UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE HUMANIDADES
DEPARTAMENTO DE CIÊNCIAS SOCIAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM SOCIOLOGIA

EUVALDO DE BARROS LIMA FILHO

DRAMATURGIA DA FRAUDE: CRIMES CIBERNÉTICOS E A MANIPULAÇÃO DE VÍTIMAS NO CEARÁ PÓS-PANDEMIA

FORTALEZA
2025

EUVALDO DE BARROS LIMA FILHO

DRAMATURGIA DA FRAUDE: CRIMES CIBERNÉTICOS E A MANIPULAÇÃO DE VÍTIMAS NO CEARÁ PÓS-PANDEMIA

Dissertação apresentada ao Programa de Pós-Graduação em Sociologia da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Sociologia. Área de concentração: Violência e Conflitos Sociais.

Orientadora: Profa. Dra. Jânia Perla Diógenes de Aquino.

FORTALEZA

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

L697d Lima Filho, Euvaldo.
Dramaturgia da fraude: crimes cibernéticos e a manipulação de vítimas no Ceará Pós-Pandemia / Euvaldo Lima Filho. – 2026.
90 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Humanidades, Programa de Pós-Graduação em Sociologia, Fortaleza, 2026.
Orientação: Profa. Dra. Jânia Perla Diógenes de Aquino.

1. Crimes Cibernéticos. 2. Dramaturgia da Fraude. 3. Sociologia Digital. 4. Letramento Digital. I. Título.

CDD 301

EUVALDO DE BARROS LIMA FILHO

DRAMATURGIA DA FRAUDE: CRIMES CIBERNÉTICOS E A MANIPULAÇÃO DE VÍTIMAS NO CEARÁ PÒS-PANDEMIA

Dissertação apresentada ao Programa de Pós-Graduação em Sociologia da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Sociologia. Área de concentração: Violência e Conflitos Sociais.

Aprovada em: 25/11/2025

BANCA EXAMINADORA

_____

Profa. Dra. Jânia Perla Diógenes de Aquino (Orientadora)

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Luiz Fábio Silva Paiva

Universidade Federal do Ceará (UFC)

_____

Profa. Dra. Larissa Ferreira Nunes

Centro Universitário Unifanor Wyden (UNIFANOR)

A D'us

A minha mãe e meus amigos

AGRADECIMENTOS

A jornada do meu mestrado foi atravessada por inúmeras dificuldades, da saúde às emoções, e isso apenas reforça o tamanho da gratidão que carrego por ter conseguido concluir este processo. Cheguei até aqui porque pude contar com pessoas cuja presença foi essencial para a realização deste trabalho.

Em primeiro lugar, expresso minha profunda gratidão ao Programa de Pós-Graduação em Sociologia e ao corpo docente que o compõe. Foram referências fundamentais, tanto pelo rigor intelectual que me inspirou quanto pelo acolhimento que encontrei quando, após um grave acidente de trânsito, precisei reconstruir meu ritmo e minha presença no mestrado. Em cada aula que consegui frequentar, em cada demanda que consegui cumprir, houve também a generosidade de quem entendeu meus limites temporários e apostou na minha continuidade.

Agradeço, de modo especial, a Jânia Perla Diógenes de Aquino, minha orientadora, que acreditou em mim quando eu mesmo duvidava das minhas próprias capacidades. Nos momentos em que tarefas antes simples se tornaram desafiadoras, sua paciência e sua orientação foram decisivas, não apenas para o desenvolvimento desta pesquisa, mas para que eu encontrasse minha rotina, minha confiança e meu lugar no trabalho acadêmico.

À Universidade Federal do Ceará, deixo meu reconhecimento por ter sido o solo onde me formei como pesquisador e cientista social. É uma alegria poder dizer que minha trajetória tem essa base, feita de aprendizados que me acompanharão por toda a vida.

Agradeço também ao CNPq, cuja bolsa tornou possível a dedicação necessária para a realização deste mestrado. Esse apoio foi mais do que um recurso: foi uma condição de continuidade.

E, por fim, com o mais intenso afeto, agradeço à minha família e aos meus amigos. Sem vocês, não posso afirmar que este caminho teria sido possível. Se alcancei a conclusão deste processo, foi porque encontrei em vocês o suporte mais generoso, a força que sustentou minha autoestima e acompanhou cada passo até o fim, sem desistir de mim. Esta conquista é nossa. Dedico-a a vocês.

“Um barco que veleje nesse informar, que aproveite a vazante da informaré, que leve meu e-mail até Calcutá, depois de um hot-link num site de Helsinque para abastecer” (GIL, Gilberto).

RESUMO

Esta pesquisa é essencialmente qualitativa ainda que dados quantitativos também sejam relevantes. O interesse central é investigar o que denomino dramaturgia da fraude: o conjunto de performances mobilizadas na execução de crimes cibernéticos e golpes mediados por tecnologias informacionais. O caráter dramatúrgico dessas fraudes é analisado com a teoria de Erving Goffman, com breves adaptações na medida em que as interações sociais, ainda que não ocorram de face a face, são diretas num contexto em que são mediadas digitalmente. Os relatos produzidos por interlocutores, vítimas desses crimes, surgem aqui como base. O foco recai sobre os impactos financeiros, sociais e subjetivos vivenciados pelas vítimas, ainda que os criminosos sejam os autores dessas performances. Busca-se, assim, compreender como essas narrativas revelam dimensões do letramento digital, da vulnerabilidade informacional e dos modos como a crescente imersão em tecnologias digitais, aprofundada com o isolamento social da pandemia de Covid-19, produz experiências, percepções de risco e estratégias de enfrentamento. O estudo dialoga com autores que analisam a centralidade das tecnologias informacionais na contemporaneidade, considerando tanto o aprofundamento da digitalização da vida quanto as desigualdades na capacidade de operar criticamente nesse ambiente. A partir desse referencial, discute-se como práticas fraudulentas articulam elementos performáticos, interacionais e tecnológicos, contribuindo para compreender os mecanismos sociais que permitem a emergência e a eficácia das fraudes no contexto da sociedade informacional.

Palavras-chave: crimes cibernéticos; dramaturgia da fraude; sociologia digital; letramento digital.

ABSTRACT

This research is essentially qualitative, although quantitative data is also relevant. The central interest is to investigate what I call the dramaturgy of fraud: the set of performances mobilized in the execution of cybercrimes and scams mediated by information technologies. The dramaturgical character of these frauds is analyzed using Erving Goffman's theory, with brief adaptations insofar as social interactions, although not yet face-to-face, are direct in a context where they are digitally mediated. The accounts produced by interlocutors, victims of these crimes, serve as a basis here. The focus is on the financial, social, and subjective impacts experienced by the victims, even though the criminals are the authors of these performances. Thus, we seek to understand how these narratives reveal dimensions of digital literacy, informational vulnerability, and the ways in which the increasing immersion in digital technologies, deepened by the social isolation of the Covid-19 pandemic, produces experiences, risk perceptions, and coping strategies. This study engages with authors who analyze the centrality of information technologies in contemporary society, considering both the deepening digitalization of life and the inequalities in the capacity to operate critically within this environment. Based on this framework, it discusses how fraudulent practices articulate performative, interactional, and technological elements, contributing to an understanding of the social mechanisms that allow for the emergence and effectiveness of fraud in the context of the information society.

Keywords: cybercrimes; dramaturgy of fraud; digital sociology; digital literacy.

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

> Simultaneamënte,as atividades criminosas e organizações ao estilo da máfia de todo o mundo também se tornaram globais e informacionais,propiciando os meios para o encorajamento de hiperatividade mental e desejo proibido, juntamente com toda e qualquer forma de negócio ilícito procurado por nossas sociedades.
> (Castells, 2002, p. 40)

Neste trabalho, oriento-me a partir de uma perspectiva sócio-antropológica, tendo em vista o objetivo central de investigar o que chamo de *dramaturgia da fraude*, a partir da perspectiva das vítimas em seus relatos sobre como ocorreram as tentativas fraudulentas. Busco observar alguns dos elementos ímpares que compõem os golpes/fraudes mediados por tecnologias informacionais e que visam causar dano financeiro, a partir da elaboração de composições dramáticas capazes de consolidar tais violências

Enquanto a *dramaturgia da fraude* é o foco desta pesquisa, dá-se especial atenção ao componente da dramatização, aqui compreendida como uma forma de atuação performática e aos seus efeitos, tanto subjetivos quanto materiais. Diferentemente de crimes menos complexos, esses golpes mobilizam narrativas sofisticadas e bem elaboradas conforme será observado neste texto, envolvendo desde o golpista/fraudador até as vítimas, em um enredo que busca induzir ao erro e, por fim, consolidar a fraude.

Esse tipo de crime, tipificado como estelionato no Código Penal Brasileiro (art. 171), já ocorria mesmo antes da sociedade estar imersa em mídias digitais. Consistem-se em violações que possuem o engano da vítima como estrutura central com o intuito de obter vantagem financeira indevida, como ocorre em diversas modalidades de fraude. A exemplo disso, os golpes telefônicos, seja por linhas fixas ou móveis, configuraram e configuram problemas desde antes da popularização de violências financeiras na internet, entre subtração de bens por meio de narrativas de falsos sequestros até roubo de dados pessoais e financeiros.

> Para se ter uma ideia do que a transformação digital da sociedade significa na vida da população, a edição 2025 da pesquisa Febraban de Tecnologia Bancária mostra um crescimento acentuado do volume de transações bancárias desde 2020, com predominância do ambiente virtual como principal acesso às mais de 570 milhões de contas correntes, contas de poupança e contas poupanças-social digital ativas para Pessoas Físicas e Jurídicas no país. Em 2020, a Febraban registrou um volume de 104,3 bilhões de transações bancárias, com 65,7% delas feitas por aplicativos de celulares (mobile banking) e/ou navegadores de internet (internet banking). Já em 2024, esse volume praticamente dobra, atingindo 208 bilhões de

> transações. E a participação dos canais digitais salta para 81,5%. (Anuário Brasileiro de Segurança Pública, 2025)

Desta feita, não seria a internet o primeiro meio remoto para aplicação de golpes, porém, o meio ao qual essas violências se sofisticaram frente às múltiplas margens oferecidas por esse novo conjunto crescente de plataformas, em suas possibilidades de troca de dados. Quando me refiro a isso, considero, inclusive, que o dinheiro passou a ser um dado informacional, mais do que uma cédula de papel, agora corrente em plataformas da internet como por meio de aplicativos de banco, acelerando o potencial transacional da moeda. Não à toa, em 2024, o próprio Banco Central do Brasil, já sinalizou que o Pix, meio digital para transações financeiras entre bancos sem cobranças de taxas, já ultrapassara o uso do dinheiro convencional. Paul Krugman, ganhador do Prêmio Nobel de Economia, sugere e que o PIX figure o futuro do dinheiro[1].

> No campo da segurança pública, essa transformação reconfigura por completo a governança criminal (a forma como o crime se organiza) e, no caso aqui analisado, influencia a inversão entre roubos e estelionatos e influencia a forma como o crime opera para subtrair bens e recursos de suas vítimas. (Anuário Brasileiro de Segurança Pública, 2025)

Nesse aspecto, várias plataformas de mídia jornalística demonstraram receio por meio de matérias e pesquisas que apontam o crescente número de fraudes e golpes propiciadas pelo leque de possibilidades abertas pela digitalização da moeda brasileira via PIX (Anuário Brasileiro de Segurança Pública, 2025). Portanto, longe de ser um terreno utópico ou democrático, a internet e suas ferramentas não necessariamente compõem um lugar seguro ou bem regulado. Se considerarmos que plataformas sociais vêm progressivamente aumentando nossa capacidade de comunicação e troca de dados, certamente, as violências financeiras não ficaram de fora desse processo exponencial em meio às nossas possibilidades comunicativas e transacionais.

Por falar de comunicação e transação, chego no ponto ao qual meu trabalho se destina, como demonstrado no início desta apresentação, à dramaturgia, à cena, à barganha, como formas de consolidar dano a outrem. Para tanto, esta pesquisa está organizada em 5 capítulos. Sendo o primeiro a introdução, onde apresento o

[1] Artigo Has Brazil invented the future of money? disponível em: https://paulkrugman.substack.com/p/has-brazil-invented-the-future-of?utm_source=chatgpt.com

objeto de estudo, a *dramaturgia da fraude*, com foco nas experiências das vítimas de golpes cibernéticos no Ceará pós-pandemia. Discuto a centralidade da dramatização e da performance na consolidação dos crimes, situando-os no contexto de crescente digitalização da vida cotidiana, das transações financeiras via internet e das transformações no campo da segurança pública. No segundo, entre teoria e rumos metodológicos, construo o quadro teórico-metodológico da pesquisa, compreendendo as fraudes não apenas como crimes econômicos, mas como práticas persuasivas e performativas. Articulando autores como Goffman, Foucault, Silveira e Bruno para discutir as vulnerabilidades digitais, o letramento digital e as assimetrias informacionais que ampliam o risco das vítimas. Exponho ainda a escolha metodológica pelas entrevistas em profundidade no Ceará e a relevância de pensar a pandemia de Covid-19 como catalisadora das dinâmicas digitais e criminosas. No terceiro, da conectividade ao golpe: um breve retrospecto dos avanços tecnológicos ao crime cibernético, faço um resgate histórico da evolução da internet e das tecnologias da informação, mostrando como se transformaram de instrumentos militares em infraestrutura central da vida social contemporânea. Analiso a plataformização das práticas cotidianas, o capitalismo de vigilância e a ampliação de vulnerabilidades digitais. Abordo as diferentes tipologias de crimes cibernéticos (fraudes financeiras, crimes contra a honra, privacidade, sistemas digitais, disseminação de conteúdos ilícitos e práticas transnacionais), evidenciando como a pandemia acelerou essas práticas e expôs o descompasso entre a sofisticação dos criminosos e a capacidade de resposta institucional. No quarto capítulo, fraudes em cena: vozes, performances e vulnerabilidades digitais no Ceará, início a exploração do material empírico da pesquisa, a partir de relatos de vítimas de golpes virtuais. Mostrando como os criminosos constroem performances de legitimidade que induzem ao erro, aproveitando-se das fragilidades emocionais, sociais e digitais das vítimas. O capítulo enfatiza os impactos subjetivos das fraudes e articula as experiências individuais com marcadores sociais de gênero, raça, classe e letramento digital. Além disso, discuto os limites das respostas institucionais e a persistência da insegurança digital como forma contemporânea de violência simbólica e econômica. O quinto e último capítulo é onde analiso de forma mais densa as entrevistas realizadas com as interlocuções dessa pesquisa, interpretando as narrativas dos interlocutores como material central para compreender a dramaturgia da fraude. O capítulo busca evidenciar como as

performances fraudulentas se articulam às vulnerabilidades digitais e emocionais das vítimas, sistematizando padrões de convencimento, estratégias de manipulação e sentidos atribuídos às experiências de fraude.

2 ENTRE TEORIA E RUMOS METODOLÓGICOS

As fraudes/golpes cibernéticas são compreendidas, aqui não apenas como um crime econômico, mas como um ato essencialmente persuasivo e performativo. O criminoso, ao criar identidades falsas ou situações convincentes, depende da convicção da vítima, manipulando confiança, medo ou expectativa de ganho. Nesse sentido, o delito se realiza através da influência social e psicológica, e não apenas da apropriação de recursos. Além disso, cada interação é uma encenação: perfis, mensagens e sites falsos funcionam como figurino e cenário que legitimam a ação criminosa. A vítima, ao acreditar na autenticidade da situação, participa involuntariamente dessa performance, tornando o ato um fenômeno social interpretativo. Portanto, compreender tais crimes como persuasivos e performativos permite analisar não apenas a técnica criminosa, mas também a dimensão simbólica e relacional que torna o crime possível.

A partir dessa problematização, a pesquisa busca analisar de que forma essas atuações digitais se estruturam e quais são os dispositivos simbólicos, no sentido de elementos ou práticas digitais que, por meio de seu significado social ou cultural, orientam ações e interpretações no contexto de crimes cibernéticos. e tecnológicos mobilizados na produção do engano. Em diálogo com autores como Goffman (1959), que trata da vida social como performance, e Foucault (1975), para quem o saber é correlato às relações de poder, procura-se compreender como o domínio (ou a ausência) de conhecimentos, inteligência emocional e técnica, sobre o ambiente digital configura situações de vulnerabilidade social, emocional e financeira.

Essas vulnerabilidades não se reduzem a questões técnicas: elas estão justapostas a assimetrias informacionais e políticas que organizam e afetam o digital. Nessas assimetrias, os sujeitos são interpelados por discursos, algoritmos e plataformas que encenam performances de legitimidade e engano (LINS, FREITAS, PARREIRAS, 2020). Pensar o digital exige compreender não apenas os fluxos colaborativos de informação, mas, sobretudo, os regimes de poder, vigilância e exclusão (SILVEIRA, 2003), bem como as formas de controle e simulação algorítmica que organizam o cotidiano nas redes (BRUNO, 2012).

O foco desta análise, ainda que observe a atuação dos golpistas, se dá a partir das experiências das vítimas e das formas como elas narram os acontecimentos. Parte-se do pressuposto de que os sujeitos vitimados não são receptores passivos, mas atuam, ainda que de modo inconsciente, dentro de uma trama complexa que envolve expectativas sociais, carências afetivas, confiança digital e (des)informação. A partir disso, torna-se possível explorar os sentidos mais amplos da prática criminosa como um fenômeno social e culturalmente situado.

Nesse contexto, é fundamental destacar que a noção de letramento digital adotada nesta pesquisa não se restringe a uma competência técnica ou funcional voltada ao uso de dispositivos informacionais. Trata-se, antes, de uma forma de inteligência situada, que envolve também dimensões afetivas e relacionais, especialmente aquelas mobilizadas para lidar com os riscos, expectativas e interações mediadas digitalmente. Tal concepção se alinha à perspectiva apresentada por Lins, Freitas e Parreiras (2020), segundo a qual o digital deve ser compreendido como um campo múltiplo, composto por objetos, ações e relações sociotécnicas atravessadas por marcadores sociais de classe, gênero, raça, idade e sexualidade. Assim, as habilidades digitais não podem ser compreendidas de forma homogênea ou universal, mas como práticas situadas, moldadas por contextos diversos.

O letramento digital, tal como aqui proposto, constitui uma competência que pode estar presente ou ausente independentemente do nível de escolaridade, ou da formação formal dos indivíduos. Isso porque se inscreve em um campo contemporâneo, instável e em constante transformação, que exige a articulação entre saberes técnicos e capacidades emocionais. A observação empírica realizada nesta pesquisa aponta justamente para essa complexidade: o letramento digital manifesta-se como um fenômeno relacional, que não pode ser reduzido a apenas uma dimensão (técnica ou emocional), mas deve ser compreendido como resultante da interação entre ambas, sempre atravessada pelas condições sociais e simbólicas que moldam os modos de engajamento com o digital.

Para tanto, esta investigação se apoia em entrevistas em profundidade, com roteiro semi-estruturado, realizadas com vítimas de golpes cibernéticos. As entrevistas buscam levantar questões como: quais foram os dispositivos utilizados pelo golpista? De que maneira a narrativa foi construída? Como se deu o processo de convencimento? Que sentimentos emergiram após a descoberta da fraude? As

respostas a essas perguntas ajudam a mapear as dimensões emocionais e cognitivas da experiência de ser enganado, bem como os elementos que contribuíram para atenuar o olhar crítico da vítima diante dos aspectos frágeis da performance, os quais evidenciam sua ilegitimidade.

A escolha de ancorar o estudo empírico no estado do Ceará tem duas justificativas principais. A primeira é metodológica: delimitar um campo de pesquisa viável para o escopo de um projeto de mestrado. A segunda é política e epistêmica: contribuir para a descentralização dos estudos sobre o digital no Brasil, ainda fortemente concentrados nas regiões Sul e Sudeste. Embora os crimes cibernéticos não conheçam fronteiras geográficas, o recorte territorial permite maior consistência ao observar especificidades culturais e educacionais relevantes para o fenômeno.

Esse ponto é particularmente importante, pois o Ceará, apesar de situado em uma das regiões historicamente mais vulneráveis do país, apresenta altos índices de desempenho educacional em avaliações nacionais. Isso suscita reflexões sobre como o conhecimento, ou a ausência dele, afeta diretamente a vulnerabilidade a crimes digitais. Como afirmava Foucault (1987, p. 26)

> Temos antes que admitir que o poder produz saber (e não simplesmente favorecendo-o porque o serve ou aplicando-o porque é útil); que poder e saber estão diretamente implicados; que não há relação de poder sem constituição correlata de um campo de saber, nem saber que não suponha e não constitua ao mesmo tempo relações de poder.

Além disso, permite observar o letramento digital como dissociado do desenvolvimento intelectual padrão nas formações escolares. Nesse contexto, o letramento digital configura-se como ferramenta de resistência ou, quando ausente, como vulnerabilidade explorada por agentes criminosos.

Em termos contextuais, a pandemia de covid-19 é aqui compreendida como um marco histórico que acelerou processos já em curso, especialmente no que diz respeito à virtualização da vida cotidiana e à intensificação da dependência de tecnologias informacionais. Com o isolamento social, práticas digitais se expandiram vertiginosamente, assim como as práticas criminosas que delas se aproveitam. Como destaca Barros (2022), a defasagem entre a velocidade da transformação tecnológica e a capacidade institucional de responder a ela escancara a necessidade de novos olhares críticos sobre o crime cibernético e as formas de controle social que tentam contê-lo.

Um exemplo emblemático da complexificação das práticas ilícitas no contexto contemporâneo é representado pela atuação da Polícia Federal brasileira em 2019, no âmbito da Operação Singular, amplamente noticiado por diversos periódicos[2]. Na ocasião foi desarticulada uma organização criminosa, com abrangência nacional e com organização via Deep Web[3], especializada em fraudes bancárias e outros crimes cibernéticos. A referida quadrilha operava em múltiplas frentes, incluindo estelionato, furtos qualificados, fraudes em concursos públicos, fraudes bancárias e, de maneira especialmente preocupante, o roubo e a comercialização de dados de cartões de crédito, principalmente após a invasão de bancos de dados onde são alocadas informações como estas, desde bancos digitais até aplicativos e/ou empresas para o qual o usuário cede tais informações.

A estrutura da organização contava com integrantes distribuídos por diversos estados da federação, entre eles o Ceará. Foram expedidas ordens de busca e apreensão, bem como de prisão, enquanto um dos sujeitos identificados mantém-se foragido. Não foi disponibilizado na mídia informações sobre os alvos dessa operação ao ponto de sabermos se há alguma conexão com facções criminosas. No entanto, os dados apresentados evidenciam o caráter transregional da atuação criminosa e apontam para uma crescente interconectividade nas dinâmicas ilícitas. Este caso não apenas exemplifica o grau de sofisticação alcançado por determinadas práticas delituosas no ambiente digital, principalmente se consideramos o uso da deep web como meio, como também evidencia os desafios enfrentados pelas instituições estatais no enfrentamento dessas novas configurações do crime, exigindo um constante aprimoramento tecnológico e institucional para a eficácia do controle social formal. Bem como afirma Renato Sérgio de Lima e Samyra Bueno no Anuário Brasileiro de Segurança Pública de 2023 quando os mesmos apontam como um dos principais desafios para as organizações policiais o

> crescimento acelerado do volume de trabalho relativo a estes golpes. Embora no Brasil a tipificação de fraude eletrônica seja recente, o crescimento dos crimes de estelionato (que não diferencia aqueles em meio eletrônico dos demais) ocorreu de modo exponencial durante a pandemia de Covid-19, saltando de 426.799 ocorrências no ano de 2018 para 1.819.409 em 2022. Um crescimento da ordem de 300% desafia a lógica de

[2] Disponível em: https://www.opovo.com.br/noticias/brasil/2019/06/04/pf-desarticula-grupo-responsavel-por-fraudes-bancarias-na-internet.html

[3] Parte da internet não indexada ou passível de busca via buscadores tradicionais.

> trabalho de qualquer organização, que dirá das Polícias Civis brasileiras, que há anos vem sendo sucateadas e cujos efetivos estão reduzidos e envelhecidos. (DE LIMA; BUENO, 2023, p.96)

A modernidade demandada as forças policiais exige, inclusive, a capacidade de lidar com esses crimes nas camadas mais profundas da internet como a supracitada deep web que, como apontam os cientistas da informação Vignoli e Monteiro (2020), representa

> uma camada exponente do ciberespaço que possui, na maioria das vezes, conteúdos não recuperáveis ou indexáveis pelos mecanismos de busca. O resultado da falta de indexação e posterior não recuperação da informação ocasiona uma quantidade significativa de conteúdos não transitáveis e, portanto, não acessados em todo o ciberespaço. (Vignoli; Monteiro, 2020, p. 3)

Por fim, este trabalho propõe ainda discutir os percursos jurídicos e as políticas públicas voltadas ao enfrentamento dos crimes cibernéticos, refletindo sobre os limites e potencialidades da legislação existente frente à complexidade dos delitos praticados em ambientes digitais. Nesse cenário, a educação surge como um eixo transversal: tanto como fator de prevenção quanto como forma de empoderamento dos cidadãos frente aos riscos digitais.

A partir da articulação entre narrativas de vítimas, performances fraudulentas e desigualdades no acesso ao conhecimento e às tecnologias, esta pesquisa propõe compreender os crimes cibernéticos como fenômenos sociais complexos, atravessados por linguagem, emoção, poder e manipulação. Ao focalizar a dramaturgia da fraude, entendida aqui como prática persuasiva e performática, e discutir os limites do letramento digital como forma de resistência, busco refletir não apenas sobre políticas de controle, mas sobre estratégias de enfrentamento crítico às violências simbólicas que se atualizam nas interações virtuais do cotidiano.

3 DA CONECTIVIDADE AO GOLPE: UM BREVE RETROSPECTO DOS AVANÇOS TECNOLÓGICOS AO CRIME CIBERNÉTICO

Esta seção postula uma incursão analítica, bem como um resgate histórico, sobre os caminhos entre o avanço histórico das tecnologias da informação e a constituição e possibilidade de um campo sociológico específico: o dos crimes cibernéticos. Longe de se restringirem a uma dimensão técnica ou meramente jurídica, ainda que as produções acadêmicas sobre o tema sejam fortemente concentradas nesse campo, tais crimes, aqui, devem ser compreendidos como fenômenos sociais complexos, que emergem da mesma matriz cultural e estrutural que molda nossas formas contemporâneas de interação, subjetivação e mediação simbólica. O foco recai, sobretudo, sobre a dramaturgia da fraude, não apenas como técnica, mas como performance social, e sua inserção nas novas arquiteturas digitais que caracterizam a era da informação.

A análise parte do princípio de que compreender o "estado de coisa" atual exige olhar para os processos históricos que forjaram as condições de possibilidade dos crimes cibernéticos tal como os conhecemos. A informatização progressiva das esferas da vida cotidiana, acompanhada por uma crescente virtualização das relações sociais, redefiniu tanto as noções de presença e identidade quanto as formas de controle, vigilância e transgressão. Assim, é necessário revisitar momentos-chave da história das tecnologias da informação para compreender como práticas fraudulentas se reorganizaram, se sofisticaram e se legitimaram, em alguns casos, como resposta adaptativa às lógicas do capitalismo digital (Zuboff, 2020).

Essa abordagem histórico-sociológica está em consonância com os objetivos gerais desta dissertação, que buscam interpretar os crimes cibernéticos não como desvios individuais ou anomalias tecnológicas, mas como expressões simbólicas e estruturais de tensões sociais mais amplas. A dramaturgia da fraude será, portanto, analisada como uma encenação social que revela, ao mesmo tempo, a fragilidade e a plasticidade das normas que sustentam o espaço digital contemporâneo.

Mesmo que as tecnologias informacionais já fizessem parte do cotidiano antes da pandemia de covid-19, se faz necessário situar de que maneira sua presença se intensificou e foi ressignificada socialmente. Mais do que um ponto de origem, a pandemia atuou como catalisadora de um processo anterior, expondo não apenas a funcionalidade dessas tecnologias para o consumo e a gestão da vida,

mas também suas implicações subjetivas, normativas e relacionais. A crescente naturalização do digital como meio preferencial para aquisição de bens e serviços, muitas vezes descolada de uma compreensão crítica de seus riscos, modificou práticas cotidianas de maneira acelerada, sem que os sujeitos acompanhassem, no mesmo ritmo, os saberes necessários à proteção e à agência nesse ambiente.

O distanciamento e isolamento social exigidos pela pandemia foram relevantes motivadores para reconfigurar abruptamente a forma como nos relacionamos com o tempo, o espaço e as tecnologias. Diante da urgência em manter dinâmicas econômicas, sociais e afetivas funcionando em meio ao confinamento, houve uma reorganização intensa e veloz das nossas práticas mediadas por plataformas digitais. Aquilo que era tendência tornou-se, em muitos casos, condição de sobrevivência e de manutenção da vida em sociedade. A Sociedade Brasileira de Varejo e Consumo, em pesquisa sobre novos hábitos digitais em tempos de covid-19, aponta que houve uma mudança no comportamento do consumidor e relata o aumento do consumo por meios digitais entre os entrevistados da pesquisa.

> 61% dos que já compraram por meios digitais afirmam ter aumentado suas compras online devido ao isolamento social. Esse aumento representa 50% a mais em compras online para 46% dos respondentes. Além disso, 79% compraram comida/ bebida para consumo imediato (por delivery) e também afirmam ter aumentado em 50% seus pedidos (44% dos entrevistados). (SBVC, 2020)

Compreender esse fenômeno exige um resgate histórico e conceitual dos processos que levaram àquilo que vem sendo discutido como *plataformização* da vida social (Silva, 2019) ou seja, a crescente imbricação entre a atividades humanas cotidianas e os sistemas digitais que as mediam, relações econômicas e formas de subjetivação. Trata-se de uma cultura construída nas intersecções entre práticas sociais, redes de informação e tecnologias de comunicação, na qual o online não se opõe ao offline, mas o atravessa, redefine e amplifica.

No contexto do capitalismo de vigilância, como analisa Zuboff (2019), os ambientes digitais não operam apenas como meios de interação, mas como arquiteturas de captura e modulação comportamental, estruturando a experiência social com base na extração e exploração preditiva de dados pessoais. Esse regime informacional de poder, fundado na assimetria de saberes e na invisibilidade dos mecanismos de controle, ressoa o que Foucault (1975) já diagnosticava como a

racionalidade disciplinar moderna: um modelo em que o poder se exerce pela vigilância contínua, pela normatização dos corpos e pela internalização dos dispositivos de sujeição. Nesse cenário, convivem possibilidades ampliadas de ação com formas cada vez mais sofisticadas de dominação algorítmica, desigualdade informacional e violência simbólica e material, como aquelas praticadas em golpes financeiros cibernéticos.

3.1 A ascensão do digital: percurso histórico da tecnologia informacional

A internet não surgiu com o propósito de se tornar a grande rede global de comunicação e sociabilidade que conhecemos hoje. Sua origem remonta ao final da década de 1950, como fruto de um projeto do Departamento de Defesa dos Estados Unidos da América, inicialmente voltado a fins militares e estratégias de segurança em contextos de guerra. Nesse período, sua função era eminentemente técnica e restrita a um seleto grupo de cientistas e militares. Não se vislumbrava, à época, que essa tecnologia pudesse, futuramente, penetrar o cotidiano civil e tornar-se um artefato central na vida doméstica, nas relações sociais e nos modos de subjetivação.

Com o passar dos anos, porém, o potencial da internet extrapolou o contexto bélico. A partir das décadas de 1980 e 1990, começou a ser atribuída a ela uma série de novas funções. Inicialmente, seu uso permaneceu restrito a ambientes laborais e institucionais, mas aos poucos passou a incorporar atividades de consumo, informação e lazer, como a compra de ingressos, o acesso a bancos de dados, e o recebimento de boletins informativos. Ainda que esse processo tenha se dado de maneira gradual, é possível observar, ao longo desse percurso, uma transformação da internet de instrumento estratégico-militar em meio de interação social, cultural e econômica de alcance planetário.

Esse deslocamento revela não apenas uma expansão técnica, mas também uma reconfiguração simbólica e social do papel das tecnologias em nossas vidas. Ao migrar do espaço da guerra para o cotidiano das pessoas, a internet se converteu em território de disputas, invenções, vulnerabilidades e potências, tornando-se, como argumenta Castells (1999), a espinha dorsal de uma nova estrutura social: a sociedade em rede. É reforçado por Tomaz Cerqueira quando o mesmo aborda a internet no Brasil e a concepção de humanidade nesta “globalização”.

> Se a globalização tem como lastro o fluxo de informações ao redor do globo, não podemos nos perceber como reais sujeitos dessa dita “humanidade” concebida como global. [...] No Brasil, a Internet só chega de fato nos anos de 1990, predominantemente às universidades brasileiras (Cerqueira, 2025, p. 59).

É ao final dos anos 1990 e início dos anos 2000 que a internet, acompanhada de uma série de outros avanços tecnológicos, passa a ocupar um novo e mais central lugar na sociedade. Sua presença se intensifica nas universidades, nas instituições públicas e, gradualmente, nos lares brasileiros, ampliando seu alcance e dialogando com demandas cada vez mais diversificadas da população. As máquinas computacionais, até então predominantemente associadas a contextos laborais e acadêmicos, começam a ser incorporadas ao cotidiano doméstico, assumindo funções de lazer, comunicação e mediação social.

Nesse período, observa-se a popularização dos jogos digitais, o surgimento de portais de conteúdo e entretenimento, bem como a expansão das redes sociais digitais emergentes e dos programas de troca de mensagens instantâneas, como ICQ e MSN Messenger. Simultaneamente, o e-mail passa a ocupar uma posição de destaque na vida cotidiana, substituindo práticas antes delegadas ao fax e aos correios tradicionais. Essa transição representa não apenas uma mudança nos meios, mas uma alteração significativa nos regimes de tempo e espaço que regulam a comunicação, permitindo a troca de mensagens de forma praticamente instantânea, sem as limitações impostas pela distância física.

Esse momento pode ser compreendido como uma fase de transição simbólica e técnica, na qual a internet deixa de ser uma ferramenta restrita a grupos específicos e passa a compor o tecido das interações sociais amplificadas digitalmente. Torna-se, assim, um espaço de socialidade, de subjetivação e de experimentação, inaugurando novas formas de presença, produção de sentido e articulação comunitária.

3.2 Da informação ao cotidiano: o digital como infraestrutura do presente

As teorias de Christine Hine (2015), Lins, Freitas e Parreiras (2020) entre outros autores da chamada antropologia digital, se tornam importantes para esta análise na medida que são obras muito centrais para a maneira como avaliamos o desenvolvimento das tecnologias informacionais e a cultura em ambientes virtuais. Parto da necessidade de delimitar o campo no qual se desenrola a prática analisada nesta pesquisa. Buscando investigar a internet em uma perspectiva etnográfica como a defendida por Hine (2015).

> Os etnógrafos muitas vezes se contentam em estudar contextos online ou offline. Combinar os dois exige repensar a relação entre etnografia e espaço, levando em conta a internet como cultura e artefato cultural. (tradução do autor)[4]

Desta forma, compreendendo o digital como um contexto sociotécnico incorporado à vida cotidiana, composto por relações, práticas e interações mediadas tecnologicamente, no qual sujeitos se engajam de forma situada e relacional.

Esse campo é central para este trabalho na medida em que a dramaturgia da fraude se apoia em elementos próprios das interações mediadas digitalmente, sendo a internet não apenas o meio técnico de execução dessas práticas, mas também o espaço onde se desenvolvem as normas culturais, valores e expectativas que as tornam possíveis. É nesse sentido que se utiliza o termo “meio”, adotado na apresentação desta pesquisa, como dimensão fundamental da trama, indicando um ambiente relacional, simbólico e técnico que estrutura a experiência social contemporânea.

Outra concepção importante para estudar tais fenômenos é a noção de internet como prática social, proposta por Christine Hine, que surge aqui como uma chave analítica fundamental para compreender as dinâmicas mediadas pelas tecnologias informacionais e que ocorrem via internet, cujas consequências extrapolam, em certa medida, para o mundo social material. Ao invés de entender a internet como um espaço separado da realidade, como sugeriria a filosofia da tecnologia de Pierre Levy a partir da clássica noção de ciberespaço, Hine propõe

[4] Originalmente em inglês como: Ethnographers have often settled for studying either online or offline contexts. To combine the two requires a rethinking of the relationship between ethnography and space, to take account of the Internet as both culture and cultural artefact.

abordá-la como parte integrante da vida cotidiana, simultaneamente um artefato cultural e um espaço de interação social. Assim, a internet deve ser analisada não só como tecnologia, mas como um conjunto de práticas sociais e culturais que moldam e são moldadas pela experiência dos usuários. Essa perspectiva enfatiza que o online e o offline estão interligados, permitindo compreender a internet como um campo fértil para a produção de significados, identidades e relações sociais. (HINE, 2000)

Deste modo, na análise da dramaturgia da fraude em relação ao fenômeno dos crimes cibernéticos no Ceará após a pandemia de covid-19, esses conceitos referem-se a esfera de atuação que se entrelaça de forma quase indissociável com a realidade material. Ideia reforçada por Santaella (2012, p. 229) quando afirma que “não há hoje um só setor da vida humana que não esteja mediado e permeado pelas tecnologias digitais”.

A partir dessas noções, a rede global de computadores, a internet, interconectados por meio de conexões de alta velocidade e acessível a uma multiplicidade de dispositivos distribuídos mundialmente, consolidou-se como um espaço ampliado de interação social, cuja dinâmica transcende os limites das fronteiras geográficas. Tal configuração possibilita a formação de coletividades e agrupamentos sociais articulados em torno de ideias, interesses ou características compartilhadas, reunindo sujeitos que, outrora na ausência desse meio técnico de mediação, dificilmente conseguiriam estabelecer vínculos comunicativos ou relações sociais de modo presencial. De modo que a mediação tecnológica se apresenta como condição essencial para a constituição de novas formas de sociabilidade na contemporaneidade.

Um lugar e uma cultura digitais já tinham seus desenvolvimentos desde antes disso, mas é com a maior absorção de um número maior de pessoas e de acessos que o digital vai se configurando para lidar com as novas demandas, na mesma medida que se desenvolve uma cultura digital a partir dos fatores que ali são mobilizados. Cabe ressaltar que essa cultura não é a mera transposição de uma realidade material offline para o online, o mundo digital estabelece suas próprias dinâmicas e aspectos que tem mais ou menos valor. Para Hine (2000) a internet se apresenta como um espaço em que valores e significados são continuamente produzidos e negociados nas interações cotidianas e mediadas pela rede.

As gerações que cresceram nesse período cresceram atravessadas por tecnologias digitais e com a crescente normalização dos computadores e da internet nas vidas cotidianas da população, mesmo as de classes menos abastadas.O avanço temporal tem promovido a popularização e o acesso ampliado a inovações tecnológicas, como os telefones celulares com toques polifônicos, os computadores portáteis e, mais recentemente, uma diversidade ainda maior de dispositivos. a exemplo de smartphones, tablets e notebooks. A crescente onipresença e acessibilidade dos dispositivos tecnológicos conectados à internet têm produzido transformações significativas nas dinâmicas do cotidiano social contemporâneo, atravessando distintas esferas da vida, desde formalidades burocráticas às práticas sociais, educacionais e laborais. Esse processo não apenas intensificou a integração digital dos sujeitos, como também ampliou o espectro etário dos usuários, incluindo de forma progressiva indivíduos pertencentes a gerações anteriores às revoluções da tecnologia informacional e também crianças de gerações mais recentes. Entre os grupos que adentram esse universo digital, destaca-se o contingente de pessoas idosas, que, motivadas por demandas sociais, familiares e institucionais, passaram a incorporar os aparatos digitais em sua rotina. Esse dado é reforçado pela Pesquisa Nacional por Amostra de Domicílio (PNAD Contínua) de 2024 quando a mesma aponta que o percentual de idosos que utilizam a internet subiu de 24,7%, em 2016, para 66,0% em 2023, crescimento relevante ainda que, junto com as crianças, os idosos ainda estejam entre os grupos menos presentes na internet.

> As crianças e os idosos são os grupos etários com menor percentual de pessoas que utilizaram a Internet em 2023. O grupo de 10 a 13 anos registrou 84,2%. Esse percentual cresce sucessivamente até alcançar o pico de mais de 96,3% de usuários no grupo de 25 a 29 anos. Em seguida, a proporção de usuários declina-se gradualmente até atingir 88,0% no grupo de 50 a 59 anos e depois cai para 66,0% entre os idosos (60 anos ou mais). (PNAD Contínua, 2024)

No entanto, essa imersão, ainda que exemplifique potencial e avanço em termos de inclusão sociotecnológica, evidencia também novas formas de vulnerabilidade. A familiarização parcial ou instrumental com os dispositivos, aliada à ausência de uma cultura digital consolidada, expõe esse grupo etário, em particular, a riscos ampliados no ambiente virtual, sobretudo no que diz respeito a fraudes, golpes e outras práticas ilícitas que se aproveitam de lacunas cognitivas, educacionais ou geracionais em relação ao uso crítico da internet. Manuel Castells

(2003) aponta como as desigualdades sociais também se expressam na internet e apresentam riscos e vulnerabilidades a uma parcela da população, não apenas em termos etários, mas também de acesso.

> A centralidade da Internet em muitas áreas da atividade social, econômica e política equivale a marginalidade para aqueles que não têm acesso a ela, ou têm apenas um acesso limitado, bem como para os que são incapazes de usá-la eficazmente. Assim, não surpreende que a proclamação do potencial da Internet como um meio de liberdade, produtividade e comunicação venha de par com a denúncia da "divisão digital" gerada pela desigualdade a ela associada. A diferenciação entre os que têm e os que não têm Internet acrescenta uma divisão essencial às fontes já existentes de desigualdade e exclusão social, numa interação complexa que parece aumentar a disparidade entre a promessa da Era da Informação e sua sombria realidade para muitos em todo o mundo.(CASTELLS, 2003, p. 251)

Assim, a difusão da acessibilidade tecnológica, ao mesmo tempo em que democratiza o acesso à informação e à comunicação, impõe desafios urgentes quanto à segurança digital e à proteção dos sujeitos historicamente marginalizados do letramento digital.

Dados do Módulo de Tecnologia da Informação e Comunicação (TIC) da PNAD Contínua, divulgados em 2024, apontam que, em 2023, a internet estava presente em 92,5% dos domicílios brasileiros (o equivalente a 72,5 milhões de lares). Além disso, 91,9% dos domicílios contavam com serviços de rede móvel celular, utilizados para acesso à internet ou para serviços de telefonia[5]. Tais indicadores reforçam os resultados de edições anteriores da mesma pesquisa, que já identificavam o telefone celular como o principal meio de acesso à internet no Brasil[6].

Para tanto se desenvolve um dos princípios centrais da sociedade em rede, o qual Manuel Castells denomina como espaço de fluxos, entendido como o modo pelo qual informações, conhecimentos e práticas circulam na rede, conectando diferentes atores e instituições de forma simultânea e global (CASTELLS. 1999)

Se opondo a ideia de que o conhecimento só é legítimo se vem de determinados espaços partindo da ideia de que ninguém sabe tudo e todos sabem

[5] Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41024-internet-foi-acessada-em-72-5-milhoes-de-domicilios-do-pais-em-2023

[6] Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/celular-e-o-principal-meio-de-acesso-internet-no-pais

algo. No entanto cabe ressaltar que o desenvolvimento das tecnologias digitais ocorreu de forma exponencial em um curto período de tempo, a tecnologia utilizada após 2010 sequer é parecida com o que ocorria no início dos anos 2000.

Processos de digitalização da economia vão ocorrer nesse período com uma maior exposição e possibilidades de atividades financeiras e econômicas através da internet, instituições como bancos ingressam nesse mundo e outras instituições financeiras como lojas e operadoras de cartão também, assim como empresas que se valem desses dados para efetuar pagamentos e assinaturas de serviços. Nesse período de maior imersão numa economia digital há grande concentração de dados em aparelhos digitais para efetuar transações.

Os cartões de crédito podem ser “instalados” nos telefones celulares para que estes funcionem por aproximação; o PIX e demais transações bancárias podem ser feitas através de aplicativos de internet banking; e existem até cartões de crédito unicamente digitais, que podem ser usado para comprar via plataformas de e-commerce[7] e também para assinar serviços que demandam um pagamento mensal. Ao mesmo passo há uma imersão das redes sociais digitais na dinâmica social do mundo material e trabalhista, assim como uma imersão desse mundo material nas redes digitais. Ambos os mundos, apesar de dinâmicas diferentes, se tornam cada vez mais indissociáveis, ainda que o mesmo indivíduo tenha comportamentos distintos para cada ambiente e suas dinâmicas.

Esse fenômeno se expressa de distintas formas na vida social contemporânea. De um lado, observa-se a deterioração das condições do mercado de trabalho, especialmente em experiências vinculadas à chamada economia de plataforma, como é o caso da Uber, iFood e outras empresas semelhantes, que promovem uma ficção de autonomia laboral, ao passo que não asseguram aos trabalhadores os direitos sociais e trabalhistas previstos legalmente, contribuindo para a informalização e precarização das relações de trabalho.

Por outro lado, nota-se também a facilitação de determinados processos burocráticos e administrativos mediante a digitalização de serviços públicos. Um exemplo disso é o portal gov.br, mantido pelo Governo Federal, que reúne uma ampla gama de funcionalidades e serviços destinados aos cidadãos, abrangendo desde o acesso a documentos oficiais básicos até a inscrição em exames nacionais

[7] Abreviação de electronic commerce que, em português, significa comércio eletrônico.

e a integração com sistemas como o Sistema Único de Saúde (SUS). Trata-se, portanto, de um cenário ambivalente, no qual as tecnologias digitais operam tanto como instrumentos de exclusão e flexibilização dos direitos quanto como ferramentas de acesso e racionalização administrativa.

Entre os anos de 2010 e 2019 (anterior a pandemia de covid-19), já se observava uma crescente digitalização de serviços no Brasil, principalmente nos últimos anos anteriores a pandemia. Mesmo por parte do Governo Federal, já se buscava a agilidade na digitalização de serviços, tendo tornado em 2019, 311 serviços públicos 100% digitais[8], e anunciado, após os anos de isolamento social em 2023, que já contavam com 90% dos serviços públicos digitalizados[9]. Diversas operações passaram a ser mediadas pela internet, com destaque para a consolidação de contas bancárias digitais e o surgimento de instituições financeiras totalmente virtuais. Cartões de crédito passaram a ser ofertados por agências digitais, e o comércio eletrônico expandiu-se significativamente, permitindo não apenas a compra de ingressos para eventos, mas também a realização de reservas em restaurantes, aquisição de livros, alimentos, medicamentos e uma ampla gama de bens e serviços. Tal transformação se deve, também, ao efeito da suspensão de diversos setores na pandemia de covid-19 que, como afirma a Sociedade Brasileira de Varejo e Consumo (2020), “fez com que muitas empresas buscassem canais digitais para minimizar os efeitos negativos nas vendas”. O comércio eletrônico vem crescendo desde 2016 chegando a marcar em 2023 a movimentação de R$ 196,1 bilhões de reais. Considerando a relevância do tema, o Governo Federal, através do Ministério do Desenvolvimento, Indústria, Comércio e Serviços lançou o Observatório do Comércio Eletrônico Nacional, como uma plataforma de monitoramento do comércio eletrônico brasileiro. Com uma série histórica desde 2016, esta é a evolução por ano apresentada pelo observatório.

---

[8] Disponível em: https://apolitical.co/solution-articles/pt/scaling-digital-how-brazil-is-rewiring-government?utm

[9] Disponível em: https://www.gov.br/governodigital/pt-br/noticias/gov-br-alcanca-90-dos-servicos-publicos-digitalizados#:~:text=O%20m%C3%AAs%20de%20maio%20j%C3%A1,4.181%20j%C3%A1%20s%C3%A3o%20digitais.

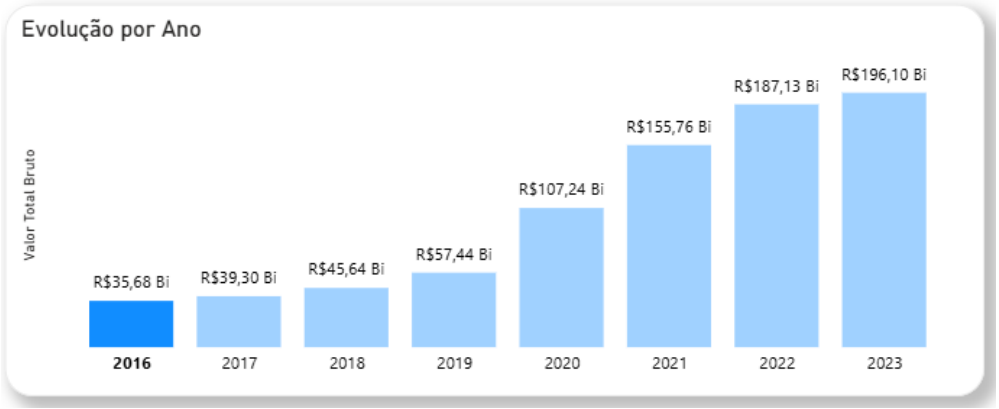

Gráfico de Evolução por ano das movimentações de recursos via comércio eletrônico no Brasil publicados pelo Observatório do Comércio Eletrônico Nacional[10].

Com o aprofundamento da pandemia de covid-19 em 2020 e a consequente imposição de medidas de isolamento social, os processos digitais anteriormente em curso foram aprofundados e acelerados. A necessidade de permanecer em casa impulsionou a utilização massiva de plataformas digitais para atender às demandas cotidianas, desde as mais triviais até aquelas consideradas essenciais. Aplicativos de transporte, entrega de alimentos, remédios, livros e produtos de supermercado tornaram-se fundamentalmente adquiridos via e-commerce.Além disso, observa-se o surgimento de novas formas de ocupações informais, notadamente aquelas mediadas por plataformas digitais, nas quais trabalhadores passaram a desempenhar atividades de entrega diretamente nas residências dos consumidores. Esse fenômeno se manifesta de forma evidente em aplicativos como Uber, 99Pop, iFood, Rappi, entre outros. Dentre essas plataformas, destaca-se de maneira emblemática a Uber, que não apenas assumiu um papel central nesse processo de plataformização do trabalho, como também forneceu o referencial conceitual para o que se convencionou chamar de "uberização" (Antunes, 2020), um trabalho que representa uma nova forma de subordinação, mediada por plataformas digitais, que oculta a relação de dependência sob a aparência de trabalho autônomo.

O setor bancário, por sua vez, intensificou a digitalização de seus serviços, com a ampliação do uso do internet banking. Em resposta às novas exigências da sociedade digitalizada, o governo brasileiro lançou o sistema de transferências

[10] Disponível em: https://app.powerbi.com/view?r=eyJrIjoiZWFmOWUzNzItMDEyYy00MzcxLTk1NzYtNzIxMDRlMDAxOTk1IiwidCI6IjNlYzkyOTY5LTVhNTEtNGYxOC04YWM5LWVmOThmYmFmYTk3OCJ9

instantâneas denominado PIX, que permite transações financeiras imediatas e simplificadas, com poucos cliques.

Esse processo de digitalização, embora tenha proporcionado significativa facilitação das atividades cotidianas, também abriu espaço para o surgimento e a sofisticação de novas práticas delituosas no ambiente virtual. Como aponta Barros (2022), há uma evidente discrepância entre a atualização das dinâmicas do crime cibernético e a resposta das instituições políticas e governamentais em termos de velocidade, na medida em que se compreende

> a distância entre os avanços tecnológicos sociais-digitais e a incorporação de suas dinâmicas em nossos sistema jurídico, tornando com que crimes virtuais se configurem como uma categoria de crime proeminente na sociedade contemporânea, uma vez que seu primeiro obstáculo para a justiça é a identificação de suas práticas e ordenamentos, já que se atualizam e se desenvolvem constantemente, e possuem ferramentas que ampliam sua gama de atuação, pois se baseiam, primordialmente na identificação das falhas de outros sistemas. (Barros, 2022, p. 39)

. As legislações e os aparatos estatais, muitas vezes ancorados em normativas obsoletas, não conseguem abarcar a complexidade das novas formas de crime, sendo frequentemente ineficazes diante de atividades ilícitas ainda não formalmente reconhecidas como tais, embora provoquem danos reais às vítimas.

Nesse contexto, observa-se que o crime cibernético evolui em consonância com o avanço tecnológico e com as inovações nos meios de transação digital da sociedade civil, desenvolvendo-se em uma velocidade superior à da legislação e das estruturas institucionais de controle. A aceleração tecnológica, catalisada pela pandemia, proporcionou um terreno fértil para a reinvenção das práticas criminosas, enquanto o aparato estatal permanece em ritmo lento diante das novas exigências da realidade digital contemporânea.

3.3 Cibercriminalidade: Novos Desafios para a Sociedade Contemporânea

No que se refere aos crimes cibernéticos, cabe ressaltar que tais fenômenos digitais não podem ser compreendidos apenas como simples transposições ou extensões do mundo material para o ambiente online. Trata-se, antes, da constituição de novas lógicas de interação, produção e ação social, que reconfiguram profundamente as relações humanas, institucionais e econômicas. O digital não replica o mundo físico, mas instaura um novo regime de significação, circulação de saberes, práticas e experiências, inaugurando modalidades inéditas de sociabilidade, subjetivação e poder.

Diante da complexidade e contemporaneidade do tema, o campo de estudos sobre os fenômenos digitais exige uma abordagem interdisciplinar. Assim, esta pesquisa transita por referenciais da antropologia, da sociologia, do direito, da filosofia e das ciências da computação, áreas que têm produzido investigações teóricas e empíricas mais densas sobre os impactos das tecnologias digitais nas estruturas sociais e nas formas de vida.

Entre os autores de referência nesse campo, destaca-se Manuel Castells, cuja obra sobre a sociedade em rede e a era da informação contribui significativamente para a compreensão das transformações provocadas pela internet nas dinâmicas globais. Castells (1999) discute o surgimento de uma nova morfologia social, a qual chama de sociedade informacional, caracterizada pela centralidade do conhecimento, da comunicação em tempo real e da reconfiguração das relações espaciais e temporais. Suas análises problematizam os efeitos de uma suposta globalização, revelando como as tecnologias digitais participam da produção de desigualdades, mas também da criação de novos territórios de resistência e participação.

Portanto, compreender os fenômenos digitais demanda mais do que uma análise técnica ou instrumental: requer o reconhecimento de que estamos diante de um novo paradigma cultural e sociotécnico, que exige categorias próprias para sua análise e problematização.

. Acredito ser necessário também abordar a questão da cibersegurança, meios de proteção contra crimes cibernéticos que não se reduzem aos ofertados

pela legislação e jurisprudência das instituições públicas, mas apresentam também métodos de segurança, campanhas de conscientização e de combate às novas formas de crime.

E que, com a aceleração de processos de digitalização consolidou-se um ecossistema digital que passou a operar como infraestrutura central da vida social contemporânea. Nesse contexto, observa-se um aprofundamento das práticas sociotécnicas, acompanhadas, simultaneamente, por transformações nos modos de atuação de agentes criminosos. O crime cibernético, em especial, passou a se atualizar em ritmo vertiginoso, explorando as brechas tecnológicas e sociais emergentes com agilidade e sofisticação. Em contrapartida, os sistemas legais e institucionais demonstraram capacidade limitada de resposta, mantendo-se em um ritmo de ação inferior e com reduzido potencial de acompanhar as novas configurações dos crimes cibernéticos ou virtuais.

Esse descompasso, que evidencia a assimetria entre a velocidade das inovações tecnológicas e a capacidade regulatória do Estado, traz como consequência um cenário de vulnerabilidade, em que os sujeitos estão expostos a riscos crescentes sem a devida proteção institucional ou legal adequada à complexidade do ambiente digital contemporâneo.

A 14° edição da Allianz Risk Barometer (Barômetro de Riscos da Allianz) identifica em 2025[11], pelo quarto ano consecutivo, os crimes cibernéticos como principal preocupação entre as empresas e os empresários em 106 países. Conforme a pesquisa, os crimes cibernéticos não só ocupam esse lugar numa perspectiva global como também lideram as preocupações entre empresas brasileiras.

Na medida em que observamos o avanço das tecnologias informacionais e a imersão de nossas vidas cotidianas no mundo virtual, a formação de grupos criminosos para realizar ilicitudes através da internet têm se tornado mais comuns, bem como outras atuações criminosas mediadas por tecnologias. O dado apresentado não só menciona a preocupação de abrangência internacional, mas

[11] Disponível em: https://www.opovo.com.br/noticias/brasil/2025/01/23/crimes-ciberneticos-preocupam-empresas-em-106-paises.html

também expõe a vulnerabilidade característica da contemporaneidade, em termos de exposição de dados, dos processos mediados por plataformas digitais. Os aspectos do avanço tecnológico que trouxeram mais praticidade para nossas vidas, enquanto cidadãos e pessoas atravessadas pelas dinâmicas institucionais e sociais das sociedades em que vivemos, também foram e são explorados por grupos e pessoas intencionadas a lesar as vítimas de diversas formas, seja financeiramente ou em outras modalidades de crime como racismo, LGBTfobia, pornografia de vingança, entre outros.

3.3.1 Crimes Cibernéticos: Tipologias e Abordagens Sociológicas Preliminares

A problemática acerca dos crimes executados mediante o uso das tecnologias informacionais e digitais tem sido objeto de investigação em diversas áreas do saber, resultando em uma pluralidade de designações e conceituações, tais como “crimes virtuais”, “delitos informáticos”, “infrações cibernéticas” e “crimes informacionais”. Cada uma dessas nomenclaturas carrega consigo determinadas inflexões teóricas e pressupostos epistemológicos que refletem diferentes compreensões sobre os impactos sociotécnicos e normativos dessas práticas. No entanto, este trabalho não tem como propósito aprofundar-se nas disputas terminológicas ou delimitações conceituais exaustivas entre essas categorias.

Para os fins analíticos desta dissertação, adoto os termos “crime virtual” e “crime cibernético” de maneira intercambiável, compreendendo que ambos estabelecem um diálogo suficientemente exitoso com o arcabouço teórico mobilizado. Trata-se, portanto, de uma escolha pragmática, orientada pela fluidez e pela adequação aos objetivos centrais deste estudo: investigar as práticas ilícitas mediadas por dispositivos digitais à luz de suas representações simbólicas e efeitos socioculturais, com ênfase na dramaturgia da fraude como fenômeno social.

Visando oferecer ao leitor um panorama introdutório que permita a apreensão das dimensões simbólicas e estruturais dos crimes virtuais, elencarei, a seguir, algumas tipologias centrais que configuram o atual campo dos crimes cibernéticos. Embora tal sistematização não esgote a complexidade do fenômeno, ela constitui

um suporte analítico relevante para a compreensão das dinâmicas contemporâneas de poder, dominação, exclusão e resistência articuladas nos espaços digitais.

Crimes Contra o Patrimônio Digital

Os crimes contra o patrimônio digital configuram-se como práticas ilícitas orientadas à obtenção de vantagens indevidas por meio da apropriação de bens intangíveis, como dados pessoais, credenciais, ativos financeiros digitais e outros elementos de valor patrimonial. Tais práticas manifestam-se em modalidades como fraudes bancárias online, phishing, roubo de cartões de crédito e ransomware.

As fraudes bancárias online consistem em quaisquer meios usados com a finalidade de acessar indevidamente os recursos e possibilidades de uma conta bancária através da internet. A Lei nº 14.155/2021, ao alterar o Código Penal Brasileiro, tipifica uma recorrente fraude bancária, o estelionato eletrônico, caracterizando-o como o ato de induzir a vítima a erro por meio de dispositivos informáticos, com vistas à obtenção de vantagem ilícita. Trata-se de uma atualização normativa que busca acompanhar as mutações das práticas fraudulentas na sociedade digitalizada.

O *phishing*, por sua vez, consiste na criação de cenários digitais fraudulentos, como sites falsos ou e-mails enganosos, destinados à captura de dados sensíveis da vítima, configurando uma simulação tecnológica da confiança como mecanismo de violência simbólica (BOURDIEU, 1998).

O *ransomware* representa uma forma contemporânea de extorsão, na qual o agente criminoso bloqueia o acesso a sistemas e dados mediante criptografia, exigindo resgate financeiro para a sua liberação. Tal prática revela as novas formas de sequestro simbólico e dependência tecnológica características da sociedade da informação (CASTELLS, 2003).

Crimes Contra a Honra e a Dignidade no Ciberespaço

No plano das interações simbólicas, os crimes contra a honra e a dignidade (como calúnia, difamação, injúria, cyberbullying, *revenge porn* e *stalking* digital) mobilizam dinâmicas específicas de humilhação pública e exposição indevida,

atualizando dispositivos clássicos da violência simbólica em ambientes de visibilidade ampliada.

O ambiente digital potencializa essas práticas, conferindo-lhes alcance, anonimato e permanência. A difamação e a calúnia, práticas historicamente normatizadas no direito penal, adquirem novas camadas de complexidade quando realizadas por meio das redes digitais. A injúria online, por sua vez, tem implicações psicológicas intensificadas pela constante circulação e arquivamento dos conteúdos ofensivos (LEVY, 1999).

O *cyberbullying* e o *revenge porn* devem, também, ser compreendidos à luz das violências estruturais de gênero e sexualidade, que se reconfiguram no espaço virtual. Segundo Hine (2015), a virtualização da violência de gênero, ou de qualqur fenômeno, não elimina suas raízes materiais, mas as rearticula, intensificando seus efeitos simbólicos e subjetivos. Essas violências se expressam tanto no ataque recorrente e elaborado via virtual (cyberbullying) como na exposição de conteúdo intímo nas mídias digitais (revenge porn).

Crimes Contra a Privacidade e Proteção de Dados

Com o advento do capitalismo de vigilância (ZUBOFF, 2020), os crimes contra a privacidade tornaram-se um dos principais vetores de conflito ético, político e jurídico nas sociedades contemporâneas. O vazamento de dados pessoais, a espionagem eletrônica, a interceptação de comunicações privadas e a comercialização ilícita de bancos de dados são práticas que tensionam os limites entre o público e o privado na era digital.

A violação da privacidade, nesse contexto, não constitui apenas um crime individual, mas uma forma de dominação estrutural articulada à lógica extrativista dos dados.

Crimes Contra Sistemas e Infraestruturas Digitais

Crimes como ataques DDoS (Distributed Denial of Service), invasões de servidores, *defacement* de páginas institucionais e sabotagem cibernética visam a

disrupção e o comprometimento de sistemas informacionais estratégicos, sejam eles públicos ou privados.

A sabotagem cibernética, em particular, pode ser definida como o ato intencional de danificar ou inutilizar recursos tecnológicos com objetivos políticos, econômicos ou bélicos, muitas vezes associados à lógica do *hacktivismo* ou ao ciberterrorismo estatal e paraestatal (DUNN CAVELTY, 2014). Trata-se de um fenômeno que evidencia a vulnerabilidade da infraestrutura digital frente a conflitos geopolíticos e interesses corporativos.

Crimes de Conteúdo e Propagação Ideológica

A disseminação de discursos de ódio, apologia ao crime, pornografia infantil e *fake news* constitui uma dimensão simbólica dos crimes cibernéticos, em que a violência opera por meio da linguagem e da informação. Nesse campo, o conteúdo digital torna-se um vetor de legitimação da violência e da exclusão social.

A produção e circulação de *fake news*, por exemplo, integram um ecossistema de desinformação que atinge diretamente os processos democráticos e os vínculos de confiança social.

Crimes Organizados e Transnacionais

Por fim, destaca-se o uso das tecnologias digitais por organizações criminosas transnacionais para práticas como tráfico de drogas e armas, lavagem de dinheiro (via criptomoedas), exploração sexual e terrorismo digital. A *dark web* emerge como um território paralelo, regulado por normas próprias e acessível apenas por usuários com conhecimento técnico específico.

> I believe that cyberspace is not an empty vessel or neutral channel. How it is structured matters for identity, human rights, security, and governance … and we need to tend to it to preserve it as a secure and open commons. (DEIBERT, 2013, p. 13)[12]

[12] Acredito que o ciberespaço não é um recipiente vazio ou um canal neutro. A forma como ele é estruturado importa para a identidade, os direitos humanos, a segurança e a governança... e precisamos cuidar dele para preservá-lo como um bem comum seguro e aberto.(Tradução livre)

Essas práticas reiteram que o ciberespaço não constitui uma esfera neutra, mas sim um campo de disputa e reprodução das assimetrias globais de poder (DEIBERT, 2013). O uso de criptomoedas para fins ilícitos, por exemplo, representa uma reconfiguração das práticas financeiras da criminalidade organizada, conferindo-lhes anonimato, transnacionalidade e autonomia em relação ao sistema bancário tradicional.

Em síntese, o percurso reconstruído neste capítulo evidencia que a ascensão do digital não resultou apenas na ampliação de possibilidades técnicas, mas na inauguração de uma gramática sociocultural inédita — uma ecologia de interações em que a dramaturgia da fraude se torna sintoma privilegiado das tensões estruturais do capitalismo de plataforma. Ao revisitar momentos-chave da história das tecnologias informacionais, demonstramos como a expansão da conectividade desdobrou-se em novas arquiteturas de vulnerabilidade, nas quais a velocidade dos crimes cibernéticos supera, de forma sistemática, a capacidade regulatória e pedagógica das instituições. A pandemia de covid-19 figurou como catalisador dessa inflexão, aprofundando tanto a dependência cotidiana dos dispositivos quanto o alcance transnacional das práticas ilícitas. Assim, os crimes cibernéticos emergem não como desvios periféricos, mas como fenômenos centrais que revelam o entrecruzamento de desigualdades sociais, lógicas de mercado extrativistas e lacunas de alfabetização digital. Reconhecer essa ambivalência — a de um ciberespaço simultaneamente emancipador e capturador — é condição para que, nos próximos capítulos, possamos discutir estratégias normativas, educativas e tecnopolíticas capazes de reequilibrar a balança entre inovação e justiça social, convertendo a inteligência coletiva em potência crítica e não em recurso explorável pelos novos empreendedores da fraude.

4 FRAUDES EM CENA: VOZES, PERFORMANCES E VULNERABILIDADES DIGITAIS NO CEARÁ

O aparelho celular provisório e mais simples gerava tensão cada vez que vibrava, como se cada notificação fosse um fio de esperança. Cláudia[13] atravessada por grande tensão, ainda estava processando o assalto que havia sofrido dias antes. Então surge, no canto da tela, uma nova mensagem: “Apple Suporte - Localize seu aparelho”. Ao abrir a conversa encontrou uma linguagem formal e um tom urgente, mas tranquilizador. “Confirme seus dados para que possamos ajudá-la a recuperar seu dispositivo”, dizia o texto, seguido de um link que levava a uma página impecável, com o logo da maçã prateada,

Naquele instante, o aparelho não se reduzia a um mero objeto, mas sim um smartphone repleto de memórias vivas, desde fotos, conversas, senhas, documentos de trabalho à acessos a contas bancárias e aplicativos de vendas. Tudo isso fazia com que tal objeto não pudesse ser apenas um bem material, mas uma extensão de sua própria vida digital. Inquieta e com as mãos trêmulas, ela entrou na sua conta apple através do link enviado via whatsapp. nome, senhas, e-mail, tudo parecia legítimo. Tudo parecia seguro. Mas não era.

No silêncio que se seguiu, a ação de clicar para “iniciar sessão” foi também o som da consolidação de uma armadilha invisível. Apenas horas depois percebeu que, junto com o telefone levado no assalto, havia perdido também o controle sobre sua identidade digital. A função de rastreamento do aparelho foi desativada. A esperança se desfez em frações de código. Seu erro? Acreditar no que parecia real.

É através de histórias como essa, coletadas a partir das interlocuções dessa pesquisa que esse capítulo se debruça, ainda mais tendo em vista o quanto cresceram os golpes virtuais nos últimos anos (BRASIL, 2024). A busca aqui é para examinar a dimensão empírica dos crimes cibernéticos no estado do Ceará com base em experiências reais. São igualmente abordados os aspectos metodológicos do trabalho de campo realizado, onde se destaca a adoção de uma perspectiva mista, mesclando os dados de ordem qualitativa como as entrevistas com vítimas de crimes cibernéticos, a observações das práticas digitais ao uso de dados

[13] Nome fictício para proteger a identidade da interlocutora

estatísticos provenientes de fontes oficiais e institucionais. Dando enfoque especial aos relatos e experiências.

A análise dialoga diretamente com as tipologias de fraudes previamente apresentadas, às examinando à luz dos referenciais teóricos e recursos analíticos que sustentam esta pesquisa. As narrativas individuais das vítimas são mobilizadas para evidenciar os impactos subjetivos das fraudes, bem como para revelar vulnerabilidades sociais profundamente atravessadas por marcadores de gênero, raça, classe e letramento digital.

Considerando que o uso cotidiano da internet e das redes digitais atravessa uma diversidade cada vez maior de campos e está presente em uma parcela mais significativa da população, somado ao crescimento exponencial dos crimes cibernéticos, tanto em termos da quantidade de tipos de crime quanto do volume de golpes realizados, especialmente em territórios marcados por elevada densidade digital, este capítulo promove uma reflexão crítica sobre as limitações das respostas institucionais diante dessas dinâmicas, sejam elas de ordem pública ou privada. Além disso, levanta hipóteses acerca da persistência da insegurança digital enquanto forma contemporânea de violência simbólica e econômica.

Antes de abordarmos alguns percursos metodológicos relacionados à coleta de dados e à realização das entrevistas, bem como explorarmos os casos relatados, considero importante informar previamente de que maneira as referências bibliográficas que norteiam esta análise são mobilizadas e adequadas para o fenômeno em questão. Isso se faz especialmente relevante diante da recorrência e contemporaneidade dos crimes cibernéticos, e do fato de que parte das referências utilizadas precedem as grandes revoluções informacionais, não tratando diretamente de fenômenos virtuais ou digitais.

4.1 Palcos digitais e encenações do engano: a dramaturgia social dos golpes virtuais

> A cultura da Internet é a cultura dos criadores da Internet. Por cultura entendo um conjunto de valores e crenças que formam o comportamento; padrões repetitivos de comportamento geram costumes que são repetidos por instituições, bem como por organizações sociais informais. Cultura é diferente de ideologia, psicologia ou representações individuais. Embora explícita, a cultura é uma construção coletiva que transcende preferências individuais, ao mesmo tempo em que influencia as práticas das pessoas no seu âmbito, neste caso os produtores/usuários da Internet. (CASTELLS, 2006, p. 41)

Ao refletir sobre a *dramaturgia da fraude no mundo virtual, na internet*, observo os fatores e elementos cruciais que contribuem para a construção de uma atuação persuasiva, capaz de conferir credibilidade à encenação criminosa e, assim, induzir a vítima ao erro. Reconheço que a criminalidade cibernética pode manifestar-se em diversas esferas, contudo, o foco inicial desta análise, além de considerar as transformações nos crimes decorrentes do avanço dos serviços digitais, recai sobre a performance dramatúrgica de indivíduos ou grupos criminosos que se fazem passar por empresas ou instituições oficiais, ou atribuem a si confiabilidade enquanto sujeitos que propõem uma transação financeira. Estes buscam conferir aparência de legitimidade às suas ações, com o intuito de induzir a vítima a fornecer voluntariamente dados sensíveis, o que possibilita a violação de seus bens financeiros. Para tanto, exploram inseguranças, medos e circunstâncias específicas que colocam o indivíduo em estado de alerta ou tensão, dificultando a identificação de falhas ou sinais que poderiam revelar a ilegitimidade da ação.

> Venho usando o termo “representação” para me referir a toda atividade de um indivíduo que se passa num período caracterizado por sua presença contínua diante de um grupo particular de observadores e que tem sobre estes alguma influência. (...) a parte do desempenho do indivíduo que funciona regularmente de forma geral e fixa com o fim de definir a situação para os que observam a representação. (GOFFMAN, 1975, .p. 29)

Ao analisar essa dinâmica, sob uma perspectiva sociológica, é possível compreender a *dramaturgia da fraude* como uma manifestação concreta das relações de poder e confiança que estruturam o universo digital contemporâneo. A fraude cibernética, ao mimetizar instituições legítimas, apropria-se de uma lógica performativa sustentada por normas sociais de credibilidade e autoridade, criando uma aparência de legitimidade que induz ao erro. Inspirando-se na teoria da teatralidade da vida social, de Erving Goffman, pode-se afirmar que os agentes

fraudulentos constroem um *front stage*[14] cuidadosamente elaborado, mobilizando signos simbólicos, como logotipos institucionais, identidades visuais e discursos formais, com o intuito de manipular a percepção da vítima e instaurar uma ilusão de veracidade.

Ao interpretar esses fenômenos a partir de uma perspectiva bourdieusiana, torna-se possível compreender a atuação do que Pierre Bourdieu denomina *poder simbólico* como um elemento estruturante das "cenas" fraudulentas. Essas performances digitais operam por meio da manipulação de signos de autoridade socialmente consagrados, os quais funcionam como vetores de uma violência simbólica, entendida como uma forma de dominação que se exerce de modo sutil, mas eficaz, por meio do reconhecimento e da internalização das classificações impostas.

Essas fraudes não são meramente transgressões técnicas ou desvios pontuais, mas sim expressões de um poder que se efetiva precisamente porque permanece invisível aos olhos daqueles que o sofrem. Trata-se de um processo em que os indivíduos, muitas vezes inconscientes de sua posição subalterna, acabam por consentir com a lógica da dominação simbólica, reconhecendo como legítimos os signos que os enganam. Como afirma Bourdieu,

> o poder simbólico é, com efeito, esse poder invisível que só pode ser exercido com a cumplicidade daqueles que não querem saber que lhe estão sujeitos ou mesmo que o exercem" (BOURDIEU, 1989, p. 7-8).

O fenômeno da fraude, portanto, não se restringe às ferramentas tecnológicas empregadas, mas reflete uma complexa interação entre estruturas sociais de confiança, vulnerabilidade e o crescente processo de intermediação digital das relações cotidianas. As performances fraudulentas, nesse sentido, expõem as fragilidades dos sistemas contemporâneos de credibilidade, especialmente em um contexto marcado pela virtualização acelerada das interações humanas.

> Quando um indivíduo apresenta um papel, implicitamente solicita de seus observadores que levem a sério a impressão sustentada perante eles. Pede-lhes para acreditarem que o personagem que vêem no momento

[14] "Front stage" é o espaço onde o indivíduo se apresenta formalmente diante de uma audiência, seguindo normas sociais, expectativas de conduta e um 'roteiro' que visa construir e manter uma determinada impressão.

> possui os atributos que aparenta possuir, que o papel que representa terá as consequências implicitamente pretendidas por ele e que, de um modo geral, as coisas são o que parecem ser. (GOFFMAN, 1975, p. 29)

Ao propor uma leitura da criminalidade cibernética a partir da sociologia de Erving Goffman, é necessário re-elaborar e atualizar alguns aspectos centrais de sua teoria dramatúrgica, tendo em vista as especificidades das interações sociais em ambientes digitais. Em primeiro lugar, é preciso reconhecer que também nas redes sociais digitais e nas plataformas online há um caráter performativo nas interações, ainda que estas não se deem no formato tradicional de contato face a face, como originalmente concebido por Goffman.

Nas práticas criminosas mediadas por tecnologias digitais, é possível considerar as comunicações mediadas por computador (CMC) como formas de "contato imediato", uma vez que, embora não se deem de maneira presencial, possibilitam interações em tempo real, frequentemente diretas e contínuas e a construção de uma fachada, definida por Goffman como

> *a parte do desempenho do indivíduo que funciona regularmente de forma geral e fixa com o fim de definir a situação para os que observam a representação. Fachada, portanto, é o equipamento expressivo de tipo padronizado intencional ou inconscientemente empregado pelo indivíduo durante sua representação"* (GOFFMAN, 1975, p. 29)

. Nesse contexto, conforme argumenta Bourdieu (1989), o discurso exerce um papel central na dinâmica do poder simbólico, constituindo um instrumento privilegiado na imposição de significados e na legitimação de relações de dominação. Assim, essas formas de comunicação digital tornam-se terreno fértil para a consolidação de fraudes cibernéticas enquanto expressões de violências simbólicas, operando por meio da manipulação estratégica da linguagem e de signos de autoridade socialmente reconhecidos.

> Os sistemas simbólicos são instrumentos estruturados e estruturantes de comunicação e de conhecimento que cumprem a sua função política de instrumentos de imposição ou de legitimação da dominação, que contribuem para assegurar a dominação de uma classe sobre outra (violência simbólica), dando o reforço da sua própria força às relações de força que as fundamentam, contribuindo assim para a submissão inconsciente dos dominados. (BOURDIEU, 1989, p. 11)

Essa transposição teórica exige o reconhecimento de que a ausência da co-presença física não elimina a performatividade; ao contrário, a intensifica por

meio da manipulação de signos, linguagens e códigos visuais próprios do ambiente digital.

Nesse cenário, torna-se necessário revisitar a distinção feita por Goffman entre *expressões de transmissão* (intencionais, controladas) e *expressões de emissão* (involuntárias, espontâneas). No ambiente digital, as expressões de emissão, que no contato físico estariam ligadas a gestos, posturas, entonações ou microexpressões, assumem novas formas. Elas não derivam do corpo, mas do *equipamento estético, gráfico e processual* que compõe a interface de interação: o design de um site falso, o uso de logotipos institucionais, a adoção de uma linguagem formal, entre outros elementos que compõem a encenação da legitimidade.

A fraude virtual, portanto, não se limita à apropriação indevida de dados ou à obtenção ilícita de recursos financeiros, mas também se materializa como uma performance cuidadosamente planejada. O fraudador digital encena um papel, construindo um "front stage" virtual a partir da manipulação estratégica do discurso, da linguagem visual e dos códigos de autoridade institucional ou de cidadão confiável, com o objetivo de provocar na vítima uma falsa sensação de segurança, veracidade e confiança.

Ao compreendermos essas práticas à luz de uma reformulação da teoria goffmaniana somado a compreensão dos sistemas simbólicos segundo Bourdieu podemos ampliar nossa noção de performance social para além dos limites do corpo físico e da presença co-localizada. Trata-se, assim, de reconhecer que a dramaturgia da fraude no contexto cibernético exige um novo olhar sobre os modos de encenação, expressão e manipulação simbólica que permeiam as interações sociais na contemporaneidade digital.

> Os outros podem então usar os aspectos considerados não-governáveis do comportamento expressivo do indivíduo como uma prova da validade do que é transmitido pelos aspectos governáveis.(GOFFMAN, 1975, p.16)

Dessa forma, compreendemos como transmissão e fraude o cálculo estratégico do discurso, um conjunto de expressões verbais e o tempo de fala adequados a determinados espaços “virtuais”, como o telefone, as redes sociais digitais e a comunicação via websites. Simultaneamente, devemos considerar como

emissão e dissimulação a construção e a forja de websites, locais digitais meticulosamente arquitetados para conferir a impressão de veracidade, seriedade e confiabilidade.

Um agente fraudulento atribui a si mesmo formatos específicos de imagem, layouts, biografias e descrições, bem como adota configurações particulares de cada rede social, que remetem a um universo empresarial, profissional ou o que mais couber na situação para parecer confiável. Observa-se, assim, uma constante ação autônoma de fraude e dissimulação, caracterizada por um processo dinâmico de atualização e transição entre espaços e modos de atuação. Tais práticas também se sustentam em estratégias voltadas à fragilização emocional da vítima, com o objetivo de comprometer sua capacidade de percepção crítica e dificultar a identificação da fraude. Como observa Goffman, não apenas o pesquisador, mas também um indivíduo socialmente “descontente” presente no público da ação pode ser capaz de reconhecer essas manipulações.

> Quando seu público está também convencido deste modo a respeito do espetáculo que o ator encena — e esta parece ser a regra geral — então, pelo menos no momento, somente o sociólogo ou uma pessoa socialmente descontente terão dúvidas sobre a “realidade” do que é apresentado. (GOFFMAN, 1975, p. 25)

Ao articular a análise da dramaturgia da fraude com a perspectiva de Pierre Bourdieu sobre violência simbólica, ampliamos a compreensão dos golpes virtuais para além do mero ato criminoso, reconhecendo-os como práticas que se sustentam em relações de poder simbólico. A falsificação da legitimidade institucional, a manipulação de símbolos e códigos de autoridade, e a exploração das vulnerabilidades subjetivas são formas sutis de dominação que operam por meio da imposição de sentidos e da naturalização da desconfiança. Assim, a fraude cibernética configura-se como uma violência simbólica que legitima e reproduz desigualdades, atingindo especialmente aqueles marcados por desigualdades estruturais de gênero, raça e classe, refletidas na dimensão do do acesso a recursos e desenvolvimento de letramento digital.

Ao analisarmos a atuação do fraudador sob a ótica da dramaturgia social proposta por Erving Goffman, evidencia-se o seu domínio sobre técnicas de disfarce e apropriação de lógicas e comportamentos socialmente atribuídos a determinados

tipos de indivíduos. Essas estratégias geram falsas sensações de segurança e sustentam suposições equivocadas, que ocultam a realidade criminosa da ação. O fraudador, portanto, desafia os processos cognitivos da vítima, manipulando expectativas e signos sociais. Como afirma Goffman:

> Talvez o verdadeiro crime do vigarista não consista em tomar dinheiro de suas vítimas, mas em roubar-nos a todos nós da crença de que as maneiras e a aparência da classe média só podem ser mantidas por pessoas da classe média. Um profissional desabusado pode ser cinicamente hostil à relação de serviço que seus clientes esperam que ele lhes preste. O vigarista tem condições de manter o mundo “legal" inteiro em desonra.’ (Goffman, 1975, p. 26)

4.2 Percursos metodológicos em território digital: aproximações e escutas

Era uma tarde comum quando, ao abrir um dos grupos de WhatsApp dos quais participo, percebi que algo chamava atenção entre as mensagens. Uma das participantes acabava de relatar que havia sido vítima de um golpe cibernético. Seu relato vinha carregado de urgência e cuidado, uma tentativa de alertar os demais, na esperança de que ninguém mais passasse pela mesma situação. Naquele instante, o que surgiu como um aviso espontâneo ultrapassava a esfera do cuidado coletivo e se transformava, para mim, em uma cena de pesquisa. A fraude, que tantas vezes parece abstrata ou distante, mostrava-se ali, em circulação, atravessando espaços de sociabilidade cotidiana e redes de confiança.

Cenas como essa e relatos de crimes cibernéticos são comuns na vida cotidiana, ainda que as pessoas, como eu, não estejam interessadas em observar esse fenômeno em termos de pesquisa. Deste modo, o acesso aos interlocutores não se deu por meio de uma busca ativa e direcionada, mas ocorreu de forma orgânica, no decorrer de interações cotidianas que posteriormente se traduziram em campo. Em diálogos informais, a menção ao tema da pesquisa, e sua evidente recorrência no cenário contemporâneo, frequentemente levava à identificação de indivíduos que haviam vivenciado diretamente crimes cibernéticos ou conheciam vítimas de diferentes modalidades desse fenômeno.

Diante dessas situações, explicitei que minha investigação, desenvolvida no âmbito do mestrado, tinha como objetivo analisar as dinâmicas associadas a tais crimes, manifestando interesse em compreender com maior profundidade os relatos compartilhados. Nos casos em que os interlocutores mencionavam conhecer

vítimas, busquei estabelecer um contato indireto, solicitando a possibilidade de mediação para um eventual diálogo com essas pessoas, sempre respeitando sua autonomia e sua disposição em contribuir com a pesquisa.

Os primeiros contatos com essa modalidade de crime ocorreram por meio de experiências vivenciadas por membros de minha própria família e por amigos, tanto aqueles com quem mantenho vínculos mais próximos quanto aqueles mais distantes, bem como experiências particulares minhas das quais já fui alvo de tentativas de golpe. Desde o início, foi possível observar a recorrência dos golpes virtuais e sua ampla disseminação, afetando indivíduos de perfis variados. Trata-se de um fenômeno que não se restringe a um grupo específico, atingindo desde pessoas com elevado nível de instrução acadêmica e científica até aquelas com menor grau de escolaridade e acesso reduzido a conhecimentos especializados. O marcador mais relevante, nesses casos, foi a familiaridade, ou a falta dela, com tecnologias digitais e as dinâmicas que nelas ocorrem.

Essa constatação inicial evidenciou a transversalidade dos crimes cibernéticos e a complexidade das estratégias empregadas pelos criminosos, os quais exploram vulnerabilidades distintas, independentemente do grau de letramento digital ou formação intelectual das vítimas.

Todos os interlocutores foram contatados por mim com o intuito de viabilizar a realização das entrevistas, sendo que apenas uma participante estabeleceu contato espontâneo, de forma autônoma e sem qualquer solicitação prévia, com o propósito de relatar e alertar acerca de um golpe virtual do qual fora vítima. A todos os interlocutores foi informado o interesse em entrevistá-los no contexto da pesquisa, com o objetivo de aprofundar a compreensão do fenômeno investigado e de suas dinâmicas.

As interações, desde os relatos preliminares até as entrevistas mais estruturadas, ocorreram por meio de diferentes canais de comunicação, variando entre conversas informais via plataformas como WhatsApp e outras redes sociais, ligações telefônicas e encontros presenciais. Essa multiplicidade de formatos de contato permitiu uma abordagem mais ampla e flexível, adaptando-se à

disponibilidade e ao nível de conforto dos interlocutores no compartilhamento de suas experiências.

Ao todo, foram entrevistados cinco interlocutores, cada um com experiências distintas relacionadas a crimes cibernéticos. Todas as entrevistas ocorridas e orientadas de modo semi estruturado como defendem Beaud e Weber (2003, p. 136)

> O roteiro de entrevista prende você ao seu tema. Diga a si mesmo que, propriamente falando, não há respostas fora do tema em uma entrevista etnográfica. Deixe sempre a possibilidade para o entrevistado de se perder, de fazer digressões ou incursões em outros domínios que não sejam o principal abordado. Se o pesquisado lhe disser “ai, me afastei”, acalme-o e incentive-o a seguir nessa direção (se, é claro, você julgar que vale a pena). Verá que tais digressões o levarão a compreender como estavam ligados os dois tipos de propósitos. As associações de ideias têm necessariamente sentido para o pesquisado e um sentido social a ser descoberto pelo pesquisador.

O foco da pesquisa não se restringiu a um tipo específico de crime, mas concentrou-se em relatos que envolvessem, de forma direta, um caráter performático na execução e consolidação da fraude. A atenção recaiu, portanto, sobre os aspectos da encenação, da simulação de legitimidade e das estratégias simbólicas empregadas pelos agentes fraudulentos para obter a confiança das vítimas e garantir o sucesso da investida criminosa. Assim como o nível de letramento digital, o uso contínuo e aprofundado dos interlocutores com dispositivos digitais, seus hábitos cotidianos e sua imersão nas redes digitais são fatores fundamentais para a compreensão das dinâmicas comunicativas contemporâneas. Nesse sentido, é importante considerar que, conforme argumenta Hine (2000, P. 18), a linguagem tem se constituído como um eixo central nas análises qualitativas das comunicações mediadas por computador (CMC). A autora destaca que “qualitative approaches to CMC have, not surprisingly, focused on the linguistic resources which participants create and use”[15], ressaltando a importância de compreender como os usuários constroem e negociam significados por meio das práticas discursivas em ambientes virtuais. Além de analisar, na perspectiva das vítimas, o discurso dos fraudadores, uma vez que entendemos aqui que

> o discurso, aparentemente, pode até nem ser nada de por aí além, mas no entanto, os interditos que o atingem, revelam, cedo, de imediato, o seu vínculo ao desejo e o poder… o discurso … não é simplesmente o que

[15] As abordagens qualitativas à CMC, não surpreendentemente, têm se concentrado nos recursos linguísticos que os participantes criam e utilizam. (Tradução livre)

> manifesta (ou esconde) o desejo; é também aquilo que é objecto do desejo. (Foucault 1996, p. 8)

Essa ênfase na dimensão linguística permite revelar as complexidades sociais e culturais presentes nas interações online, que vão além da simples transmissão de informação, evidenciando processos de construção identitária, negociação de normas e produção de sentidos em contextos digitais.

4.3 Quando a promessa se torna armadilha: relatos de fraudes

É no entrelaçar das vozes, das experiências e dos atravessamentos que emergem as tramas deste trabalho. A seguir, compartilho narrativas que não são apenas relatos de vítimas, mas expressões de mundos que se friccionam entre o digital e o social, entre o visível e o invisível, entre o confiar e o desconfiar. São histórias que, ao se fazerem palavra, revelam não apenas os mecanismos dos golpes, mas também as vulnerabilidades, os afetos e as estratégias que permeiam essas vivências. Cada caso aqui apresentado não é mero exemplo ilustrativo, é território de análise, repleto de sentidos, onde procuro caminhar junto das vozes que me foram confiadas. As reflexões que acompanham cada relato buscam, portanto, lançar luz sobre os modos como esses fenômenos se corporificam na vida cotidiana, revelando as fronteiras, por vezes borradas, entre o real e o fraudulento, o material e o simbólico, o técnico e o afetivo.

Cada caso será apresentado aqui com o uso de nomes fictícios atribuídos aos interlocutores, a fim de proteger suas identidades e resguardá-los de qualquer possível constrangimento. Tal cuidado se justifica, sobretudo, pela recorrência, nos próprios relatos, de sentimentos como vergonha e receio em compartilhar essas experiências, que, muitas vezes, são atravessadas por julgamentos sociais sobre a condição de vítima.

O primeiro caso, já narrado brevemente na abertura deste capítulo, refere-se a um crime que se consolida tanto na esfera material quanto na digital. Cláudia, graduada em teatro, atriz e professora de artes teve seu telefone celular, um smartphone da marca Apple, roubado. Dias após registrar o boletim de ocorrência pelo roubo e tentar localizar o aparelho por meio do sistema de rastreamento da própria Apple, ela recebeu mensagens via WhatsApp, enviadas de um número que

se apresentava como um contato oficial da empresa. As mensagens eram redigidas em linguagem formal e técnica, acompanhadas do logotipo da Apple, e solicitavam que ela acessasse sua conta Apple ID por meio de um link disponibilizado na própria conversa. A justificativa apresentada era de que, com isso, seria possível localizar o aparelho e auxiliá-la no processo de recuperação do bem “perdido” após o assalto.

A vítima, ainda abalada pela perda do dispositivo, que representava para ela um dano financeiro significativo, foi mobilizada emocionalmente pela possibilidade de reaver seu celular e, assim, seguiu as orientações enviadas pelo número que a contatou. Somente após acessar o link e inserir seus dados de acesso ao Apple ID é que percebeu que a função de rastreamento do aparelho, a qual ela já vinha utilizando, havia sido desativada a partir de sua própria conta, o que impossibilitou sua localização. Nesse momento, constatou que o contato não pertencia à empresa Apple, mas se tratava de uma tentativa fraudulenta adicional, articulada para consolidar o roubo, bloquear os mecanismos de rastreamento e, consequentemente, impedir qualquer chance de recuperação do dispositivo.

Nesse relato, é possível observar como a vulnerabilidade emocional se torna um recurso central na materialização do crime, funcionando como dispositivo que favorece a sua eficácia. A comoção provocada pela perda, somada ao desejo urgente de reaver o bem, contribuiu para que a vítima não questionasse por que uma empresa solicitava, por canais informais, dados sensíveis de acesso. O engano se operou por meio de uma estratégia dramatúrgica, na qual são simulados elementos de comunicação institucional, como linguagem formal, tom técnico e uso de logotipos, para construir um cenário de legitimidade capaz de gerar confiança.

Essa encenação digital pode ser entendida como uma ação *ingovernável*, na medida em que os criminosos não detêm o controle sobre os canais legítimos de comunicação da empresa. Por outro lado, mobilizam *ações governáveis*, como a escolha das palavras, a estética visual da mensagem e a construção de um roteiro comunicativo que busca mitigar a percepção da fraude.

Dessa maneira, ainda que o crime tenha se originado no espaço físico, com o roubo do aparelho, ele se consolida na esfera digital ao induzir a vítima ao erro e, paradoxalmente, ao levá-la a realizar, “por conta própria”, a desativação dos

mecanismos de rastreamento do dispositivo. A empresa, por sua vez, não se percebe como parte lesada no processo e, muitas vezes, pode alegar que a desativação foi feita mediante autorização da titular da conta, o que retira dela qualquer responsabilidade posterior. Tanto que em uma perspectiva de buscar reparação, a vítima não obteve bons resultados com a instituição policial nem após um segundo boletim de ocorrência especificamente sobre a fraude virtual. Isso impõe à vítima obstáculos adicionais no caminho da reparação, evidenciando, mais uma vez, as assimetrias que marcam as relações entre consumidores, empresas de tecnologia e as dinâmicas dos crimes cibernéticos.

O segundo caso se refere a compra de um ingresso para um festival de música, vendido de forma informal por uma pessoa que supostamente teria comprado e não iria mais. Gerando conversações na rede social instagram, bem como a construção estética e discursiva de um perfil que atribui a vítima a sensação de segurança e confiabilidade.

Mariana e sua companheira buscavam ingressos para um evento local bastante procurado. Em conversas sobre o evento em páginas do instagram, elas encontraram uma suposta vendedora anunciando, cujo perfil parecia confiável à primeira vista: apresentava fotos de um mulher branca e que aparentava ter aproximadamente 40 anos, uma biografia construída com cuidado (mencionando maternidade) e escrita atenta, elementos que simulam autenticidade e empatia.

A transação foi feita via Pix (R$ 200,00 por dois ingressos) e com plena confiança na transação, mas após o pagamento, a golpista tornou as mensagens autodestrutivas, depois bloqueou o contato e desapareceu. Mariana e sua companheira constataram que outras pessoas também haviam sido vítimas do mesmo golpe. Descobriram, inclusive, que já havia um outro perfil atuando de forma semelhante sobre o mesmo evento e nas mesmas páginas.

Apesar de divulgarem o ocorrido a outras pessoas e ao perfil do evento, não conseguiram reaver o valor nem tomar medidas legais imediatas. Ao passo que o ocorrido se revelou uma experiência significativa de vitimização digital por meio de um golpe aplicado nas redes sociais, mais especificamente no Instagram. A vítima, mesmo sendo uma usuária com graduação e com familiaridade cotidiana com tecnologias digitais, especialmente aplicativos de banco, não se identificava como

uma usuária intensiva das redes sociais, o que, paradoxalmente, pode tê-la deixado mais vulnerável a certos mecanismos de engenharia social aplicados por golpistas.

O terceiro caso analisado refere-se a um episódio de fraude digital que envolveu a apropriação indevida do aplicativo WhatsApp da vítima, por meio de um ato que explorou a confiança nos procedimentos de plataformas digitais de compra e venda. A vítima, Luciana, uma mulher branca de 33 anos e já mãe, havia recém-publicado um anúncio de venda na plataforma OLX quando foi contatada telefonicamente por um indivíduo que se apresentou como representante da referida empresa. O suposto atendente solicitou que a vítima fornecesse um código que, segundo ele, seria enviado via SMS como parte de um processo de verificação destinado a "consolidar a publicação" e "otimizar as chances de venda do produto anunciado".

No entanto, o código solicitado não tinha qualquer relação com a plataforma de vendas, tratando-se, na realidade, do código de verificação de segurança do WhatsApp, utilizado para autenticar o acesso à conta em um novo dispositivo. A ação causou tanto a sensação de confiabilidade na vítima que a mesma forneceu o código de forma rápida e sem observar que o SMS contendo o código trazia explicitamente a informação de que se tratava de um código de ativação do Whatsapp. Ao fornecer tal código, a vítima permitiu, inadvertidamente, que o golpista assumisse o controle de sua conta pessoal no aplicativo de mensagens.

Uma vez em posse da conta, o fraudador passou a utilizar a identidade da vítima, por meio de suas interações e vínculos sociais previamente estabelecidos, para solicitar valores em dinheiro sob a justificativa de empréstimos emergenciais. A confiança depositada pela rede de contatos na identidade digital da vítima facilitou a consumação do golpe, resultando em prejuízos financeiros tanto para ela quanto para as pessoas de seu convívio, como também a privação de sua presença em uma rede de uso cotidiano para diversas esferas da vida.

Esse tipo de crime evidencia não apenas a sofisticação dos métodos de engenharia social empregados por golpistas, mas também as fragilidades existentes na forma como os usuários se relacionam com a segurança digital. Como observa Castells (2003), a sociedade em rede é caracterizada pela circulação veloz de

informações, mas também pela ampliação das possibilidades de manipulação simbólica e de vulnerabilidade dos sujeitos no espaço digital.

Na quarta interlocução, é Janete quem ocupa a cena. Mulher parda, 23 anos, sem ensino superior, construiu sua trajetória como comerciante local, mantendo uma loja física em Fortaleza, cujas fronteiras se expandiam para além do espaço material por meio das plataformas digitais. Seu relato remonta a janeiro de 2023, quando vivenciou o episódio que a colocou na condição de vítima.

Em sua prática cotidiana, as transações virtuais eram parte indissociável do trabalho, quase uma extensão da própria loja. Realizava vendas recorrentes por links de pagamento, especialmente utilizando o serviço Mercado Pago, que, para ela, representava não só um meio técnico, mas também uma promessa de facilidade, de segurança e de agilidade no fluxo comercial. Contudo, seria justamente nesse cruzamento entre o físico e o digital, entre a rua e a rede, que o golpe atravessaria sua experiência.

No referido caso, a comerciante foi procurada por uma suposta cliente, também residente em Fortaleza, que realizou três compras utilizando o método de pagamento via link de cartão de crédito. À primeira vista, tudo parecia seguir o roteiro habitual das práticas comerciais cotidianas, sem qualquer sinal evidente de fraude. A interlocutora manteve uma comunicação constante, cortês e alinhada às dinâmicas esperadas numa relação de consumo.

Realizou os pagamentos, apresentou comprovantes e, inclusive, organizou a retirada dos produtos por meio de um serviço de entregas via Uber, detalhe que, na percepção da comerciante, operou como um marcador de legitimidade, reforçando a ideia de que se tratava de uma transação segura, dentro dos parâmetros do comércio digital que se sobrepõe e se entrelaça com o território urbano.

Contudo, cerca de dez dias após as transações, a vítima foi surpreendida por notificações de contestação (chargeback) referentes às duas primeiras compras, que já haviam sido entregues. A terceira compra também foi contestada, embora a mercadoria ainda não tivesse sido despachada. Ao buscar esclarecimentos junto à suposta cliente, esta alegou que a contestação fora realizada por uma terceira pessoa (sua tia) sob a justificativa de que não reconhecia a transação no extrato

bancário. Em seguida, a cliente solicitou o reenvio do link de pagamento, mas, após esse pedido, toda comunicação cessou abruptamente.

Diante da constatação da fraude, a comerciante buscou diversos mecanismos institucionais de resolução de conflitos e reparação de danos. Registrou boletim de ocorrência na delegacia especializada, acionou órgãos de defesa do consumidor, como o Procon, e ingressou com demandas judiciais em juizados de pequenas causas. Apesar das tentativas formais, não obteve êxito na resolução do caso, arcando integralmente com os prejuízos financeiros, decorrentes tanto do estorno dos valores das vendas quanto da perda das mercadorias previamente entregues.

Este relato ilustra um padrão recorrente nas fraudes eletrônicas contemporâneas, caracterizado pela simulação de práticas comerciais legítimas, apropriação indevida de dados financeiros e uso de intermediadores de pagamento que, apesar de conferirem aparente segurança às transações, frequentemente não oferecem respaldo efetivo às vítimas em situações de contestação fraudulenta.

No quinto caso temos Rafael, um homem branco de 26 anos, ex-militar e profissional da área de engenharia mecânica, atuando como analista de telemetria, e sem ensino superior, vivenciou um episódio emblemático que revela as dinâmicas complexas da vitimização em contextos digitais. A queima inesperada de sua televisão, objeto que transcende sua função técnica para se configurar como elemento integrante do cotidiano e das práticas culturais, o impulsionou a buscar, com urgência, uma nova unidade por meio de plataformas digitais de revenda.

Na plataforma OLX, Rafael identificou um anúncio que apresentava um preço significativamente abaixo do mercado, o que inicialmente pareceu uma oportunidade vantajosa. A negociação remota com o suposto vendedor estabeleceu uma interlocução marcada por uma aparente credibilidade, fundamental para a construção da confiança necessária à transação virtual.

Entretanto, o desdobramento da negociação revelou-se ambíguo quando o vendedor comunicou sua ausência no local indicado para a entrega, delegando a tarefa a um primo e condicionando a entrega à transferência antecipada do valor. Esse deslocamento do contato direto e a exigência de pagamento prévio acionaram

um mecanismo de desconfiança em Rafael, que passou a questionar as condições da venda.

A adoção de uma postura mais agressiva e crítica por parte de Rafael, interrompendo a dinâmica convencional do diálogo comercial, resultou na exposição da fraude: o vendedor, ao perder o controle da interação, abandonou a máscara do personagem fraudulento. O golpe, assim, não se consolidou.

Posteriormente, Rafael estabeleceu contato com o morador do endereço indicado no anúncio, o vendedor legítimo da televisão, e confirmou a apropriação indevida de suas imagens e dados para a construção da fraude. Esse episódio evidencia a complexa articulação entre o espaço digital e o mundo material, onde a confiança se constrói e se desfaz rapidamente, e onde os mecanismos de vigilância e desconfiança se tornam elementos centrais na proteção contra golpes.

Dessa forma, a experiência de Rafael oferece um recorte significativo para a análise das relações de poder, vulnerabilidade e resistência presentes nas transações digitais, iluminando como o contexto da urgência e da escassez pode ser explorado por agentes fraudulentos e como a capacidade de crítica e intervenção do indivíduo pode mitigar os riscos.

Diante do contexto pós-pandemia, observa-se, a partir dos dados do *Anuário Brasileiro de Segurança Pública*, um crescimento exponencial dos crimes cibernéticos, especialmente dos estelionatos eletrônicos e de outras fraudes virtuais. Paralelamente, verifica-se uma redução significativa nas ocorrências de crimes convencionais, como roubos de celulares, veículos, residências, estabelecimentos comerciais e delitos cometidos em espaços públicos. Esse cenário sugere a existência de um movimento de migração da atividade criminosa para o ambiente digital, onde as redes tornam-se meios privilegiados para a prática de delitos. Tal dinâmica evidencia não apenas uma transformação nos modos operatórios da criminalidade, mas também impõe novos desafios às autoridades, particularmente no que diz respeito à identificação dos autores e à coleta de provas, dada a natureza transnacional, descentralizada e, muitas vezes, anônima dos crimes perpetrados no ciberespaço.

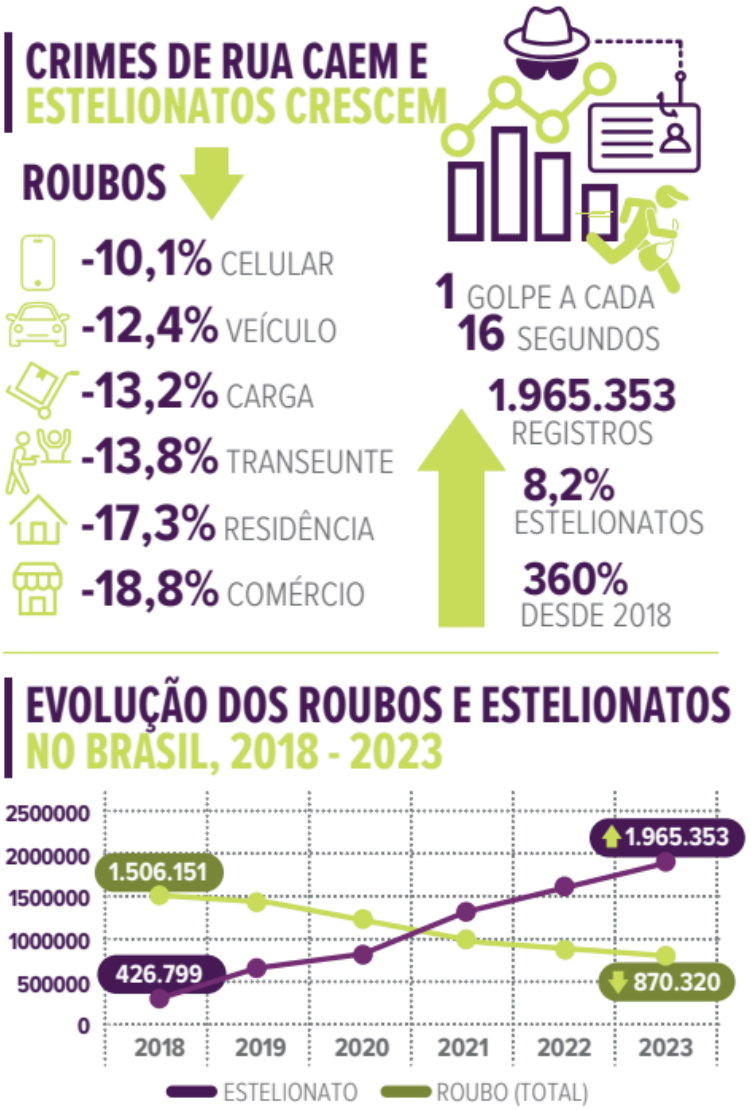

Imagem e dados retirados do Anuário Brasileiro de Segurança Pública 2024

A análise desses relatos abre um espaço sensível para compreendermos os contornos múltiplos da vitimização no tempo da digitalidade, onde o tecido social se entrelaça com o virtual de maneiras complexas e permeadas por desigualdades. As interlocutoras, atravessadas por suas trajetórias singulares, revelam perfis marcados por diferenças sociobiográficas que ressoam na forma como cada uma experimenta o golpe.

Cláudia, com seus 35 anos à época do relato, traz na bagagem a formação teatral e a familiaridade com o universo digital profissional, uma presença que, paradoxalmente, não foi suficiente para protegê-la da armadilha. Mariana, aos 25 anos e já graduada em Ciências Sociais, navega com menos intensidade nas redes,

mas carrega uma experiência prévia de transações virtuais, que, ainda assim, não a blindou contra a fraude. Luciana, aos 33, sem formação acadêmica e imersa nas responsabilidades da maternidade, encarna um perfil onde o capital cultural e as condições sociais se entrelaçam de modo distinto, moldando sua vulnerabilidade. Janete, a mais jovem, sem ensino superior, cuja relação com as redes se dá sobretudo pela esfera comercial, evidencia a diversidade dos usos e dos riscos que perpassam o digital. Por fim, Rafael, aos 26 anos, ex-militar e profissional da engenharia mecânica, demonstra como a urgência material, neste caso, a necessidade premente de substituir uma televisão que queimou, aliada a uma postura crítica e vigilante, pode tanto expor o indivíduo a riscos quanto permitir a resistência e o rompimento da tentativa fraudulenta. Sua experiência destaca as tensões entre a pressa, a desconfiança e a construção cuidadosa da confiança no espaço digital.

Essas vozes nos convidam a perceber que, para além do golpe em si, o que se confronta é um cenário tecido por diferenças sociais, afetos, saberes e práticas, um espaço onde o digital não é um campo neutro, mas sim um palco de disputas e reencontros com as desigualdades que já percorrem o mundo material.

Apesar das distinções de idade, formação, frequência de uso da internet e modalidade de golpe sofrido, observa-se uma estrutura comum nas estratégias fraudulentas empregadas. Em todos os casos, houve a mobilização de *performances dramatúrgicas* elaboradas com o intuito de simular confiabilidade e legitimidade. Tais performances operam por meio da construção de identidades falsas, sustentadas por narrativas verossímeis, que exploram elementos de linguagem, aparência e comportamento socialmente associados à credibilidade.

Essas práticas fraudulentas se articulam com uma lógica teatral de encenação, no sentido goffmaniano, em que os golpistas constroem “frentes” sociais convincentes, manipulando os marcos da interação para criar uma ilusão de autenticidade. O sucesso dessas ações depende, em grande parte, da capacidade de ativar emoções específicas nas vítimas, como urgência, empatia, medo ou excitação, que reduzem sua capacidade de julgamento racional e as impedem de identificar os indícios de ilegitimidade presentes nas interações.

Além disso, é importante destacar que as fraudes analisadas não operam unicamente no plano técnico ou informacional, mas incidem diretamente sobre aspectos afetivos, subjetivos e relacionais da vida das vítimas. A confiança, enquanto mecanismo fundamental das interações sociais e comerciais, é instrumentalizada como ferramenta de manipulação. Assim, os golpes não apenas se valem das vulnerabilidades técnicas, mas, sobretudo, das vulnerabilidades emocionais e relacionais.

Compreende-se, portanto, que uma reflexão crítica sobre esses casos demanda uma abordagem que considere tanto os marcadores socioculturais das vítimas quanto os dispositivos simbólicos e afetivos mobilizados nas práticas fraudulentas. A interseção entre teatralidade, performance e emoção revela-se, assim, um eixo analítico fundamental para compreender os modos pelos quais os golpistas constroem suas estratégias e as vítimas, por sua vez, são levadas ao engano.

5 QUANDO O GOLPE ACONTECE: NARRATIVAS SOCIAIS DA FRAUDE E DA VULNERABILIDADE DIGITAL

> A Polícia Civil de Santa Catarina (PC/SC) deflagrou, nesta quinta-feira (23), a Operação Litis Simulatio para desarticular uma associação criminosa especializada no golpe do falso advogado. Foram expedidos 25 mandados de busca domiciliar e 16 de prisão temporária, cumpridos no Ceará e no Rio de Janeiro, contra suspeitos e pessoas que receberam valores ilícitos em suas contas bancárias. (Notícia veiculada pelo Ministério da Justiça de Segurança Pública)[16]

Golpes como esse tem se tornado cada vez mais comuns e se valem de uma lógica onde as interações digitais são utilizadas como uma espécie de “palco” onde são construídas de forma cuidadosa e planejada as fachadas: perfis falsos, nomes de advogados, a identidade visual de escritórios, linguagem jurídica e um conjunto de documentos que mimetizam os documentos comuns a esse campo. Esse tipo de encenação nos ajuda a observar o quão central são as gestões de impressão na consolidação desses eventos, tal qual como apresentada por Goffman, a definição da situação demanda esse esforço com a finalidade de que o outro (a vítima) acredite na autenticidade do papel desempenhado.

Enquanto isso, os sujeitos a serem vitimados adentram esse jogo de significações por confiar na aparência de “cenário institucional” (se valendo de elementos comuns ao campo e neles respeitados, como a justiça, o direito, a figura do advogado). Dessa forma, o golpe se reduz a uma fraude financeira, mas só é possível a partir de uma performance bem-sucedida de credibilidade e legitimidade, uma dramaturgia que encena a autoridade.

A ideia de capital simbólico é importante aqui na medida em que a fraude só é possível exatamente porque existem capitais de alto valor sendo mobilizados na execução de cada golpe. No caso desde anteriormente mencionado, os capitais se referem ao campo jurídico com a finalidade de definir a situação como sendo a de um espaço da seriedade, técnica, moralidade e confiança pública. Os golpistas se apropriam desse capital, operando uma espécie de *usurpação simbólica*. Ao passo em que as vítimas se submetem a essa “autoridade” na medida em que

---

[16] Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/golpe-do-falso-advogado-operacao-nacional-prende-suspeitos-no-rio-de-janeiro-e-no-ceara

reconhecem os símbolos e neles acreditam. Uma espécie de dominação que se exerce através da crença de legitimidade.

Vale ressaltar que ao trabalhar a etnografia virtual, Christine Hine pontua o digital como um ambiente social e não meramente um meio. E é nesse contexto que a farsa do fraudador se sustenta, com elementos de uma cultura digital que desmaterializa a confiança e atribui os sinais de autenticidade a uma estrutura que dispensa o encontro presencial.

Deste modo, podemos afirmar que os golpistas exercem uma espécie de micro poder, como diria Foucault, na medida em que suas ações são planejadas de modo a orientar a resposta das vítimas, prescrever comportamentos (pagamento de taxas, envio de dados pessoais, acesso a sistemas semelhantes aos reais) e operam através de narrativas que soam racionais e oficiais.

Esses são elementos importantes na hora de analisar as experiências de golpes digitais ou cibernéticos, ainda que se reconheça a suas complexidades e o quanto tais experiências podem ser lidas através de um olhar mais interseccional. Em suma, o avanço tecnológico informacional produziu uma série de vulnerabilidades que são exploradas e confrontadas com uma carga expressiva de novos tipos de golpes, desde o golpe do falso advogado como o mencionado a outros que mobilizam a vítima a serem os autores (ainda que sem a plena consciência do ato) da cessão de seus dados ou recursos para os fraudadores. E estes critérios estarão bastante presentes nas análises dos casos coletados nesta pesquisa.

5.1 Análise das experiências relatadas pelos interlocutores

É costumeiro que a atenção pública se concentre em aspectos técnicos, jurídicos e morais quando o assunto é golpes e fraudes em ambientes digitais. Todavia, como já observado no decorrer desta dissertação, tramas sociais, performances e interações são elementos presentes por trás de cada transação fraudulenta, de cada mensagem enganosa e de cada interação digital que resulta em prejuízo, e que sustentam o próprio funcionamento do golpe. Nesse capítulo há um enfoque especial nas narrativas apresentadas pelos interlocutores com a finalidade de compreender quando o golpe acontece, ou seja, mergulhar nas

experiências concretas de indivíduos que, de diferentes posições, viveram, testemunharam ou analisaram os mecanismos de fraude no Ceará.

A este ponto as contribuições dos interlocutores não são apresentadas como meros dados, mas como narrativas sociais repletas de informação que não se reduzem aos fatos objetivos do crime, mas expressam sentidos, vulnerabilidades, estratégias e emoções que perpassam o fenômeno da fraude digital. São histórias de quem foi convencido, enganado, explorado, mas também de quem estuda, combate ou observa, desde diferentes lugares, os bastidores e os roteiros desse tipo de crime.

De forma direta, a análise de como esses golpes se constroem socialmente é o foco deste capítulo, quais são os elementos que compõem seus roteiros, que performances são acionadas pelos golpistas, e de que formas as vítimas, atravessadas por diferentes condições socioeconômicas, culturais e subjetivas, se tornam mais ou menos suscetíveis a esses enredos. É sobre olhar para as fraudes de forma a não percebê-las como atos isolados, mas como um fenômeno social situado, relacional e profundamente enraizado nas estruturas e nas dinâmicas da vida digital contemporânea.

A seguir nos debruçarmos sobre as narrativas coletadas nas entrevistas concedidas a esta pesquisa, as análises construídas a partir do cruzamento entre teoria e empiria, e os significados que se revelam neste campo complexo onde se encontram tecnologia, subjetividade, precariedade, desejo, confiança e risco. Quando o golpe acontece, é possível observar bem mais que a execução de um crime, mas também um espelho das contradições, das fissuras e das vulnerabilidades de uma sociedade hiperconectada e, ao mesmo tempo, profundamente desigual.

Os casos foram brevemente apresentados no capítulo anterior e os examinaremos de forma mais aprofundada. A começar pelo primeiro caso apresentado, o da interlocutora que, aqui, chamamos de Cláudia.

- Claudia e o roubo de aparelho celular que se concluiu digitalmente

Podemos iniciar essa análise pensando as questões relativas à regulação da impressão que se tem do outro e a construção da imagem nas interações. Um dado interessante sobre o trabalho de campo desta pesquisa é que, ainda que seja relativamente fácil encontrar pessoas que já foram vítimas de tentativas ou golpes bem sucedidos, a disposição em abordar esse evento em entrevista é bem menor. E observa-se que, ainda que a pessoa se disponibilize para tal, a gestão da impressão ainda é um forte fator na maneira como ela relata a sua história.

É possível observar na entrevista de Claudia desde o início um esforço por parte do fraudador para regular a impressão que causa na outra parte da interação (a vítima). Ela narra como houve cuidado em construir uma "identidade" que dialogasse com o que ela acreditava ser seguro e, por consequência disso, a levaria a fornecer seus dados, a erro. Analisaremos a partir de seu relato esses elementos de convencimento

A história de Cláudia expressa de forma intensa um jogo clássico de gestão das impressões, tanto da parte do fraudador e seu cuidadoso trabalho de parecer confiável quanto de Cláudia que está sempre reafirmando em sua apresentação sua posição como "usuária experiente, cautelosa e moralmente correta", ao mesmo tempo em que o episódio do roubo expõe uma fratura entre a imagem apresentada e a vulnerabilidade que se abre no backstage.

> "eu acompanho a internet desde a adolescência, da migração... acompanhei o crescimento do... a saída do orkut, do facebook, do messenger até hoje, aos dias atuais, que a gente tem ai instagram… Então eu acompanhei todas essas tecnologias…" (Entrevista com Claúdia para esta pesquisa)

A mensagem SMS/WhatsApp falsa explora precisamente esse hiato entre frontstage (o "login da Apple" confiável, a autoridade institucional) e backstage (a ansiedade, o receio de perder um bem com parcelas em andamento).

> Então ai fui furtada, tentei resgatar o aparelho e não consegui e ai o golpe veio quando... a Apple tinha orientado que ela só manda os avisos por e-mail, não manda por whatsapp, não manda por sms, pois bem, com essa informação. E nesse momento eu esqueci, e foi quando eu recebi uma mensagem SMS dizendo veja a câmera, a pessoa que furtou, e eu cliquei. E também teve uma mensagem pelo whatsapp que eu também achei que fosse da apple quando na verdade até meu nome não estava idêntico na

> escrita a grafia do meu registro. (Entrevista com Claúdia para esta pesquisa)

Do ponto de vista de Bourdieu, a ação vivida por Cláudia mostra um habitus digital formado por história social e práticas acumuladas: ela “acompanha a internet desde a adolescência”, tem estratégias (cartões virtuais, senhas diferentes) que são formas de capital técnico e cultural acumulado, mas ainda assim vulnerável a táticas de engenharia social que exploram estados emocionais que fragilizam sua atenção técnica. Ainda que a ideia de um habitus digital possa revelar disposições prévias que orientam modos de navegação, entre outras formas de estar em ambiente digital.

Christine Hine nos auxiliar a enxergar os artefatos comunicacionais, as mensagens e a página de login falsos, como elementos que funcionam através de “performances” técnicas, não se reduzindo a texto, mas também design (lay-out que imita a Apple), grafia levemente alterada, e a imediaticidade imposta via canais como SMS e WhatsApp. O design da comunicação (um link curto, chance de ver a imagem do assaltant, interface parecida com login oficial) é uma estratégia de persuasão que opera sobre rotinas de uso (clique para “ver a câmera”), dificultando a distinção de sinal de ruído no fluxo do dia a dia.

> E a TIM fornecia o seguro da zurich, então no momento do ato da compra do aparelho eu adquiri o seguro da zurich… Busquei e eles falaram que era com a Zurich, eu entrei em contato com a Zurich e a Zurich falou que não podia por questão de divergência de titularidade. (Entrevista com Cláudia para esta pesquisa)

Há uma operação de poder em curso, como observa Foucault, não sendo uma mera criminalidade, mas uma micro-tecnologia de governo das condutas, mensagens que induzem comportamentos, dispositivos que disciplinam o corpo/tempo da vítima (clicar, inserir senha) e instituições (seguradora, operadora, polícia) que regulam e normalizam a resposta, muitas vezes deixando ao indivíduo a sensação de desamparo ou solidão.

> “Na verdade eu acho que foi o emocional mesmo, porque era uma mensagem simples 'clique aqui para ver..." a imagem, a cara da pessoa que furtou. E eu cliquei e ai depois a página que abriu parecia realmente uma página do login e senha da Apple, ai eu acreditei.” (Entrevista com Claúdia para esta pesquisa)

Detalhes desde os mais simples até a linguagem utilizada, Cláudia identifica indícios suspeitos, grafia diferente, nome não idêntico, mas mesmo assim acredita ter sido o “emocional” que não a permitiu observar esses detalhes com desconfiança. Isso mostra como a linguagem das plataformas se apresenta como autoridade, possuem algum capital simbólico (conteúdo curto, imperativos: “veja a câmera”) e como a semiótica do design imita instituições de confiança. A burocracia institucional (TIM, Zurich, Apple) funciona como fricção que pensa a perda com normalidade e reconfigura a confiança institucional.

A trajetória de Claudia nos mostra também um letramento digital acumulado e prático: uso da internet desde a mais tenra idade, desde a internet discada, hábito de memorização de senhas, uso combinado de aparelhos como computador e celular, estratégias práticas como cartões virtuais de 72 horas, verificação em duas etapas, separação de e-mails e contas bancárias. “Eu também... quando eu vou fazer uma compra virtual, eu uso um cartão virtual que dura 72 horas, que expira. Então eu procuro ter esses cuidados, as redes sociais eu coloco verificação de duas etapas” (Entrevista com Cláudia para esta pesquisa). Este letramento exibe tanto uma familiaridade com um habitus digital, como também pode ser visto como capital técnico e capital cultural; na visão de Bourdieu e como um conhecimento aprendido na prática e na observação de terceiros como apontado por Hine

> Eu diria que a internet é maravilhoso, assim. É realmente é um... eu não acho ruim, todo mundo deveria acessar, mas com cautela, com cuidado. Redes sociais... não ver mutias horas por dia, por exemplo, eu limito... Ter cautela nesses acessos, ter cuidado com as suas senhas, onde você vai salvar, salvar suas coisas sempre na nuvem, seu material sempre na nuvem. Ter um e-mail de emergência, de reserva. (Entrevista com Cláudia para essa pesquisa)

O relato de Cláudia é um bom exemplo de como o letramento não se restringe às competências técnicas e adentra sim uma dimensão emocional decisiva. As performances são afetadas pelo estado emocional e neste caso, em específico, o roubo físico e a carga afetiva (aparelho comprado parcelado, conectado a memória/segurança) limitam a escuta crítica dos detalhes da fraude. A própria Cláudia reafirma o peso do emocional na ação de cada clique, o impacto em sua capacidade cognitiva para lidar com a internet, que é boa em termos procedimentais, mas que, temporariamente, foi atravessada e reduzida por estresse e o sentimento de urgência. Hine enfatizaria como parte de um letramento digital

efetivo para além da habilidade técnica também a construção de rotinas de preparo emocional (protocolos que se seguem apesar do estresse).

Cabe observar como apesar da fragilidade de Cláudia diante do caso que viveu, houve também um movimento de aprendizado e letramento com a experiência prática que a fez construir protocolos sobre o uso da internet a partir de uma inteligência que vai do técnico ao emocional e dos conhecimentos sobre os riscos em ambientes digitais. E reforçando a ideia do emocional como parte do letramento, podemos observar como uma pessoa mesma repleta de técnicas e estratégias ainda está sujeita a ser levada a erro por elementos que vão da linguagem ao design dos ambientes onde o golpe acontece.

> Eu me senti muito assustada, a querer sair de casa, a pegar ônibus, a pegar moto. Então sempre que eu pegava um motorista de aplicativo, por moto, se aproximava uma moto eu ficava assustada
>
> ai eu tive que mudar meu número de telefone, eu mudei pra outro celular, outro chip que eu tinha. Porque eu fiquei com medo de... de quem ficou com o meu telefone puder ficar ligando pra mim e fazer algum golpe, alguma coisa. Então até isso eu precisei mudar, esse cuidado. (Entrevista com Cláudia para essa pesquisa)

Cabe pensar também nos impactos posteriores à fraude. O golpe consolida perdas materiais e simbólicas, desde a perda do aparelho em si, transtornos administrativos com B.O.s, tentativas de seguro e também o custo emocional prolongado (medo ao ver motos, ansiedade em transportes). Simbolicamente, a perda acontece também no exercício da confiança, canais de comunicação instantâneos, instituições e empresas passam a ser espaços frequentados com maior cuidado em uso de contas digitais, e mesmo empresas como bancos, por mais sérias que possam parecer, agora ocupam um lugar de dúvida e cuidado. Em consonância com as ideias de Castells sobre a sociedade informacional, nós vemos aí a reconfiguração da vida cotidiana pela lógica informacional: a perda do aparelho celular, que antes ocupava um lugar central, reorganiza redes pessoais e práticas financeiras.

> Redes sociais... não ver muitas horas por dia, por exemplo, eu limito... Tudo bem que eu desativei o instagram, mas eu limitar... limito a uma hora por dia. Eu deixava livre, então acessava 4,5 ou 6 horas por dia. Então eu limitei a 1 hora. O Facebook eu procurava uma vez por mês acessar, os meus e-mails, nem todo dia eu acesso. Acesso assim um dia sim e um dia

> não. Ter cautela nesses acessos. (Entrevista com Cláudia para essa pesquisa)

Isso pode ser observado a partir do relato de Cláudia quando a mesma afirma que adotou práticas outras e passou a ter mais desconfiança e receio, a fazendo limitar tempo de redes, usar cartões virtuais, autenticação dupla, separar e-mails, não cadastrar cartões em serviços permanentes, reduzir participação em grupos amplos no WhatsApp. Há uma aprendizagem que surge em termos de adaptação ao se confrontar com a realidade das fraudes. Constroem-se rotinas de segurança que visam reduzir a exposição. Por outro lado, no caso de Cláudia os receios não se deram apenas no ambiente digital, mas também no offline com susto com motos, considerar fechar conta digital e vergonha que a levaram a compartilhar o caso com amigos, estratégia de externalização que funciona como reparação social, mas também revela estigma na medida em que mesmo quem “sabe” pode ser pego. Em um capitalismo de vigilância e de individualização é comum que a vítima internalize a responsabilidade, sendo sujeita a um juízo moral que legitima a vergonha.

O caso de Cláudia é uma perfeita interseção entre emoção, rotina e habilidade técnica, ainda que o letramento técnico exista, não substitui práticas institucionais e sociais de acolhimento e prevenção e também demonstram a carência de melhor habilidade emocional perante situações atravessadas por fortes sentimentos como estresse e a urgência por reparação.

- Mariana, revenda de ingressos por redes sociais

Aqui no caso de Mariana seguiremos a mesma perspectiva de análise, no entanto, o que observamos a priori foi uma cena típica de economia digital e de elementos de confiança que não são ligados diretamente a empresas e instituições. O relato de Mariana nos mostra uma fraude que tem entre seus elementos centrais uma performance cuidadosamente construída na rede social Instagram, uma plataforma que se mostra como terreno fértil para a gestão da impressão e construção da imagem. O perfil do fraudador, falso, apresenta “uma mulher, mãe, com descrição organizada e linguagem cuidadosa”, sendo interessante enxergar isso como mais do que um artefato técnico, mas uma apresentação do eu, uma encenação, com o propósito de gerar credibilidade, trazendo a domesticidade e a maternalidade para fortalecer a moral, como elementos que, se pensados a partir de Goffman, compõem um “front stage” de confiabilidade, capaz de conter as desconfianças e induzir à entrega.

> o perfil era de uma mulher, mãe, tinha toda essa descrição assim que tentava passar uma certa confiança, né. Era uma mulher que aparentemente… Eu prestei mais atenção depois que aconteceu do que na hora. E essa mulher disse que estava vendendo o ingresso. Eu já havia vendido e comprado ingressos pela internet, de forma não profissional, não formal, outras vezes e não tinha acontecido problemas né (Entrevista com Mariana para essa pesquisa)

A vítima, por sua vez, também performa uma identidade social dentro do campo digital: mulher branca, de classe média, pós-graduanda, usuária cotidiana da internet e financeiramente autônoma. Também detinha certo grau de um habitus digital devido a uma socialização em meio a tecnologia e de um acúmulo de capital cultural e técnico, ainda que isso não a tenha imunizado contra a manipulação simbólica das redes. A fraude se expressa como mais do que um evento econômico,mas um embate deesses capitais simbólicos, onde o fraudador mobiliza um “capital de confiança” fictício e a vítima se vê desautorizada cognitivamente após cair em um golpe.

> É... então a gente fica tão acanhado diante daquele sentimento de emburrecimento que a gente fica com receio de procurar a policia pra dizer "olha, eu fui bem burra e eu dei duzentos reais na mão dessa pessoa aqui que nitidamente não é uma pessoa real (Entrevista com Mariana para essa pesquisa)

Em uma perspectiva aliada a visão de Hine, podemos atribuir ao golpe a ideia de uma performance sociotécnica, onde design, interface e linguagem se alinham com a finalidade de produzir sentido. A fraude não se limita à troca textual: envolve a estética da biografia, o número “razoável” de fotos, a coerência gráfica e o sentido afetivo do “ser mãe”. “Eu acho que ela tinha uma escrita cuidadosa, sabe... eu acho que isso também contou um pouco” (Entrevista com Mariana para essa pesquisa). O design da comunicação, ainda que soe apenas como pequenos detalhes, atua como dispositivo de convencimento e parte de uma cultura visual e estética que confere a impressão de autenticidade na experiência online.

> …a gente não conseguiu pegar o dinheiro de volta, a gente só conseguiu avisar pra outras pessoas que não comprassem. Eai acabou que a página do evento fez um post explicando que a página não se responsabiliza por ingressos comprados fora das bilheterias oficiais, e que a gente evitasse fazer esse tipo de compra, de transação... (Entrevista com Mariana para essa pesquisa)

Com relação à busca por reparação, podemos observar as operações de poder entre os envolvidos na fraude, desde as redes que foram palco para tal, às empresas que as representam, o evento em si e as instituições policiais. O discurso das plataformas transfere a responsabilidade para o sujeito, naturalizando a autovigilância e a culpabilização. Assim, o poder circula, descentralizado, disciplinando comportamentos através da norma implícita: “seja cuidadoso, desconfie, proteja-se”. Individualizando de tal forma a culpa por ações desse tipo levando até as vítimas a um constrangimento que as impedem de buscar a polícia.

> Sim, hoje em dia eu basicamente só uso aplicativos de bancos para resolver todas as minhas questões financeiras… eu tenho evitado ir para bancos por questão de ser mais prático. (Entrevista com Mariana para essa pesquisa)

O letramento digital de Mariana, ainda que ela afirme não fazer mais tanto uso da internet como antes, é demonstrado e aprendido na prática. Ela afirma fazer uso constante de diversos aparelhos, aplicativos como internet banking e possuir estratégias de segurança (como usar e-mails específicos e evitar exposição de dados pessoais). Assim como no caso anterior, podemos afirmar que há um capital técnico considerável aqui e diretamente relacionado com a classe e escolaridade de Mariana. Ela age como alguém que domina o espaço digital e compreende suas lógicas estruturais.

Mas vale destacar que este episódio também nos mostra o quão o letramento digital não pode ser visto de forma unidimensional. Há um contraste entre as habilidades técnicas, o acúmulo de experiência de Mariana com a internet e a menor familiaridade da companheira, que tomou a frente da transação. Essa assimetria ilustra como o letramento digital é um campo relacional, atravessado por disposições, afetos e poder simbólico. A pessoa que assume a frente de cada clique é também quem ocupa, ainda que naquele instante, a posição mais vulnerável. A urgência e o desejo de garantir o ingresso, de participar de um evento, impactam no exercício racional daquela transação e ativam um modo de ação mais ligado ao emocional, onde as expectativas se sobrepõem às avaliações técnicas e racionais.

Goffman nos ajuda a entender esse deslocamento do racional para o emocional. A pressa e pouca possibilidade de aquisição daquele produto constroem um cenário que sustenta a performance de confiança e, por conseguinte, reduz a distância reflexiva entre estímulo e ação. Ao passo que, quando o ambiente é digital, percebemos uma pedagogia invisível da internet, que pressiona os sujeitos a agir com rapidez, agir sem grande reflexão, responder instantaneamente, perpetuando a lógica do controle pelo impulso.

E podemos pensar com Hine novamente sobre o quanto o aprendizado é prático e situado quando Mariana reconhece que “prestou mais atenção depois que aconteceu”. O aprendizado se dá a posteriori, pelo trauma, fortalecendo o quanto há ausência de formação emocional para o uso das tecnologias. E mostrando como o letramento digital para ser de fato efetivo, demanda também à capacidade de autogerir emoções e vulnerabilidades.

> Sim, porque basicamente a gente abordou no próprio instagram. Então, as outras pessoas que estavam ali naquela movimentação pra também comprarem ingresso... ela ficaram... elas receberam bem e se engajaram no nosso protesto por assim dizer, pela nossa denúncia. Eai... no caso delas sim, mas no caso de outras pessoas a gente fica um pouco constrangido comentar sobre o que aconteceu. Porque... é como se a gente tivesse ido atrás do golpe, entendeu? (Entrevista com Mariana para essa pesquisa)

No pós golpe de Mariana as perdas também não se reduzem ao financeiro. Vemos nas falas de Mariana com frequência a ideia de que ela se sentiu “emburrecida, culpada”, um impacto moral e subjetivo que acompanha a vítima mesmo após a execução da fraude. O constrangimento, descrito repetidas vezes, corrobora com a individualização das experiências online e funciona como um mecanismo disciplinador. A vergonha ocupa uma ação onde Estado falha, silencia denúncias e reduz drasticamente as possibilidades de reparação.

> Eu evito comprar coisas de sites e perfis não oficiais, apesar de que até perfis, aparentemente oficiais, estão sendo utilizados pra golpe, então... é... eu tenho evitado fazer compras em sites que eu já não fazia, sabe,... Esses sites que abrem muito espaço pra uma terceirização da venda, eu evito. Então, basicamente eu só compro na amazon e na shoppee porque são os canais que eu sei que... que o dinheiro... ou no mercado livre, que o dinheiro vai ser ressarcido caso ocorra alguma tentativa de fraude. (entrevista com Mariana para essa pesquisa)

Esse processo e o que se aprende com ele impacta diretamente a sociabilidade digital. Mariana reconfigurou suas atividades de compras mediadas pela internet e passou a evitar compras fora de plataformas reconhecidas, diminuir interações e evitar ao máximo a exposição, buscou cada vez mais mecanismos de autoproteção (e-mails específicos, codinomes). Mais uma vez um movimento de reconfiguração e adaptação diante do risco.

Em termos do simbólico há um impacto também em sua posição social e cognitiva. O golpe para além dos sentimentos já mencionados também os aprofunda a partir da narrativa de que, mesmo sendo “instruída” e portadora de um diploma ela foi vítima, caiu em um golpe, gerando uma ruptura entre sua identidade e sua experiência. Essa ruptura provoca um desacordo entre os capitais simbólicos que ela possui e sua experiência, ou o que, em termo goffmanianos, poderia ser visto como uma quebra de uma fachada já consolidada, uma vez que sua imagem enquanto detentora de intelectualidade é posta em xeque.

A diferença aqui no campo emocional se dá na medida em que o golpe foi experienciado por duas pessoas e que constituem um casal, então mesmo com a falta de suporte comum a esses casos, elas tem uma a outra para compartilhar. A ausência do estado e das plataformas é brevemente ocupada por essa rede afetiva de acolhimento, ainda que marcadas pela vergonha. Em suma, reforça o quanto a questão econômica não é o único fator relevante no golpe, mas também uma

reconfiguração do modo como o sujeito se inscreve na moral da conectividade, o digital deixa de ser espaço apenas de prazer e passa a ser território de risco.

> É... eu acredito que seja uma questão de constrangimento, tipo assim, da gente não querer falar sobre. Então, a sorte é que no nosso caso nós duas sofremos o golpe, então a gente meio que consolou uma a outra, entendeu!? Mas acredito que a gente não falaria pra ninguém, assim nesse sentido. (Entrevista com Mariana para essa pesquisa)

- **Luciana** e a OLX como mediadora de compras e vendas

A vulnerabilidade em ambientes digitais fica explícita no relato de Luciana. É possível observar como elementos como estrutura social e afetividade se cruzam nas práticas cotidianas mediadas por tecnologia informacional.

> Daí eu fui fazer um... publicar um produto pra vender na OLX. Publiquei e, com segundos após que eu publiquei esse meu produto, me veio uma mensagem por whatsapp dizendo que a minha publicação só ficaria ativa após eu confirmar o código da OLX. Se não, não ficaria ativa. (Entrevista com Luciana para essa pesquisa)

A fraude por ela narrada e sofrida aconteceu atravessada por várias plataformas, OLX, SMS e WhatsApp, o que já demonstra o caráter complexo do que Hine chama de espaço etnográfico digital, apresentando camadas de interação e suas múltiplas formas de manifestação que vão desde o texto, a interface ao automatismo na construção de uma experiência de credibilidade. Esse caso apresenta uma forte utilização da estética como atribuidora de legitimidade: o fraudador se vale da linguagem institucional da OLX e do design comunicacional típico de mensagens oficiais, com “logo, formalidade textual e um tom burocrático”. O dispositivo técnico, nesse caso, é também um dispositivo simbólico, em termos de seu impacto social e cultural que atua sobre a confiança.

Há um processo de regulação da impressão onde a vítima, recebendo a mensagem nesse contexto e tempo hábil, entende a ação como continuação natural de seu próprio ato de publicar o produto. Considerando a verossimilhança da ação ao modus operandi da plataforma, o fraudador interpreta o papel institucional. O frontstage dessa relação, o discurso e o formato do contato, é tão convincente que o backstage (o pensamento crítico, a desconfiança) é momentaneamente suspenso. Luciana é capturada pela coerência performática, não pela ingenuidade.

> Eu estava fazendo mil e uma coisas no momento, não me atentei, só que, na mesma hora que eles falaram, o código chegou e eu vi pela barra de notificação mesmo, só copiei o código e mandei.

Se pensarmos o habitus digital nas expectativas sobre essas ações, podemos interpretar que este pesou junto da formação social da interlocutora. Luciana reforça que seu domínio sobre o digital é “básico”, *“Pra redes sociais, pra fazer transações bancárias, e basicamente isso. Eu não trabalho com internet, eu*

não sei nem editar uma foto." (Entrevista com Luciana para essa pesquisa), ainda que ela tenha alguma familiaridade com ferramentas tidas como essenciais. Seu habitus é construído pelo uso no dia a dia e bastante pontual da internet, de forma mais utilitária, não simbólica, uma característica comum às classes médias urbanas tanto por necessidade formal, quanto por praticidade e pertencimento tecnológico. "Sim, tinha OLX, tinha tudo bem bonitinho" (Entrevista com Luciana para essa pesquisa). A confiança atribuída a uma interface institucional, que a faz crer de imediato que a própria OLX lhe mandou mensagem, expressa a internalização do capital simbólico das marcas e plataformas, o que as torna agentes legitimadores na estrutura de poder digital e na execução das fraudes.

O formato técnico da comunicação produz um efeito de verdade, a interface "comunica como a instituição" e dessa forma conduz a interação. Há o exercício de um poder aqui, ainda que não de forma coercitiva, mas que orienta o comportamento do sujeito se a necessidade de ordens explícitas e ainda assim resultando no cumprimento das normas implícitas do ambiente digital (confirmar códigos, clicar rapidamente, autorizar acessos). Luciana mesmo reconhece ter enviado o código sem sequer abrir a mensagem (apenas visualizando pela notificação), agiu como um gesto automático que pode ser compreendido como uma disciplina funcional que Foucault aponta como fruto da modernidade disciplinar.

> Porque foi com exatos segundos que eu tinha postado, segundos. Não fazia um minuto. Eu achei que fosse uma mensagem automática da OLX. Como eles sabem? Não sei se eles ficam ali olhando porque tu já viu que na OLX diz a exata hora que a pessoa postou? E quando ela posta com minutos tem lá, 32 minutos, 30 minutos que a pessoa postou. Então eu não desconfiei por conta disso porque faziam segundos. Foi eu postar o produto, chegar a mensagem já no meu whatsapp.(Entrevista com Luciana para essa pesquisa)

O letramento digital de Luciana, ainda que seja, em seu relato, apontado como básico, revela competências situadas em suas falas na medida em que não se reduzem ao uso técnico. Ela possui em sua experiência prática transações bancárias, a compreensão da importância do selo de verificação e a identificação de mudanças institucionais. Mais uma vez podemos observar o quão prático é o letramento, profundamente contextual e construído nas experiências e necessidades cotidianas. Trata-se de uma usuária periférica da tecnologia, mas sem domínio reflexivo total das regras do campo.

A diferença entre a vulnerabilidade de Luciana e as supracitadas não se dá pela ausência de conhecimento técnico e sim pela fragilidade emocional e temporal da ação. A ideia de como sua capacidade cognitiva estava voltada para outras atividades produz um cenário de ritmo acelerado e fértil para a infiltração de golpes. Goffman explicaria isso como uma quebra momentânea na gestão da impressão: sob pressão e sobrecarga, a atenção se desloca, e o sujeito age performativamente, responde ao estímulo sem reelaborar o contexto. O ambiente digital, desenhado para a instantaneidade, captura o usuário exatamente nesse lapso.

> Rapaz, você se sente primeiramente burra. É... porque eu baixei a notificação, se eu tivesse abrido a mensagem, ia ter lá dizendo que era do whatsapp. Então no primeiro momento eu me achei burra e em segundo momento você fica... é quase a mesma coisa de você ser roubado de verdade, como quem rouba um celular ou algo seu, você se sente assim impotente. (Entrevista com Luciana para essa pesquisa)

A reação de Luciana após a consolidação do golpe, a vergonha, a atribuição de características depreciativas, nos mostra uma tecnologia de sujeição como diria Foucault, de modo que o poder não está apenas no ato do golpe, mas no disciplinamento subjetivo e nos sentimentos como a culpa que são gerados com ele. O sentimento de incompetência funciona como um mecanismo de controle moral, levando a vítima a ajustar seus comportamentos futuros, internalizando a norma da “cautela constante”.

> Sim, tomei um cuidado diferente. Até hoje em dia eu tomo, questão de SMS, de verificar se realmente é um banco, de olhar o número. O whatsapp hoje é... aparece lá como oficial, que facilita muito, antigamente não tinha aquele… Aquele selo de oficial, eu procuro ver aquele selo, se ele é de verdade, só comecei a tomar um cuidado a mais. (Entrevista com Luciana para essa pesquisa)

O desenvolvimento cognitivo de Luciana é atravessado por essa experiência de modo a aprofundar sua consciência reflexiva do risco e a incorporar novas práticas de cuidado Há um aprendizado experiencial e afetivo, onde o trauma se converte em vigilância e prudência, um aprofundamento do caráter emocional do letramento digital.

O golpe gera em Luciana um impacto que vai do emocional ao simbólico. Quando ela afirma o sentimento semelhante ao de ter sido roubada e ficado impotente, ela explicita como o dano não se reduz ao financeiro. O “roubo” toma dela sua identidade simbólica e digital no whatsapp. É sequestrado uma extensão

de sua sociabilidade digital para que sua imagem seja usada para enganar pessoas próximas.

> Inclusive esse amigo meu que na época "emprestou" eu já tinha pedido dinheiro a ele acho que um mês antes, por isso ele não desconfiou. E eu acho que ele (o fraudador) olhou, ele recuperou né? Fez backup. Ele pediu quase o exato mesmo valor. (Entrevista com Luciana para essa pesquisa)

Nesse sentido, o golpe age como uma forma de violência relacional e moral. O fato de um amigo ter transferido dinheiro “porque ela já tinha pedido antes” mostra a profundidade da performance de confiança, o golpe opera dentro da intimidade.

A falta de respostas institucionais e sociais mesmo após ter feito B.O. e comunicado para as pessoas reforça o desamparo da vítima. A polícia não ofereceu solução, e a rede afetiva reagiu com julgamento ao invés de acolher. Mais uma vez a vítima é responsabilizada pela própria vulnerabilidade e pelo golpe, reforçando o estigma e disciplinamento através de sentimentos como a vergonha e o constrangimento.

Na medida que avança o tempo, Luciana também modifica sua relação com as redes sociais digitais e plataformas, passa a evitar a OLX e aderir maiores cuidados com relação a compras e vendas, pesquisando antecedentes de vendedores e dando maior atenção às avaliações coletivas. Esse habitus digital, antes atravessado por uma visão mais ingênua, é deslocado até um habitus com maior prudência.

O caso de Luciana expressa os paradoxos da vida digital contemporânea onde sujeitos ainda que contem com determinado grau de letramento em termos tecnológicos, são desamparados emocional e institucionalmente, uma plataforma, como a do caso, simula autoridade, mas não protege seus usuários.

- Janete e as vendas por plataforma digital

> E essa cliente não quis se identificar, mas ela era daqui de Fortaleza, fez a compra e pagou no cartão. Pediu o link para pagar pelo cartão, e nessa época a gente fornecia. A gente vendia por link e nunca tinha acontecido isso, da cliente pedir estorno. (Entrevista com Janete para essa pesquisa)

Diferente dos casos anteriores, Janete ocupa o lugar da proponente da venda sendo uma vendedora com negócio próprio e que oferta a possibilidade de pagamento mediado pela internet. O golpe do qual ela foi vítima se dá no cruzamento de performances de confiança por parte da fraudadora, do design e do funcionamento institucional das plataformas digitais. Com linguagem informal e fluída e se valendo de um repertório de comunicação comum a este tipo de transação se inicia a conversa com a fraudadora que, naquele momento, era apenas uma compradora. “Vou comprar agora”, “envia o link”, “o motoboy está a caminho” diversas expressões comum ao contexto de negociação. Como diria Goffman, há aqui uma dramaturgia de credibilidade onde o golpista reproduz o que se espera de uma cliente comum, familiar, com gestos de compra que ativam o frontstage comercial de Janete. O cenário, dividido entre o WhatsApp e o Mercado Pago, legitima a performance carregando esse caráter de oficialidade.

> Só que ela comprou três vezes utilizando o cartão, todas as três vezes foram compras grandes de 900, 1100 e uma de 800 e pouco, que foi a última, que na mesma hora foi contestada. Ai na mesma hora eu entrei em contato com ela. Eu ainda não tinha entregado as mercadorias. A última, só a última, porque as outras duas eu já tinha enviado. Ela já tinha mandado o motoboy pegar. E a última eu entrei em contato com ela e falei o que tinha acontecido. E ela falou "Nossa, é porque esse cartão é da minha tia. Eu não sei o que aconteceu, eu vou falar com ela" e sumiu.(Entrevista com Janete para essa pesquisa)

A fraude se apresenta nesse evento como uma performance sociotécnica e apresenta como as plataformas estruturam a percepção de autenticidade e não são neutras.

> …a mercado pago gera um comprovante pra gente também, certo? Só que esse comprovante não dá acesso a tudo. É tipo assim, só o final. Cartão NuBank, cartão... entendeu? E o último nome. E ai foi quando eu percebi que todas as compras foram em cartões diferentes e que nenhuma tinha sido parcelada (Entrevista com Janete para essa pesquisa)

O layout do comprovante de pagamento, com os dados limitados ou incompletos, funciona como um elemento de persuasão visual, e o próprio fluxo comunicacional das interfaces favorece respostas rápidas e resguarda menos

tempo a dúvida. Cabe considerar que Janete já possui um habitus comercial e digital com relação a sua atuação enquanto trabalhadora autônoma, mas isso não impede que seu capital técnico seja não reflexivo, ainda que seja construído no cotidiano das vendas, há uma sustentação em valores de confiança interpessoal. O envio do link para pagamento sem a desconfiança e verificação, sem o estranhamento dos cartões diferentes, é expressão desse habitus: uma disposição a agir de forma eficiente e cordial, típica de quem aprendeu a negociar pela internet como extensão das relações presenciais.

> Por que, tipo assim, às vezes, até mesmo quando alguma de nós ia passar o cartão. Pessoas que iam passar o cartão e não dava certo. Pediam pra verificar. Então eu achei que a mercado pago tinha alguma coisa de segurança. Algum método de segurança que fosse eficaz, tipo, a mesma cliente entrar no site três vezes no aplicativo. Três vezes e usar três cartões diferentes? Eu pensei que eles tivessem esse mecanismo de segurança pra evitar com que a pessoa fizesse isso. (Entrevista com Janete para essa pesquisa)

Podemos observar também como o exercício do poder não se concentra no engano, mas também como as estruturas tecnológicas orientam condutas. A comunicação oficializada pelo Mercado Pago somada a ideia de que o “cliente tem sempre razão” regulam comportamentos por meio da normalização: Janete não encontra outra alternativa a não ser seguir o fluxo da plataforma, mesmo diante de dúvidas, pois agir fora dele significaria romper com a racionalidade comercial dominante.

> Continuo vendendo por links, só que não mais pela mercado pago, agora é pela Infinity. E só para clientes mesmo qeu eu já vendia antes de tudo isso. Que já me compravam há muito tempo. Esse método de pagamento é só pra clientes mesmo que está comigo já desde o inicio. (Entrevista com Janete para essa pesquisa|)

Essa cena se observa no contexto de Sociedade em Rede apresentado por Manuel Castells na medida em que o golpe só é possível porque a vida econômica e simbólica está distribuída em fluxos digitais, e a confiança se desloca do relacional para sistemas informacionais. O risco se torna estrutural e invisível, embutido na infraestrutura das redes.

Janete apresenta um letramento digital funcional, desenvolvido em uma prática recorrente de se valer de plataformas de pagamento, redes sociais, aplicativos de entrega e ferramentas de comunicação com clientes. Ainda assim, a

entrevista explora os limites desse saber prático quando o contexto emocional interfere.

> Eu até fechei a loja, eu também tinha acabado de perder o vô, foi na época que o vô morreu. Estava muito recente, foi uma dor juntando com a outra e aquilo acabou comigo. Eu não conseguia, não conseguia. Não tinha forças pra nada… …Eu acredito que sim porque eu sempre fui muito atenta em relação a isso. E nessa época quando a gente voltou com a loja eu percebia que eu estava muito desatenta, até soma eu estava errando (Entrevista com Janete para essa pesquisa)

Quando o golpe aconteceu, Janete vivia um período de luto e sobrecarga emocional que a desestabilizou reduzindo sua capacidade crítica e atenção aos estímulos digitais. Ao afetar o controle de sua fachada a usuária passa a responder de forma automática, guiada por rotinas internalizadas, e não por análise consciente.

Janete internalizou o controle de tal forma de modo a se responsabilizar por sua vigilância. Observou os sinais que ela não observou anteriormente e teve sentimentos como medo e culpa motivando mudanças de comportamento, regulando suas práticas e transformando o trauma em regra moral: “Mudou muito, porque eu passei a não confiar mais em todo mundo. Principalmente clientes de Fortaleza. Não vendo por link de cartão pra clientes daqui de Fortaleza.” (Entrevista com Janete para essa pesquisa. .

Os prejuízos na vida de Janete causados por esse golpe vão desde os financeiros e materiais, a perda de mais de R$3.000 em produtos e a desestabilização do capital que gerou o fechamento temporário de sua loja e o impacto emocional na medida em que ela atribui o sucesso do golpe à “incapacidade” e à perda de concentração que ela sentiu, narrando que se sentia “no automático” após o luto.

> Eu fiz B.O. Eu entrei com uma ação contra a mercado pago, tentei de tudo, mas no final era um processo muito longo e muito cansativo. Eu acabei mesmo que deixando pra lá… porque uma ficava me jogando pra outra. (Entrevista com Janete para essa pesquisa)

As instituições envolvidas e que a deveriam proteger, Mercado Pago, Procon, polícia, fragmentam a responsabilidade e devolvem a culpa à vítima, se tornando uma pedagogia implícita sobre o comportamento da vítima. Ainda assim, a resposta de Janete não é de desistência, mas de reorganização.

> Sim, eu comentei. Tem um grupo de fabricantes no whatsapp. De lojistas da feira e eu coloquei lá. E eu descobri que eu não era a única. Que é muito comum isso acontecer, também por PIX, que fazem PIX agendado, PIX falso, e na correria o pessoal acaba caindo. (Entrevista com Janete para essa pesquisa)

Ela passa a modificar sua presença nos grupos de vendedores, promovendo alertas e informações e criando novas rotinas de checagem. Uma reconfiguração da presença em rede que reconstitui a confiança coletivamente.

A entrevista de Janete é um bom exemplo de como um habitus permeado por confiança pode se deslocar para uma lógica de maior prudência. Se antes a oferta de links e demais ferramentas do comércio digital era uma extensão natural do seu trabalho como empreendedora, agora ele se torna um campo de tensão, cercado por protocolos, estratégias e verificações. Podemos observar a ambiguidade da vida contemporânea em ambientes digitais a partir desse novo estado de alerta ao mesmo tempo em que amplia possibilidades de renda e visibilidade, impõe uma sobrecarga cognitiva e emocional permanente. Janete, como tantas outras mulheres trabalhadoras autônomas, surge mais vigilante, mas também mais cansada e desconfiada.

A história vivida por Janete nos mostra que a vulnerabilidade digita é menos uma falha individual e mais um evento atravessado por diversos fatores externos, o que, reforça o quão necessário é que o letramento digital ocupe um lugar de maior relevância em nossos processos de socialização.

> Eu acho que as pessoas tinham que desconfiar de tudo. Ah é um cliente normal. Às vezes não é. Às vezes não é! A gente tem que estar atento, a gente tem que... literalmente ficar atento mesmo. Porque hoje eles inventam de tudo. É dinheiro falso, PIX falso, é... então também tem o golpe da maquineta, que eles botam e não passam e eles fazem sair o papel do mesmo jeito como se tivesse passado e não passou. Então, tipo assim, é golpe de tudo que é jeito. A gente tem que ficar sempre atento e se certificar sempre. (Entrevista com Janete para essa pesquisa)

- Rafael e a desconfiança mesmo na urgência

O caso de Rafael é o único caso protagonizado por um sujeito do gênero masculino não por uma escolha desta pesquisa, mas porque no processo de busca de interlocuções a presença e disposição de mulheres a compartilhar relatos foi superior e mais possível. A entrevista com Rafael também nos oferece uma narrativa diferente dos outros casos apresentados, pois, ainda que este caso não apresente uma fraude que obteve sucesso, podem ser observadas estruturas de confiança, vigilância e racionalidade técnica que organizam a vida digital contemporânea.

> Ai como eu estava lá bem de verba, fui atrás de uma usada pra poder suprir a necessidade imediata e depois comprar uma melhor. E aí apareceu uma boa num preço bem tentador. Não era tão baixo pra deixar na cara que era golpe e nem tão cara que não coubesse no bolso. (Entrevista com Rafael para essa pesquisa)

A fraude relatada por Rafael também apresenta como relevantes uma verossimilhança técnica e a forma como é posta a comunicação. O golpe se inicia a partir de um anúncio, muito bem munido de imagens, dados e endereço e número de contato. Nesse caso explicita-se como a fraude depende de uma gestão de impressão e da confiança gerada por uma coerência estética e performativa, os dados eram reais, assim como as fotos, apenas o número de contato sendo trocado. O fraudador em comunicação com Rafael domina a dramaturgia da autenticidade, apresenta uma linguagem técnica e rica em detalhes sobre o produto e reproduz a linguagem impessoal de um vendedor profissional. A desconfiança inicial é desarmada pela normalidade com que ocorre a transação neste “palco digital".

> Eu fui... comecei a trocar com o cara, né? E foi um papo normal, falava normal, passava o endereço. Ele estava usando o... como é que funciona, ele pega o anúncio de uma pessoa real, ele pega um anúncio real. Ele faz uma cópia exata, ele anuncia com as mesmas fotos e os mesmos dados, o mesmo endereço, só muda o número de telefone. (Entrevista com Rafael para essa pesquisa)

Esse caso demonstra também o quanto a infraestrutura digital é parte ativa da performance. A OLX, enquanto plataforma, não garante a autenticidade da identidade dos autores de propostas de vendas, ainda que organize, em certa medida, a confiança por meio de layout, filtros e fluxos de interação. O usuário percebe a plataforma como espaço seguro justamente porque ela performa

segurança, mas são nos sinais construídos pelo próprio sistema que o fraudador encontra espaço para aplicar seus golpes.

> Quando eu fui buscar eu filtrei por valor na OLX e caiu esse. E aí começou, conversa normal, falei com ele pela OLX, fui falando, mandei mensagem no whatsapp e começamos a conversar, aí foi que a gente fechou um acordo, um valor e aí eu fui lá, na casa do verdadeiro dono. (Entrevista com Rafael para essa pesquisa)

Ao falarmos sobre a atuação do habitus de Rafael podemos identificá-lo como tecnocêntrico e relacionado a sua área de atuação profissional, ele se mostra atento aos detalhes e aspectos técnicos da comunicação e da transação. Ele se define como “da área de exatas”, “analítico”, alguém cuja confiança se concentra nos dados e na consistência técnica. Essa disposição é o que o sensibiliza a determinados capitais simbólicos (como especificações, números e descrições técnicas) ao passo que o desloca da atenção a aspectos relacionais e afetivos da comunicação. Um ponto relevante dessa interação é justamente o fato do golpista ser capaz de manipular e mobilizar Rafael a sair de casa rumo ao endereço indicado na plataforma devido a seu diálogo com o próprio capital técnico do interlocutor, entregando provas que são satisfatórias as expectativas da possível vítima.

> Ele botou um preço razoável pela TV. E ai... e a consistência dos dados né? Até porque era uma... era uma TV disso aqui e tinha as fotos tudo direitinho. Ele estava agindo perfeitamente como se fosse realmente o dono. (Entrevista com Rafael para essa pesquisa)

O discurso técnico, o formato institucional da OLX e a arquitetura digital funcionam como dispositivos que orientam as condutas. O fraudador age dentro de um regime de verdade produzido pela racionalidade tecnológica, a aparência de formalidade e os dados “consistentes” funcionam como operadores de obediência.

> Rapaz, na minha época a gente fazia curso de informática. Hoje em dia já não se faz, mas eu sei, não só acesso a internet, mas ferramentas de fato. Porque hoje em dia o jovem usa a internet, mas não sabe usar o word. Então eu acho que eu posso dizer com autoridade que eu sei sim. Sou um usuário de tecnologia, até porque eu trabalho com isso. (Entrevista com Rafael para essa pesquisa)

Rafael se apresenta como um indivíduo altamente letrado digitalmente. Foi iniciado a formação técnica desde os 14 anos e atua profissionalmente em um setor em que uso intenso de planilhas, softwares e autenticações múltiplas são recorrentes e exigidos. Observamos esse letramento como diferente dos casos anteriores, o letramento de Rafael é instrumental, especializado e racionalizado. Ele

compreende as ferramentas, entende protocolos de segurança, e até utiliza múltiplos fatores de autenticação**,** práticas típicas de usuários tecnicamente competentes.

> Eu uso autenticator nas minhas contas da microsoft e google, e além disso eu crio um... eu uso múltiplos fatores de autenticação MFA nas minhas contas. Então mesmo que você tenha acesso, é preciso que você tenha (a chave) do acesso. Até porque eu já vi gente sendo hackeada de graça aí, inclusive estavam tentando pegar a minha conta parece que o MFA dificulta o caminho. (Entrevista com Rafael para essa pesquisa)

No entanto, vale destacar que a entrevista com Rafael também expõe como o letramento técnico e ainda que autodeclarado alto, não descarta a vulnerabilidade emocional e cognitiva. Rafael mesmo que não tenha sido “enganado”, reconhece que houveram momentos em que de fato ele acreditou na autenticidade do anúncio e que isso só foi rompido quando o fraudador não sustentou a performance e alterou a linguagem (saiu do personagem).

> Eu acredito mais fácil em coisas quando elas tem dados técnicos, não caio muito naquela conversa comercial subjetiva. Entendeu? Então como o cara tinha realmente os dados da máquina, facilita muito concretizar. (Entrevista com Rafael para essa pesquisa)

A compreensão de Rafael aconteceu após perceber e estranhar uma quebra na coerência do personagem do fraudador e não por um cálculo racional. Essa transição é goffmaniana, a performance do golpista não se sustenta, e o “palco” revela o backstage da fraude.

> E aí enquanto eu estava lá ele ficava instigando, tipo assim... paga logo pra tu levar... entendeu? E é assim que funciona. E como eu já estava achando estranho porque o dono original também não estava na casa, acho que era pai, tio, sei lá, dos que estavam lá. E eu tive contato com o filho e o filho também não estava reconhecendo essa tratativa. Até porque não foi feita com ele. Aí foi que eu mandei ele pr'aquele canto pra testar se ele saia do personagem e ele saiu. Aí eu vi que ele saiu do personagem e pronto, a gente ficou trocando insultos um ao outro e eu achei melhor ir pra casa. (Entrevista com Rafael para essa pesquisa)

O discurso de Rafael apresenta essa distância emocional como meio de proteção, comum a sujeitos que dominam linguagens técnicas. Mesmo a interlocução é narrada com frieza e ironia “Rapaz, foi aquela raiva mais... eu me senti mais caindo numa pegadinha do que uma frustração de fato, tá ligado.” (Entrevista com Rafael para essa pesquisa), atribuindo a racionalidade o lugar do afeto. Essa autodefesa é uma forma de preservar a fachada e não demonstrar o impacto dos sentimentos apresentados nos outros casos, protegendo a coerência

de sua identidade de homem técnico, analítico e autocontrolado. Ainda que tenha afirmado “O cara se sente burro, né? O cara se sente burro, como é que eu fui cair numa merda dessas?” (Entrevista com Rafael para essa pesquisa),, o sentimento de vergonha não aparece nesse relato.

> Não é uma questão de vergonha, é só que é um fato que não vale a pena ser mencionado, pra quem mencionei achou graça. Mas não contei como um desabafo ou frustração. (Entrevista com Rafael para essa pesquisa)

A lógica da vigilância também aparece aqui, mas como uma postura que internaliza isso de modo a também atribuir a si a responsabilidade de sua própria segurança. O uso de MFA, a desconfiança das instituições e a recusa de denunciar são práticas de autogoverno e de desinstitucionalização: Rafael transfere o papel de proteção do Estado para si mesmo, encarnando o sujeito auto vigilante

> Não porque eu não acredito no sistema, não dá em nada. E a maioria não faz por conta disso, então quem é esse cara? Eu não sei. Ninguém vai se dar ao trabalho de rastrear ele pelo número, se é que o número está no nome dele. Então é um cara meio que está fantasmático ali. E... deixei pra lá. (Entrevista com Rafael para essa pesquisa)

Os impactos desse golpe podem ser observados ainda que o mesmo não tenha se consolidado com sucesso, há impactos simbólicos e comportamentais. Rafael reforça sua desconfiança generalizada. E apresenta uma descrença nas instituições como a polícia, plataformas e a justiça em si, se encaminhando a um caminho isolado e defendendo a autossuficiência como forma de defesa.

Esse caso possui de forma sutil marcas afetivas. Rafael quando fala de sentimentos rejeita a ideia de vergonha, não fala em medo ou dor, mas em raiva e ironia, emoções mais socialmente aceitáveis no registro masculino, o que indica também o direcionamento desta fachada. A admissão de sentimentos outros que fogem a este papel e expõem a vulnerabilidade do homem racional autossuficiente seria uma quebra desta fachada, a masculinidade atua aqui como um mecanismo de “controle” emocional.Sobre compartilhar a experiência com alguém, mesmo com a esposa, Rafael afirma:

> Não, eu não fiquei estressado, não. É... ainda mais com ela eu não gosto de por sentimentos de... nesse caso especificamente eu não tive, como eu te disse eu mais senti que eu caí numa pegadinha. E ainda que eu tivesse ficado puto eu não ia compartilhar com ela, não.(Entrevista com Rafael para essa pesquisa)

Um outro elemento interessante dessa interlocução se dá na medida em que a experiência ou trauma não transforma radicalmente a Rafael, mas reforça disposições já existentes e aprofunda um habitus que já é atravessado por ideias de controle e prudência. A recusa em denunciar ou de alocar a busca por reparação como um estresse “que não vale a pena” é um reflexo do funcionamento de um poder que naturaliza a ineficácia institucional. Rafael internalizou o ato de não ter expectativas sobre a justiça e converte essa sensação de abandono institucional em uma suposta autossuficiência.

As análises feitas nesta pesquisa e ao longo deste trabalho nos permitem, a priori, concluir que os golpes cibernéticos ou fraudes digitais não se limitam a desvios individuais, erros de usuários ou falhas técnicas. Mas se constituem como expressões sintomáticas de uma sociabilidade profundamente conectada e mediada por plataformas, onde elementos como confiança, identidade e segurança ficam ainda mais instáveis e permanentemente negociados. Com Castells, se explicita como a autonomia do indivíduo conectado é complexa e paradoxal, pois a busca por proteção mobiliza o sujeito a uma maior dependência de dispositivos técnicos, métodos de autenticação e infra estruturas que operam segundo lógicas alheias à sua vontade. São padrões de vigilância que constantemente se reelaboram sustentando a ideia de uma liberdade digital somados ao autocontrole substituindo formas tradicionais de confiança social.

Os casos analisados mostram esse movimento. A vulnerabilidade se impõe sobre sujeitos dos mais leve ao mais alto grau de letramento digital, não por desconhecimento, mas porque o golpe atua sobre regimes de verdade, afetos e performances identitárias que estruturam a vida online e fazem sentido para cada uma das vítimas. A vulnerabilidade é sociotécnica: emerge nas dinâmicas personalizadas e dos algoritmos, das redes sociais e dos mercados digitais, que produzem ambientes informacionais acelerados e assimétricos. A experiência de Rafael ilustra um mal-estar característico da era digital, marcado pela desconfiança permanente, pela racionalização da solidão e pela transferência progressiva da confiança para mecanismos automatizados.

Nesse sentido, a fraude não se reduz ao acesso indevido a um código; ela opera como uma invasão na arquitetura simbólica do eu conectado. A identidade, os vínculos e a reputação, dimensões antes ancoradas em interações presenciais e instituições sociais dependem agora da mediação técnica, abrindo espaço para formas de poder que exploram a velocidade dos fluxos informacionais e a fragilidade emocional dos sujeitos conectados.

Considera-se, portanto, que a sociologia dos crimes digitais exige compreender a tecnologia não como simples ferramenta, mas como estrutura que redistribui riscos, produz novas formas de desigualdade e reorganiza a gramática da confiança. O golpe, nessa perspectiva, é menos um evento isolado e mais um fenômeno que expressa tensões constitutivas da sociedade em rede. A conectividade incorpora a vida social, afetiva e econômica de forma irremediável e expõe o caráter emocional do que esta pesquisa entende como letramento digital, reforçando a necessidade urgente de políticas públicas, regulações e práticas educativas capazes de recompor formas coletivas de proteção e de reconstruir a confiança para além dos limites das máquinas.

6 CONSIDERAÇÕES FINAIS

A pesquisa apresentada nesta dissertação procurou entender o que chamamos de dramaturgia da fraude como um fenômeno sociotécnico complexo, onde se articulam múltiplos fatores como performances, discursos, narrativas e dispositivos digitais com a finalidade de sofisticar práticas de manipulação. Goffman aparece como central a essa análise por, ao observar eventos semelhantes aos dos relatos, o caráter dramatúrgico e de encenações se mostra evidente e relevante, além de que, essa escolha de pensar as experiências das vítimas nos permite observar tais ações para além da racionalidade dos criminosos e da dimensão tecnológica das fraudes., de modo a direcionar a leitura a uma compreensão que parte da combinação entre vulnerabilidades emocionais, assimetrias de letramento digital e dos exercícios de poder da forma em que estão postos em uma sociedade informacional.

As narrativas e relatos que compõem essa pesquisa explicitam que os crimes cibernéticos, golpes, não ocorrem apenas em razão de falhas técnicas, mas

necessitam de uma construção cuidadosamente performada e dramatúrgica de cenários de confiança, legitimidade e que gerem um senso de urgência. Os golpes, em seu caráter dramatúrgico, mobilizam dispositivos simbólicos diversos como linguagem formal, o design estético das interfaces, simulação de autoridade institucional e exploração do que a vida digital contemporânea produz em termos de fragilidade. A manipulação e sucesso dos golpes se dão menos a partir de um erro individual e mais pela intersecção entre estruturas sociais, emoções e expectativas disseminadas pelo ecossistema digital.

Em suma, as análises realizadas para essa pesquisa expõem o quanto a vulnerabilidade digital não pode ser alocada no lugar de um atributo pessoal, tampouco pode ser resolvida meramente com uma maior atenção por parte dos usuários. Ela é socialmente distribuída e produz impactos diversos na medida em que são atravessados por classe, gênero, raça, idade, escolarização e, principalmente, pelos diferentes graus de letramento digital, entendido aqui como uma forma de inteligência situada, que não se reduz a técnica, mas se articula com confiança, outros elementos emocionais e repertórios culturais. As vítimas não são agentes passivos: a atuação delas nestas tramas simbólicas e que lhes são acessíveis orientam tomadas de decisão dentro dos limites de conhecimento, urgência e pressão emocional do momento.

A pandemia de covid-19 aparece mais como um evento que influenciou um aprofundamento tecnológico que já estava em curso, a dependência de dispositivos digitais para diversas atividades. E o estudo demonstra que isso ocorreu sem que houvesse, no mesmo ritmo, um preparo ou construção de mecanismos sociais, institucionais e pedagógicos capazes de lidar com as demandas desse campo e proteger os sujeitos. Essa disparidade entre os avanços tecnológicos, a apropriação por parte de criminosos e o combate institucional desses crimes aloca os crimes cibernéticos como uma expressão contemporânea das desigualdades estruturais brasileiras, elementos como desigualdade de acesso, de uso de aparelhos, de repertório, de proteção e de capacidade institucional de resposta.

O estudo suscita diversas reflexões para além da pesquisa, nos leva a refletir sobre governança digital, sobre políticas públicas, letramento e de inserção dessa pauta nos campos da educação e da segurança. Na contemporaneidade tem

havido debates acerca da regulação das plataformas e, principalmente, sobre a necessidade urgente de produzir formas de cuidado que tornem possível aos cidadãos compreender a lógica que organiza os ambientes digitais. O que chamamos de dramaturgia da fraude torna explícito os pontos cegos de nossa sociabilidade digitalizada.

Ainda que essa pesquisa não tenha a pretensão de oferecer soluções técnicas definitivas, as reflexões aqui feitas nos ajudam a fazer uma leitura mais sensível e complexa das violências simbólicas que atravessam os ambientes digitais e que, ao serem naturalizadas, por vezes são compreendidas socialmente como responsabilidades individuais. Visibilizar as experiências de vítimas, ainda que em alguns momentos também falemos dos fraudadores, permite ir além dos mecanismos da fraude e nos permite observar as marcas subjetivas deixadas por ela: vergonha, culpa, medo, sentimento de incapacidade e, não raro, o silenciamento, a rejeição de contar com as instituições públicas e privadas para buscar reparação. Cabe ressaltar que produzir um enfoque sobre essa experiências a partir da sociologia nos auxilia a ir além do olhar técnico e realocá-las no centro de um fenômeno que é estrutural, relacional e profundamente marcado por desigualdades, o que remove, simbolicamente, o peso moral do fracasso que se impõe sobre as vítimas.

Se os golpes ou fraudes são encenados, são uma dramaturgia num contexto em que as pessoas estão mais a sós e individualizadas, com experiências personalizadas, entender seus roteiros, cenários e personagens é crucial para a construção de práticas de resistência, educação e proteção capazes de disputar as narrativas e reequilibrar as relações de poder que estruturam a vida digital. Este trabalho com veemência reafirma a urgência de um olhar crítico sobre o presente, para que os futuros (digitais) possíveis sejam menos vulneráveis, mais conscientes e mais justos.

REFERÊNCIAS

ALLIANZ COMMERCIAL. *Allianz Risk Barometer 2025: Identifying the major business risks for 2025*. Allianz Commercial, 2025. Disponível em: https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/240116_Allianz_Media-Release_Allianz-Risk-Barometer-2024.pdf. Acesso em: 15 jun. 2025.

ANTUNES, Ricardo (org.). *Uberização, trabalho digital e Indústria 4.0*. 1. ed. São Paulo: Boitempo, 2020. 336 p. ISBN 978-6557170113

BARROS, Euvaldo. *É fácil pra tu, é fácil pra eles: crimes virtuais em uma sociedade digitalizada*. 2022. Monografia (Graduação em Ciências Sociais) – Universidade Federal do Ceará, Fortaleza, 2022.

BEAUD, Stéphane; WEBER, Florence. *Guia para a pesquisa de campo: produzir e analisar dados etnográficos*. Tradução de Sérgio Joaquim de Almeida. 2. ed. Petrópolis: Vozes, 2014.

BOURDIEU, Pierre. *A dominação masculina*. Tradução de Maria Luiza X. de Almeida. Rio de Janeiro: Bertrand Brasil, 2001.

BOURDIEU, Pierre. *O poder simbólico*. Tradução de M. B. de Queiroz e S. R. Queiroz. Rio de Janeiro: Bertrand Brasil, 2003.

BRASIL. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. *Observatório do Comércio Eletrônico Nacional*. Brasília: MDIC, [2023–atual]. Disponível em: https://www.gov.br/mdic/pt-br/assuntos/observatorio-do-comercio-eletronico. Acesso em: 26 abr. 2025.

CASTELLS, Manuel. *A Era da Informação: Economia, Sociedade e Cultura. Vol. 2 – O Poder da Identidade*. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2001.

CASTELLS, Manuel. *A sociedade em rede: A era da informação – economia, sociedade e cultura*. 6. ed. São Paulo: Paz e Terra, 2002. v. 1.

CAVELTY, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. 1. ed. Londres: Routledge, 2008. ISBN 978-0-415-42981-8.

CERQUEIRA, Matheus Tomaz. *“O negrê é o projeto da minha vida”: entre tramas e vozes à construção de um jornalismo independente negro e nordestino*. 2024. [número de folhas] f. Dissertação (Mestrado em Antropologia) – Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB), Redenção, 2024.

DEIBERT, Ronald J. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. 1. ed. Toronto: McClelland & Stewart, 2013. ISBN 9780771025358.

FOUCAULT, Michel. *A ordem do discurso*. Tradução de Maria Luiza B. de Almeida. São Paulo: Loyola, 1996.

FOUCAULT, Michel. *Vigiar e punir: história da violência nas prisões*. 30. ed. Petrópolis, RJ: Vozes, 2014.

GOFFMAN, Erving. *A representação do eu na vida cotidiana*. 15. ed. Petrópolis, RJ: Vozes, 2015.

GOFFMAN, Erving. *Estigma: a identidade deteriorada*. Tradução de Vera Ribeiro. 3. ed. Rio de Janeiro: Zahar, 2009.

HINE, Christine. *Virtual Ethnography*. London: SAGE Publications, 2000. ISBN 9780761958956.

IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Pesquisa Nacional por Amostra de Domicílios Contínua: resultados de 2024*. Rio de Janeiro: IBGE, 2025.

LÉVY, Pierre. *A inteligência coletiva: por uma antropologia do ciberespaço*. Tradução de Profa. Lucia Santaella e Edgard de Assis. São Paulo: Loyola, 1998.
LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMA, Renato Sérgio de; BUENO, Samira. As novas configurações dos crimes patrimoniais no Brasil. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (Org.). *Anuário brasileiro de segurança pública 2023*. 17. ed. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. p. 90-107.
RIFIOTIS, Teófilo. *Políticas etnográficas no campo da cibercultura*. Porto Alegre: Editora UFRGS, 2014.

SANTAELLA, Lúcia. Para compreender a cibercultura. São Paulo, Ática, 2012.
SOCIEDADE BRASILEIRA DE VAREJO E CONSUMO. *Novos hábitos digitais em tempos de Covid-19*. São Paulo: SBVC, 2020. Disponível em: https://www.aberje.com.br/wp-content/uploads/2020/07/COVID-SBVC-EstudoConsumo.pdf . Acesso em: 25 de maio de 2025
TERCEIRO, Cecílio da Fonseca Vieira Ramalho . O problema na tipificação penal dos crimes virtuais. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7 , n. 58, 1 ago. 2002 . Disponível em: https://jus.com.br/artigos/3186. Acesso em: 4 out. 2022.

VIGNOLI, Richele Grenge; MONTEIRO, Silvana Drumond. Deep Web e Dark Web: similaridades e dissiparidades no contexto da Ciência da Informação. Transinformação, v. 32, p. e190052, 2020.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.