando o ambiente digital, entendemos que a abertura de discussões pode fazer parte do resultado da organização comunicada, aquela que advém da interação entre organizações e sujeitos em suas publicações oficiais ou discursos da empresa (Baldissera, 2009). Entender as menções e os comentários também é uma forma de transformar dispositivos para o usuário em dispositivos de pesquisa (Venturini; Munk, 2021). Dessa forma, o presente trabalho selecionou um acontecimento específico: o ataque às Lojas Renner em setembro de 2021. Para contextualizar o caso, iniciaremos elencando informações sobre o episódio.

No final da tarde do dia 19 de agosto de 2021, os sistemas das Lojas Renner começaram a apresentar instabilidades. Isso significa que aqueles que tentavam acessar o site ou os aplicativos não encontravam uma página on-line, além das interrupções dos serviços físicos como o pagamento de cartões e compras no caixa. A partir desse momento, os clientes começaram a perceber os efeitos negativos durante o uso, até que veículos jornalísticos iniciaram publicações sobre o ocorrido. Do dia 19 de agosto até o dia 24, os sistemas continuaram com instabilidades, variando seus níveis de apresentação. Ou seja, em alguns momentos era, sim, possível acessar o site, enquanto em outros horários ele voltava a sair do ar. O mesmo aconteceu com os outros serviços prestados que, de alguma forma, tivessem ligação com os *softwares* utilizados pela empresa. Vale pontuar que não identificamos nenhuma publicação de aviso sobre o ocorrido nas páginas das Lojas Renner, manifestação que aparece apenas em respostas nos comentários e utilizando o termo que citamos aqui – instabilidade – para detalhar o que estava acontecendo.

Durante a exploração prévia em navegação flutuante para selecionar o *corpus* deste trabalho, foi possível notar um diferencial: saindo da média de comentários no perfil da empresa no Instagram – que beira de 700 a 800 interações por publicação – a postagem no dia do ataque cibernético (19 de agosto de 2021) tem quase 4 mil comentários. Essa dimensão, quatro vezes maior que o normal, chama a atenção devido à manifestação do público.

Dessa forma, utilizando a linguagem de programação Python, foi possível

rodar uma aplicação de *scraping*, coletando todos os comentários da postagem, função permitida pela presença de uma *Application Programming Interface* (API) no Instagram. A biblioteca resultante do *scraping* gerou um arquivo .csv com 3.851 comentários. Desse número, fizemos um recorte: os comentários das Lojas Renner foram excluídos. Não como tentativa de ignorar a presença da organização, mas porque o objetivo do artigo está nos imaginários acionados pelos públicos: quais são as principais questões? Como se referem ao acontecido? Quais são as preocupações mais latentes? O resultado do recorte foi de 22,7%, deixando-nos com 2.979 comentários advindos de usuários.

Com esse material em mãos, nutrimos alguns passos empíricos: a) Utilizamos a ferramenta Flourish para filtrar quais palavras foram mais citadas durante esse período para entender os termos que mais aparecem em uma nuvem de palavras; b) Pesquisamos cinco ideias relacionadas ao tema e suas variações (plural e artigos): "*hacker*", "ataque", "dados", "instável", "acesso", visando compreender como o acontecimento foi abordado pelos públicos; c) Retornamos aos termos mais utilizados do primeiro e do segundo passo para entender as preocupações mais latentes que cercavam os comentários, procurando contextualizar os dois primeiros resultados em uma análise mais cuidadosa e qualitativa. Essas classificações, inicialmente mais soltas e que vão determinando caminhos durante a própria análise prática, retomam a ideia de seguir os atores: "Não presumirei saber melhor do que as pessoas que estou estudando. Aprenderei com eles o que é relevante e importante, o que faz parte da controvérsia e o que não faz" (Venturini; Munk, 2021, p. 43) (Tradução nossa) [3].

Antes da efetivação do primeiro passo, também foi preciso nortear algumas medidas de busca, como é o caso da soma entre termos que estivessem no singular, plural e gerúndio (exemplo: *acesso*, *acessos*, *acessando*), além da exclusão de artigos e conjunções, dando preferência para termos e palavras. Ademais, os resultados foram destacados na nuvem de palavras da ferramenta Flourish (2024) após constatação de que se repetiam mais de 15 vezes – uma vez que diversas palavras poderiam aparecer somente uma ou duas vezes e não apareceriam em tamanho hábil na nuvem. Outro ponto importante é que na *word cloud*, palavras com tons mais fortes e maior tamanho representam uma repetição maior. O contrário também é válido, em que termos mais apagados e com tamanho menor aparecem com menos recorrência (Imagem 1).

Imagem 1 - Nuvem de palavras resultante dos comentários analisados.

Fonte: Elaborado pela autora a partir da plataforma Flourish.

Alguns pontos importantes para visualizar nessa nuvem de palavras estão em termos-chave: *problema*, *sistema*, *cartão*, *site*, *acessar*, *aplicativo* (*app*). A percepção do ataque fica nítida quando tentamos entender as citações mais recorrentes dos clientes, uma vez que a maior parte delas está justamente ligada às funcionalidades técnicas. *Aplicativo* – que aparece em uma de suas variações, enquanto *app* – é a palavra mais citada em todos os comentários da publicação, rendendo 239 menções ultrapassando a própria marcação do *user* das Lojas Renner (@lojasrenner), utilizado para chamar a atenção da conta. Outras perspectivas de atendimento sobre o ocorrido também aparecem no mural, como é o caso da busca por *resposta*, *contato* e *telefone* da empresa.

Nosso segundo movimento empírico foi rastrear cinco termos fundamentais neste debate: *hacker*, *ataque*, *dados*, *instável*, *acesso*. Quando buscamos pela expressão *hacker* encontramos 67 resultados que apontam para a utilização da palavra com variáveis. Em sua maioria, ela está unida de termos como "invasão", "alvo" e "ataque". Outro fato interessante é que a maioria dos comentários menciona o resgate solicitado pelos *hackers*, tema que foi noticiado na imprensa (Lopes, 2021). Dessa forma, parte das indagações se volta para se – ou quando – as Lojas Renner fariam o pagamento. Nesse simples vislumbre, é possível perceber que o próprio termo *ataque* está presente em 99,9% das citações ligadas à palavra *hacker*. Em comparação ao acionamento utilizado na academia (ataque cibernético) identificamos que o uso é muito menor que *ataque hacker*: apenas 1/3 do primeiro. Essa ênfase nos mostra

diferenças em relação ao imaginário dos públicos e das discussões apresentadas na literatura acadêmica, como pontuado anteriormente, sobre o estigma da palavra *hacker*.

Em contrapartida, a palavra dados aparece 37% a mais nas indagações que o próprio termo *hacker*. Dentro desse número, apenas cinco clientes parecem questionar um possível vazamento dos dados ou até a perspectiva de proteção dessas informações. Enquanto isso, a maioria das citações está voltada para a denúncia de um possível golpe de uma conta *fake* das Lojas Renner que, durante o momento de instabilidade, também estava pedindo dados pessoais para resolver os problemas enfrentados. Alguns clientes chegam a reiterar que os dados foram enviados no *chat* privado oficial das Lojas Renner para análise de cada caso, seja para detalhar os golpes ou procurar soluções.

Quando partimos para os termos *instabilidade* (*instável* e suas variações) e *acesso*, os problemas técnicos são destaque na colocação dessas palavras. Nesses dois pontos, é possível presenciar um primeiro contato dos sujeitos com o acontecimento, pois geralmente as perguntas estão mais ligadas a entender porque o acesso não funciona ou por quais motivos o site e o aplicativo estão instáveis. É um momento notável de dúvidas, em que não há certeza sobre o acontecimento e sobre o que se deve esperar.

Fizemos um movimento importante de voltar à nuvem de palavras, a partir do contexto analisado, de forma mais específica. Logo após as quatro palavras mais citadas (*app*, *lojasrenner*, *site* e *sistema*) destacamos as expressões "pagar" e "fatura", ambas na linha das 80 menções – citadas individualmente mais que a própria palavra *hacker*. Em um primeiro momento, pode parecer que a lógica dessas duas questões está voltada apenas para o olhar técnico de instabilidade, análise semelhante a do parágrafo anterior. Porém, quando partimos para o entendimento do contexto, é possível perceber que os clientes estão demonstrando suas principais preocupações: os juros.

Em todos os termos elencados anteriormente, encontramos perguntas em relação aos juros dos boletos e dos cartões da empresa. Isso porque, com os sistemas fora do ar, era impossível ter acesso às próprias contas ou sequer verificar quanto devia. Nos comentários nos dias seguintes ao ataque, principalmente durante as voltas parciais dos sistemas, os sujeitos reiteravam que juros estavam sendo cobrados por boletos vencidos durante o período.

Temos, então, algumas perspectivas conclusivas a partir dessas análises. Em primeiro lugar, é possível compreender que o receio do uso do termo *hacker* na academia, principalmente na defesa em se afastar do estigma negativo da palavra e reiterar o uso de *ataques cibernéticos* é uma realidade que se apresenta diferente na vivência dos sujeitos. Para os públicos que se manifestaram nesse acontecimento específico, *hackers* é o nome dado para os responsáveis pela instabilidade na

dualidade do bem e mal. Durante esse tipo de mapeamento, aquilo que se define como verdade é constituído em conjunto (Venturini; Munk, 2021). Logo, os imaginários que se apresentam nessa esfera podem diferir da perspectiva estudada no momento teórico e desaguar em visões diversas por parte daqueles que estão sendo afetados. Todavia, o que podemos problematizar em conjunto das discussões teóricas está justamente na imagem desse *hacker* mencionado, afinal, ela continua fazendo parte de uma visão ligada aos crimes e danos.

Em segundo lugar, é importante notar que a preocupação com a segurança dos dados ficou de escanteio no acionamento de imaginários durante o ataque. Isso porque, as menções em relação à segurança digital dos dados eram muito menores em relação aos outros questionamentos apresentados. É possível inferir que, por vezes, as vulnerabilidades dos públicos que enxergamos vão além da superfície, pois é preciso entender quais perspectivas de fato afligem os sujeitos durante esse momento e se as preocupações da academia estão voltadas para a realidade do acontecimento: permeado de dúvidas, questionamentos e boatos. Imersos em preocupações, a principal defesa para os clientes era fugir de mais golpes que apareciam naquele momento.

Por fim, a perspectiva dos juros segue esse mesmo princípio em relação aos imaginários sociodiscursivos. O acionamento das maiores preocupações durante o acontecimento estava na possibilidade de "ter que pagar mais" por algo que sequer era culpa dos clientes. É justamente nesse momento que há a possibilidade de observar possíveis controvérsias e disputas de sentido, uma vez que outras temáticas podem entrar em disputa, como no caso de contratos e perspectivas dos direitos dos consumidores em relação à cobrança.

Considerações Finais

A partir das discussões apresentadas, foi possível perceber um rastro dos imaginários acionados durante um ataque cibernético, principalmente voltado para as preocupações que cercam os públicos, suas vulnerabilidades e principais manifestações sobre o caso. Identificamos que pautas debatidas na academia aparecem de formas distintas quando tratadas na ótica dos públicos, além do surgimento de fragilidades diversificadas que aparecem durante o acontecimento.

As principais questões abordadas pelos agentes envolvidos podem nos mostrar um cenário contrasta com o fato de os sujeitos estarem imersos durante esse caso e, especialmente, sobre as disputas de sentido permeadas por ele (Venturini; Musk, 2021). Quando encaramos, por exemplo, a tentativa de proteção dos golpes que apareceram de contas que simulavam o perfil oficial das Lojas Renner, percebemos uma tentativa unificada de avisar os outros usuários e o próprio impacto que isso também gerou na percepção do ataque. Essa experiência tomou o espaço da própria repercussão do

ponto inicial da controvérsia: a invasão do banco de dados da empresa.

Além disso, afetados, os públicos buscaram formas para agir (Dewey, 1954). Nesse caso, a dinâmica que cerca os comentários – e o próprio volume fora da curva que totalizava 4 mil interações na publicação – demonstra o espaço que eles encontraram na infraestrutura digital para realizar suas manifestações sobre o ataque, sejam estas relacionadas às indagações, ao compartilhamento de informação com outros clientes ou às preocupações com as cobranças indevidas, como foi possível observar.

Vale ainda considerar que todos nós, enquanto usuários presentes no ambiente digital, estamos sujeitos às vulnerabilidades desse tipo de acontecimento. Isso porque as infraestruturas dos dados estão imbricadas no dia a dia humano, tratando diversas informações sensíveis sobre nossas vidas. Dessa forma, investigar como esse tipo de ataque se revela e o que podemos esperar deles, pode ajudar a minimizar cada vez mais as vulnerabilidades dos públicos, entendendo que as organizações também podem visar ao mesmo objetivo.

Entendemos a necessidade da continuidade de pesquisas que possam unir esse campo de estudos, principalmente mergulhando em outras categorias de observação, sem deixar de lado a lente comunicacional. Uma perspectiva interessante para continuidade do processo iniciado neste artigo está justamente no mapeamento de possíveis controvérsias que podem aparecer durante esses momentos, reunindo esforços que possam notar ambas as perspectivas – clientes e empresas – aprimorando a vertente aplicada neste trabalho.

Notas

[1] Conversão da palavra “Oi” em código binário.

[2] *The algorithmic imaginary is not to be understood as a false belief or fetish of sorts but, rather, as the way in which people imagine, perceive and experience algorithms and what these imaginations make possible.*

[3] *I will not presume to know better than the people I am studying. I will learn from them what is relevant and important, what belongs to the controversy and what does not.*

Artigo submetido em 10/12/2024 e aceito em 01/07/2025.

Referências

AMORIM, D. Softwares de sistemas e de aplicações livres: benefícios e limitações no uso dessas tecnologias nos negócios. **Revista Científica Semana Acadêmica**, n. 69, p. 1-25, 2015. Disponível em: http://bit.ly/3OzumZo. Acesso em: 08 jun. 2024.

D’ANDRÉA, C. F. B. **Pesquisando plataformas online**: conceitos e métodos. Salvador:

EDUFBA, 2020.

ARAÚJO, F.; ROSSI, J. **A evolução dos ataques cibernéticos**. 2020. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana Ministro Ralph Biasi, Americana/SP, 2020. Disponível em: http://bit.ly/4lqabvg. Acesso em: 08 jun. 2024.

BALDISSERA, R. Comunicação Organizacional na perspectiva da complexidade. **Organicom**, v. 6, n. 10/11, p. 115-120, 2009. DOI: https://doi.org/10.11606/issn.2238-2593.organicom.2009.139013.

BRAGA, J. Neomaterialismo & Antropológicas. **Galáxia**, n. 45, p. 20-33, 2020. Disponível em: https://bit.ly/3Vkj4eO. Acesso em: 08 jun. 2024.

BUCHER, T. The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms. **Information, Communication & Society**, v. 1, n. 20, p. 30-44, 2017. DOI: https://doi.org/10.1080/1369118X.2016.1154086.

CHARAUDEAU, P. Os estereótipos, muito bem. Os imaginários, ainda melhor. **Entrepalavras**, v. 7, n. 1, p. 571-591, 2017. DOI: http://dx.doi.org/10.22168/2237-6321.7.7.1.571-591.

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

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

FLOURISH. [*S. l.*], 2024. Disponível em: https://flourish.studio. Acesso em: 17 jun. 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.

GUERRA, A.; D'ANDREA, C. Atravessando o "mar vermelho" algorítmico: ubertubers e seus modos de conhecer o preço dinâmico da uber. *In*: TOZI, F. (Org.). **Plataformas digitais e novas desigualdades socioespaciais**. São Paulo: Editora Max Limonad, 2023, p. 59-80.

LEMOS, A. Epistemologia da Comunicação, Neomaterialismo e Cultura Digital. **Galáxia**, n. 43, p. 54-66, 2020. DOI: http://dx.doi.org/10.1590/1982-25532020143970.

LEMOS, A.; SEARA, S.; PÉRSIO, W. Hackers no Brasil. **Contracampo**, n. 6, p. 21-42, 2002. DOI: https://doi.org/10.22409/contracampo.voi06.463.

LIMA, G. E. Ciberataques: uma reflexão sobre a responsabilidade internacional dos estados. **Caderno de Relações Internacionais**, v. 8, n. 15, p. 201-221, 2017. DOI: https://doi.org/10.22293/2179-1376.v8i15.646.

LIPPMANN, W. **Opinião pública**. Petrópolis: Vozes, 2008.

LOPES, A. Após ataque hacker, Renner nega que pagou US$20 milhões aos criminosos. [*S. l.*], **Exame**, 19 ago. 2021. Disponível em: http://bit.ly/3Uqa3jA. Acesso em: 05 jun. 2024

MAFFESOLI, M. Michel Maffesoli: o imaginário é uma realidade. **Famecos**, v. 8, n. 15, p. 74-82, 2001. DOI: https://doi.org/10.15448/1980-3729.2001.15.3123.

MAGER, A.; KATZENBACH, C. Future imaginaries in the making and governing of digital technology: multiple, contested, commodified. **New Media & Society**, v. 23, n. 2, p. 223-236, 2021. DOI://doi.org/10.1177/1461444820929321.

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, p. 759-780, 2007. DOI: https://doi.org/10.1177/0306312706077367.

NUNES, E. Hacking ético: da rebeldia à profissão. **Blog PUC-Rio**, [*S. l.*], 19 abr. 2025. Disponível em: https://bit.ly/4lt6y6R. Acesso em: 12 ago. 2025.

NUNES SOBRINHO, J.; GROTT, S. Os sujeitos ativos no cibercrime e a responsabilidade penal do ofensor. **Revista Científica Multidisciplinar do Ceap**, v. 4, n. 2, p. 1-10, 2022. Disponível em: https://bit.ly/49lEyOj. Acesso em: 08 jun. 2024.

POELL, T.; NIEBORG, D.; DIJCK, J. Plataformização. **Fronteiras – Estudos Midiáticos**, v. 22, n. 1, p. 1-10, 2020. DOI: https://doi.org/10.4013/fem.2020.221.01.

RENNER diz não ter pago resgate de dados depois de ataque hacker. [*S. l.*], **Poder 360**, 24 ago. 2021. Disponível em: http://bit.ly/3GHmWCM. Acesso em: 18 jun. 2024.

RICAURTE, P. Epistemologias de dados, colonialidade do poder e resistência. **Dispositiva**, v. 12, n. 22, p. 6-26, 2023. DOI: https://doi.org/10.5752/P.2237-9967.2023v12n22p6-26.

SILVA, T. Por outros imaginários sociotécnicos no novo normal. Observatório Itaú Cultural, n. 28, p. 37-41, 2020. Disponível em: http://bit.ly/3IGIdgx. Acesso em: 20 jul. 2025.

SILVA, W. W. M. **A evolução da criptografia e suas técnicas ao longo da história**. 2019. Trabalho de Conclusão de Curso. (Graduação em Sistemas de Informação) – Instituto Federal Goiano, Ceres, 2019. Disponível em: https://bit.ly/3DosfLd. Acesso em: 08 jun. 2024.

SITE das Lojas Renner sai do ar após ataque hacker. **G1**, [*S. l.*], 19 ago. 2021. Disponível em: http://bit.ly/4kV3XlV Acesso em: 20 jul. 2025.

SUTTO, G. 83% das companhias que sofreram ataques hackers no Brasil pagaram

resgates em 2023. **InfoMoney**, 09 maio 2024. Disponível em: https://bit.ly/49iOCHM. Acesso em: 08 jun. 2024.

VENTURINI, T.; MUNK, A. K. **Controversy mapping**: a field guide. Cambridge: Polity Press, 2021.

WALTERS, R. **Cyber Attacks on U. S. Companies Since November 2014**. [Washington, DC]: The Heritage Foundation, 2015. Disponível em: https://bit.ly/3ZmkIh8. Acesso em: 08 jun. 2024.

WINQUES, K. Imaginários algorítmicos: reflexões a partir de um estudo de recepção de matriz sociocultural. **Fronteiras – Estudos Midiáticos**, v. 24, n. 2, 2022. Disponível em: https://bit.ly/41g52P6. Acesso em: 08 jun. 2024.