REVISTA DO CAAP
fundada em 1921

CIBERCRIMES NO BRASIL: ANÁLISE DA OPERAÇÃO DARKROOM

Sophia Baccan Noronha[1]

RESUMO: Com o crescente número de novos usuários de internet a cada ano, a sociedade globalizada está cada vez mais conectada através da tecnologia; problemas online dão continuidade ao mundo físico e problemas físicos passam para o mundo online, seguindo os desejos de criminosos, que possuem maior rede para atrair suas vítimas. Assim, em face da onda de cibercriminalidade suprimida pelas forças policiais nas últimas décadas, o estudo busca examinar a relação de ambientes virtuais, sua organização e interpretação, sob a óptica da criminalidade, de modo a identificar dimensões da formação de crime nas redes e auxiliar na resolução de casos futuros. Utiliza-se a metodologia de pesquisa descritiva sobre a "Operação Dark Room" – também chamada popularmente de "Caso Discord", a qual se refere a uma série de crimes de violência sexual cometidos dentro da plataforma –, em estudo de caso, de modo a averiguar o *modus operandi* dos crimes, a diferença de personalidade online e offline, método de caça e sadismo. O artigo realiza, ainda, uma análise de crimes virtuais e a posição nacional sobre o tema, trazendo luz quanto às dimensões do problema.

Palavras-chave: cibercriminologia, direitos digitais, comportamento desviante online

[1] Graduanda na Universidade Federal de Minas Gerais (UFMG). ORCID: https://orcid.org/0009-0000-8660-5665. E-mail: sosobaccan@gmail.com

Revista do Centro Acadêmico Afonso Pena, Belo Horizonte, Vol. 29, N. 2, 2024

ISSN (impresso): 1415-0344 | ISSN (online): 2238-3840

Editor responsável: Raphael Geraldo Estanislau Vaz Ribeiro | Revisão: Maryanne Pimenta Fargnoli

Data de Submissão: 02/09/2024 | Data de Aceite: 30/12/2024

CYBERCRIMES IN BRAZIL: AN ANALYSIS OF OPERATION DARKROOM

ABSTRACT: Upon the growing number of new internet users every year, the globalized society is increasingly connecting through technology; online problems continue into the physical world and physical problems move into the online world, fulfilling the will of criminals who have a larger network to attract their victims. Thus, as the wave of cybercrime is suppressed by police forces in recent decades, this study seeks to examine the relationship between virtual spaces, their structure and interpretation, from the perspective of crime, in order to suggest the dimensions of the development of the crime on the web and provide a base for the resolution of future cases. A descriptive research methodology is used on "Operation Darkroom" – also popularly called the "Discord Case", which refers to a series of sexual violence crimes committed on the platform – in a case study with analysis, in order to ascertain the *modus operandi* of the crimes, the difference of online and offline persona, the hunting method and the sadism. The article also carries out an analysis of cybercrime and the national position on the subject, so that it can make the dimension of the problem understandable.
Keywords: cybercriminology, digital law, deviant online behavior.

INTRODUÇÃO

O cenário de cibercriminalidade atual se formou, durante as últimas décadas, escorado na convergência de tecnologias de informação e comunicação global. Elevadas ao extremo devido ao crescimento exponencial de usuários e ao desenvolvimento de novos canais para a prática criminosa, a internet se tornou meio e objeto para aqueles que desejam usá-la para infringir a lei. O alcance transnacional e a estruturação de habilidades adjuntas ao sistema computacional possibilitaram a orquestração dos ataques e suas dinâmicas em uma maior possibilidade geográfica e em toda a extensão de crimes.

Yepes (2016) considera essencial o conhecimento extenso da polícia em várias disciplinas para êxito na detenção de infratores digitais, sendo que a investigação forense digital, as técnicas de entrevista e interrogatório e o conhecimento de linguagem entre pares são dispositivos importantes para análise de propagação, replicação, ocorrência e perfil de vítimas e criminosos. Esse tipo de conhecimento ajuda a conter os casos e a obter formas válidas de denúncias contra criminosos que acham que podem ficar "acima da lei" (TJRJ, 2024). Outros

pesquisadores também apontam a importância de compreender a vitimologia (Oerlemans; Van der Wagen, 2022; Olshaker; Douglas, 2021), a linguagem entre pares (Kurek, 2018; UNODC, 2013; Cooper, 2000), psicologia geral (Katz, 1989; Suler, 2004; Douglas et al, 2006), conhecimentos digitais (Goldsmith; Wall, 2019; Wall, 2005; Yepes, 2016) e direito criminal nacional (MPRJ, 2023; TJRJ, 2024).

O presente estudo tem como objetivo compreender a relação de ambientes virtuais, sua interpretação e organização, sob a óptica da criminalidade, perpassando por delitos, crimes e infrações nacionais, de modo a sugerir dimensões da formação desse crime nas redes e propiciar a resolução de casos emergentes.

O artigo analisa os conceitos pautados em estudo de caso de crimes acontecidos no Brasil, que ficou conhecido como "Crimes do Discord" – por terem acontecido nessa plataforma – ou, pelo nome da operação policial "Operação Darkroom".

O artigo se divide nas seções: Aumento de Tecnologia e Preceitos Básicos, em que serão introduzidos dados sobre o aumento global de tecnologia e comunicação na era digital; Discussão sobre Cibercrimes, na qual serão apresentados conceitos gerais e específicos acerca dos crimes cometidos em ambiente virtual; em seguida se aprofundará na Visão da Cibercriminalidade no Brasil.

1 AUMENTO DE TECNOLOGIA E PRECEITOS BÁSICOS

Em 2011, foram estimados 2.3 bilhões de usuários de internet, apenas um terço da população mundial da época (UNODC, 2013). Em comparação, durante janeiro de 2024, pode-se perceber o dobro do número, com 5.35 bilhões de usuários de internet e pouco mais de dois terços da população (Data Reporter, 2024). A explosão de conectividade se deu pela adequação global ao novo sistema socioeconômico do século XXI de maneira tão rápida que não houve controle de suas consequências – o aumento do cibercrime intrínseco a esses fatores (UNODC, 2013).

A utilização de computadores e telefones celulares adentrou a vida quotidiana, de modo que se observou a criação de uma nova estrutura física e sociológica de comunicação

(McDowell, 1997). As interfaces de uso[2] se tornaram mais intuitivas e, os produtos, mais baratos e fáceis de utilizar; empresas e famílias adotaram o novo ambiente para mandarem mensagens pela própria rede, permitindo que as pessoas permanecessem em contato por outro meio que não as cartas (Lloyd, 2005). A oportunidade de se conhecer pessoas sem sair de casa ou de se permanecer atualizado com as notícias sem consumir qualquer jornal físico demonstra a mudança contínua de meios de informações e contatos, que alteraram não apenas as relações interpessoais, mas também a relação dessas com o Estado, a partir de um novo canal para a prática de comportamentos criminosos (Wall, 2005).

O alcance para esses atos prejudiciais é tão amplo quanto a própria internet. Assim, mesmo que a natureza fundamental dos crimes pareça familiar – com o objetivo de crimes já conhecidos anteriormente, como roubo ou pornogafia infantil – há uma mudança no padrão comportamental orientado por essa ferramenta (Wall, 2005). O grande número de oportunidades, a velocidade e o anonimato, por exemplo, são elementos chave para esse tipo de crime, que apenas esse território consegue prover – como Cooper (2000) propôs em sua teoria sobre quais motivos fariam a internet tão chamativa.

As oportunidades aparecem entre pessoas com mesmos interesses que se encontram em fóruns específicos para discutir os crimes e aprimorá-los (UNODC, 2013), ou na própria rede que acaba levando as possíveis vítimas aos infratores. Durante as entrevistas conduzidas por Steinmetz com hackers dispostos a comentar suas primeiras motivações para o crime virtual, um dos entrevistados constatou que a vasta escala da internet – devido ao seu fácil acesso – significa que não há carência de alvos ou oportunidades para quem deseja iniciar ou desenvolver suas habilidades (Steinmetz, 2016). Os algoritmos[3], ainda, de modo imperceptível e quase incompreensível mesmo para os mais experientes no uso da internet, atuam de modo influente ao conectar as vítimas aos agressores (Finn, 2017), de maneira fácil e irracional; assim que o criminoso determina seu padrão e age ostensivamente para infringi-lo, a internet é capaz

[2] Interface de uso é o espaço entre a interação dos humanos e o sistema operacional da máquina; cria a possibilidade de controle sobre suas atividades. Quanto mais intuitiva a interface, mais pessoas utilizam o serviço – o que influenciou a criação do Sistema de Nomes de Domínios para que mais pessoas pudessem utilizá-lo (Leiner et al., 2003).

[3] Segundo o Dicionário de Oxford, "algoritmo" é definido como um "conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas". Na internet, os algoritmos são responsáveis por processar um grande número de informações rapidamente. Eles são utilizados, muitas vezes, como um filtro que une gostos, pesquisas e comportamentos e alinham o indivíduo a um tipo de grupo buscando "melhorar sua experiência" criando recomendações personalizadas.

de conectar indivíduos parecidos com base em suas características. O processo ocorre de maneira subconsciente, sem que pareçam estar se adequando, lentamente, a essa dinâmica.

Aqui, tanto a abordagem do "estilo de vida" de Hindelang, Gottfredson e Garofalo (1978) quanto a teoria da "atividade rotineira" de Cohen e Felson (1979) são analisadas de maneira virtual. A primeira teoria defende que comportamentos de determinados indivíduos podem os expor a determinadas situações de risco, enquanto a segunda considera que o ato de "tornar-se vítima" é resultado da intenção do infrator. No ambiente digital, ambas as teorias se mostram verdadeiras, já que os possíveis criminosos podem ir a lugares específicos da rede com base no comportamento que esperam de suas vítimas (por exemplo, os que procuram por pessoas idosas podem facilmente encontrar em grupos com esses participantes), assim como o algoritmo, novamente, impulsiona esse contato.

Em crimes contra a máquina (*hacking*, *malware*, ataques de dados, r*ansomware*, *botnets* e outros), a vitimologia é direcionada ao sistema computacional, permitindo que os agressores selecionem seus alvos pela disponibilidade de métodos vulneráveis – como softwares desatualizados ou websites corrompidos. Em contraponto, em crimes contra a pessoa, a infração é direcionada a pessoas físicas, sem a alteração de mecanismos para que o ser humano caia em uma "cilada" – dessa maneira, alternativamente, a vitimologia tem ligação maior com o comportamento em rede, fiscalizada pelo algoritmo e orientada para outras pessoas que possam ter interesse nesse tipo de conduta. Desse modo, como observado por Van der Wagen e Pieters (2020), os atos acontecem em uma cadeia, sem uma entidade única e homogênea; a internet conecta milhares de agressores a milhares de possíveis vítimas, com ataques simultâneos ou cronológicos de diferentes pessoas em direção a uma mesma.

Assim, com tantos possíveis alvos e tantas conexões por segundo, também há a influência da velocidade de informações e rapidez dos acontecimentos. O sentimento de adrenalina e entusiasmo gerado pelos crimes cibernéticos é equivalente à exposição de atividades de ritmo acelerado e dopamina rápida[4], que substitui a necessidade de criminosos procurarem por essa sensação em situações físicas – muitas vezes, podendo nem mesmo sair de sua residência. Essa "vertigem" digital (Kurek, 2018) gerada pela ampla exposição de possibilidades contribui para a indiferença (Virilio, 1991), para a desinibição (Suler, 2004), para

[4] Tanto Cooper (2000) quanto Valkenburg e Pietrowski (2017) trazem em seus textos a análise de que a adrenalina sentida pelas pessoas que praticam atividades ilícitas na rede é próxima ao que atletas sentem em esportes radicais.

a tomada de riscos (Goldsmith; Wall, 2019) e para o incentivo da busca de sua própria satisfação (Shay, 2017).

O anonimato aparece de forma abrangente com identidades falsas, fotos *fakes* e nomes fantasia; fingir ser uma pessoa diferente, se esconder através de uma persona criada ou não revelar a sua presença são ações comuns no ambiente virtual. Com a possibilidade de se reinventar e de não expor sua identidade na rede, os indivíduos podem procurar materiais e conversar com pessoas com os mesmos interesses, sem qualquer julgamento ou pressão das pessoas a sua volta (Goldsmith; Wall, 2019). Por outro lado, essa característica também serve para a despersonalização do outro indivíduo, havendo a renúncia à responsabilidade por quem comete as ações, ao acreditar que o outro apenas existe em uma realidade inventada, deixando de existir após término da interação (Suler, 2004).

Longe dos olhares de conhecidos e escondido de seu verdadeiro perfil, é possível agir conforme a sua própria vontade atrás de recompensas emocionais (Shay, 2017), mesmo que isso signifique enganar outros usuários e cometer crimes pensando que o anonimato o impedirá de ser descoberto. Atrás da tela, há a sensação de que as pessoas lesadas na internet não existem de verdade e não passam de conceitos binários gerados pelo sistema eletrônico. Segundo Phillips e Milner (2017), o ambiente virtual embaça a linha entre o que é considerado "normal" e o que é "aberrante", pelas distinções sociais clássicas, e segundo Suler (2004), os processos de cognitividade moral podem ficar temporariamente suspensos da psique online, desassociando suas ações para um segundo "eu".

Katz (1989), por sua vez, considera a ação para cometer o ato criminoso como um "flerte" e Goldsmith e Wall (2019) trazem essa percepção para os crimes virtuais, considerando a internet como a "terra encantada" – local observado por Katz em que o indivíduo pode explorar seu "desejo secreto e interior de ser desviante", com apenas uma pequena margem de possibilidade de ser detectado. O ambiente degrada e diminui a percepção consciente e racional de seus utilizadores, cria a sensação de irrealidade, que atenta contra as vítimas, ao reduzir a sua percepção de danos, e contra os agressores, que ultrapassam limites que talvez não ultrapassariam em ambiente físico – (Rimer, 2017). Desse modo, a sistemática faz com que os indivíduos online nunca estejam plenamente no controle a ponto de "conseguir impedir que as tecnologias operem sobre eles de formas inesperadas ou indesejadas" (Williams, 2018, tradução nossa).

A combinação desses itens está presente no cotidiano de todos os usuários da rede e não torna a internet intrinsecamente perigosa, mas podem combinar-se para aumentar a velocidade do crime e seu volume (Wall, 2005). É importante compreender do que se trata verdadeiramente o cibercrime e de que maneiras ele pode ser encontrado.

2. CIBERCRIMES

No passado, autores se questionaram se crimes cibernéticos existiam (Brenner, 2001 *apud* Wall; Goldsmith, 2019) ou se essa forma de delito deveria ser tratada por teorias já existentes (Jones, 2003), sem pensar nas lacunas do comportamento e as adversidades de oportunidades, com domínios inteiramente novos de criminalidade, como descrito por Wall (2005). Com o tempo, casos concebidos de maneira "tradicional"[5] passaram a ser reconhecidos como parte do cibercrime – fraude, pornografia e pedofilia, por exemplo, deixam de ter um conceito puramente físico e passam a necessitar de uma compreensão dentro do sistema informático. Segundo Wall (2005), a mudança na convergência de propriedade e controle, civil e criminal, direito público e privado, mostra a diferente dinâmica desses assuntos na era digital e carece de estudo específico em seus tópicos de um fenômeno que deve ultrapassar as barreiras de legalidade a cada nova atualização.

Desse modo, desde 2013, no site oficial do Escritório das Nações Unidas sobre Drogas e Crimes, há a publicação do estudo abrangente de cibercrimes pelo mundo; após a resolução 65/230, a Assembleia Geral solicitou à Comissão para a Prevenção do Crime e à Justiça Penal a criação de um grupo de peritos intergovernamental para realizar um estudo sobre a cibercriminalidade sob diferentes perspectivas – setor privado, internacional, intercâmbio de informações, práticas, assistência técnica e legislações. Esse estudo possibilitou o entendimento geral-governamental de como a sociedade hiperconectada desenvolveu um sistema em que todos os crimes têm provas eletrônicas e, ao mesmo tempo, nenhum deles é puramente informativo; da mesma forma que estabeleceu preceitos estudados por acadêmicos e delimitou definições específicas de diferentes crimes, como "ciberdependentes" e "cibercapacitados"[6].

[5] Crimes "tradicionais" são considerados como os tipicamente registrados nas ocorrências policiais e geralmente cometidos de forma física e *offline* (McGuire; Dowling, 2013).
[6] Os termos "cyber-dependent" e "cyber-enabled" foram traduzidos de maneira interpretativa mas imediatamente similar à original, para melhor entendimento dos tópicos aqui tratados.

2.1 Ciberdependentes

Os crimes ciberdependentes, anteriormente chamados de "vandalismo virtual" (Williams, 2006) ou "crimes de computador" (Douglas *et al*, 2006), são delitos cometidos através de computadores, redes informáticas ou tecnologias de informação e comunicação, com o intuito de atacar o software[7] de outros computadores, podendo corromper seus dados, afetar seu funcionamento e até sequestrar as informações. Desse modo, eles se tornam "simultaneamente alvo e meio do crime" (Van der Wagen; Oerlemans, 2023), considerando apenas os crimes primários – infrações "contra" computadores, como explicado por McGuire e Dowling (2013), e não seus resultados secundários, que podem se encaixar mais adequadamente no tópico sobre "cibercapacitados".

As motivações para esses crimes centram-se no ganho financeiro, protesto ou dano criminal, com ramificações emocionais para a satisfação pessoal do indivíduo – considerando a curiosidade, o desafio intelectual, a vingança, a malícia geral ou o simples tédio, como observado por Kirwan e Power (2012). A vitimologia do crime é mista, podendo haver vítimas específicas ou de natureza aleatória; por exemplo, um vírus pode ser amplamente disseminado pela rede e infectar rapidamente um grande número de usuários, enquanto as ameaças persistentes avançadas (APT) se pautam em ataques com um objetivo específico, geralmente voltadas a uma pessoa, empresa ou organização (Symantec, 2012).

2.2 Cibercapacitados

Inicialmente considerados como crimes tradicionais de amplo alcance pelo seu uso de redes informáticas ou crimes virtuais impróprios[8] (Jesus, 2016), os crimes cibercapacitados apresentam uma mescla do que já era conhecido como "ciber", trazendo a discussão de qual deveria ser o novo entendimento conforme o termo e o tipo criminal – e se deveria haver realmente essa distinção. Wall (2005), um dos pioneiros na pesquisa de cibercrimes, por outro

[7] Segundo o Dicionário de Oxford, "software" se refere ao conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador. O "hardware", por sua vez, se refere ao conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um computador. Assim, é possível atacar o computador físico, corrompendo suas peças (por exemplo, HD) e estragando seu sistema operacional, porém os crimes ciberdependentes consideram esse ato por meio do software não como destruição de um objeto qualquer, mas de seus dados e meio tecnológico.

[8] Considera-se um crime virtual próprio aquele que depende do computador como vítima e meio, o que foi citado aqui como ciberdependentes.

lado, discorreu sobre seu entendimento de crimes cibercapacitados enquadrando-os como delitos possibilitados por computadores – o que poderia coincidir com o questionamento anterior de que seriam "evoluções' de crimes tradicionais, se não fosse pelo ângulo de estudo: os crimes sempre exibem qualidades específicas da Internet.

Esse ambiente transnacional oferece oportunidade interativa com atividades nocivas – por exemplo, fraude (como *phishing* e golpes de namoro) e crimes sexualmente relacionados (como pornografia infantil e pornografia de vingança) (Oelermans; Van der Wagen, 2022) – que seriam encontradas de maneira diferente em sua natureza tradicional. Dessa maneira, assim como visto nos preceitos básicos de motivação, a vitimologia e o modus operandi[9] estão intrinsecamente ligados com o conhecimento e meio tecnológico de operação; a infração tem novidade material e psicológica, mas se desenvolve paralelamente aos crimes tradicionais, ao invés de ser uma continuação deles (Oelermans; Van der Wagen, 2022). Crimes assistidos[10] também são considerados uma criminalidade informática (Wall, 2005).

3. NO BRASIL

Desde o fim do século XX, a emergência das mídias digitais desencadeou uma reconfiguração no modo em que pessoas buscam informação, entretenimento e sociabilidade (Kubota, 2016). Entretanto mais recentemente, outro acontecimento deu valor ampliado aos meios de comunicação e as redes tecnológicas: a pandemia de COVID-19. O isolamento social, sendo uma das medidas principais adotadas para o controle da doença, forçou a interrupção de trabalhos presenciais e a adesão ao trabalho remoto (Alves Tomaz Silva; Arruda Marinho, 2022), impulsionando a adesão de milhares de pessoas ao uso de novas tecnologias – e, aos que já se utilizavam dessas, mais horas de conectividade.

Segundo o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (2019 e 2020), em suas pesquisas anuais sobre usuários de internet, houve um crescimento de 19 milhões de usuários entre 2019 (133,8 milhões) e 2020 (152 milhões), como

[9] *Modus Operandi* (conhecido popularmente como MO) é um conjunto de comportamentos aprendidos pelo infrator a fim de perpetuar seu crime, costuma ser dinâmico e maleável até se manter estável a medida que funciona e atua conforme seu desejo (Douglas; Douglas, 2006).

[10] Crimes assistidos são auxílios de infrações realizadas por computador, como fóruns em que se discutem formas de cometer crimes. Essa divisão ocorre apenas no estudo de David S. Wall (2005), sendo considerada por outros autores como parte dos crimes cibercapacitados.

modo de se adaptarem ao isolamento. A inclusão foi dinâmica, com o crescimento de 20 pontos em atividades escolares, 9 em cursos a distância e 5 em atividades de trabalho (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, 2019, 2020). Entretanto, mesmo em um período sensível de crise econômica, emocional e política, os usuários também tiveram que se atentar aos cibercrimes; a instabilidade foi uma oportunidade para os criminosos que tiveram acesso a mais alvos (Alves Tomaz Silva; Arruda Marinho, 2022), tanto para a formação de novos infratores – como será observado no caso.

O crescimento expressivo de ciberataques mostra-se notável no relatório do FortiGuard Labs (2021), que examinou 8,5 bilhões de ataques no Brasil durante o ano de 2020 (sendo 5 bilhões apenas no quarto trimestre), influenciando diretamente os 88,5 bilhões de ciberataques em 2021. Esse crescimento abrupto deu-se a partir da ampliação de habilidades criminais online, aumento de possíveis vítimas e de novos infratores (que podem ou não já ter carreira criminal anterior), ao terem de se adaptar ao novo sistema de crimes. Ademais, jovens também demonstraram interesse em performar cibercrimes ao utilizarem das características da internet citadas anteriormente para explorar sua satisfação interna com *hacking* e a adrenalina gerada por esse (Goldsmith; Wall, 2019).

Todavia, cabe aqui citar que, mesmo com o aumento contínuo, o combate a esses crimes não é recente e vem sendo dominado por diferentes entidades (como a Delegacia Especializada em Investigação de Crimes Cibernéticos) durante muitos anos. Um dos crimes do gênero de maior notoriedade, por exemplo, foi a abertura para a criação da lei 12.737/2012, responsável por inserir o crime de invasão de dispositivo eletrônico no código penal e tipificar crimes informáticos. O dispositivo ficou conhecido como Lei Carolina Dieckmann, propriamente pelo fato de a atriz não ter recebido amparo de legislação específica quando teve seu computador pessoal invadido, suas fotos íntimas roubadas e diversas ameaças com extorsão (DPE-CE, 2022).

A seguir, faz-se a análise da Operação Dark Room, sob o ponto de vista da psicologia criminosa e computacional, junto à perspectiva de desinibição de personalidade. O estudo também utiliza de objeto outros crimes cometidos no Brasil.

3.1 Operação Dark Room

O processo teve seu início no aplicativo X – chamado de Twitter na época dos acontecimentos (Investigação Criminal, 2024). Por mais que houvesse tentativas de denúncias

anteriores, o caso apenas ganhou notoriedade quando a conta intitulada "Discord Fora de Contexto" publicou uma captura de tela do aplicativo Discord, a qual mostrava uma jovem (menor de idade) sendo obrigada a engolir borrifadas de SBP (um inseticida em aerossol). Nos comentários da publicação, um dos usuários se identificou como participante do grupo e descreveu a situação com tonalidade de zombaria; afirmou que eles estavam com os dados e os "nudes" (imagens de nudez) da garota, ameaçando enviar o conteúdo para seus familiares, então mandaram ela fazer várias "coisinhas"[11] (X, 2023).

O usuário "MerDarte" recolheu capturas de tela desta publicação e conseguiu vídeos de abusos a outras garotas, fotos de bandeiras e conversas sobre o nazismo, depoimentos de outras fontes, todas reunidas num post com mais de 67 mil curtidas. Contas oficiais da polícia, jornalistas e famosos foram marcados para divulgar de maneira extensa a informação de que haviam grupos no aplicativo Discord cometendo crimes (X, 2023). Depois dessa publicação, em março, não houve mais atualizações sobre o caso fora da força policial, mas a primeira fase da Operação Dark Room já estava em andamento (Fantástico, 2023).

No dia 26 de junho de 2023, o Fantástico[12] estreou uma reportagem acerca dos acontecimentos descritos, entrevistando vítimas e seus familiares, agentes da lei e psicólogos, assim como um representante do aplicativo. A reportagem também anuncia a prisão de 5 agressores identificados e a apreensão de 2 menores de idade, durante a primeira fase da Operação Dark Room. Já na segunda fase, mais dois indivíduos foram presos, entre os dias 4 e 12 de julho.

De acordo com o MPRJ (2023), os participantes da associação criminosa, em primeiro momento, vasculharam as redes sociais, sites de bancos e consulta de crédito para obter informações pessoais da vítima, também usuárias do aplicativo Discord. Em seguida, podiam estabelecer uma amizade com a vítima para obter mais informações, fotos íntimas ou instantaneamente ameaçá-las com chantagens afirmando possuírem fotos comprometedoras que seriam enviadas para os pais e colegas de turma, caso não praticassem as ordens dadas pelo grupo. Gorissen *et al.*, (2020) descreve esse tipo de comunicação de relação de confiança ao

[11] O termo "coisinhas" foi utilizado pelo usuário e, posteriormente, os atos seriam identificados como "Lulz".
[12] Programa de televisão brasileiro transmitido aos domingos pela TV Globo.

fornecer ao agressor o material com que pode chantagear um menor de idade como "*grooming*" – ou, em tradução livre, "aliciamento"[13].

Prontamente, eram criados grupos (ou utilizados grupos já existentes para esse fim) para publicar vídeos e expor as vítimas, numa prática conhecida como "*exposed*", caso não cumprisse as ordens (MPRJ, 2023; O Dia, 2023). Os desafios eram chamados de "Lulz"[14] (Metrópoles, 2023) e podiam ser cometidos por outros membros – além das vítimas aliciadas – para ganho de cargo dentro do servidor (Agência Brasil, 2023). As adolescentes eram chantageadas e coagidas a se tornarem escravas sexuais dos líderes, que as submetiam a estupros virtuais transmitidos dentro dos servidores, inclusive sendo obrigadas a se automutilarem (Agência Brasil, 2023). Segundo a denúncia do Ministério Público do Rio de Janeiro no julgamento de Pedro Ricardo Conceição da Rocha, preso na segunda fase da Operação Darkroom:

> Os integrantes da associação criminosa, dentre eles o denunciado, atuavam não só através da contemplação virtual, mas também pela determinação ao vivo e online de ações proativas de vítimas, crianças e adolescentes, constrangidas sob ameaças de causar mal às vítimas e seus familiares e de divulgação de fotos e vídeos íntimos anteriormente hackeados, a praticarem atos de automutilação, degradação física, exposição íntima, zoofilia e atos libidinosos, colocando em risco a saúde, integridade física e psicológica das vítimas (MPRJ, 2023).

Segundo investigação da Polícia Civil do Rio de Janeiro, a decisão judicial ainda aponta que o integrante da associação criminosa vendia ingressos para as chamadas de vídeos ao vivo em que os crimes eram cometidos (G1, 2024). Piadas racistas também eram permitidas e incentivadas (G1, 2024).

3.2 Reflexões

Segundo os acontecimentos descritos e conforme a deliberação do julgamento do réu supracitado:

> [...] como 'dono' da plataforma 'SYSTEM X', no Discord, o réu replicava e amplificava o que de pior existe na sociedade, acreditando que ao se esconder atrás

[13] A definição do termo "grooming"/"aliciamento" aparece como "a comunicação online com um menor na intenção de cometer abuso sexual ou produzir imagens de pornografia infantil (Lindenberg; Van Dijk, 2016)" segundo o capítulo "Tipos de cibercrimes e sua criminalização" de Oerlemans e Van der Wagen (2022).
[14] Phillips (2016) reconhece a expressão como uma derivação da sigla "LOL" ("laughing out loud") e associa o rótulo a um grupo de indivíduos que extrai divertimento relacionado ao sofrimento alheio.

> de máscaras, bandanas e outros subterfúgios, poderia ficar impune indefinidamente, como se alguém pudesse ficar fora do alcance das autoridades ou acima da lei (TJRJ, 2024).

A plataforma Discord, nesse contexto, é utilizada como a "terra encantada" de Katz (1989), sendo primeiramente concebido como uma rede social para jogos, mas popularizada entre os jovens com interesses comuns para outros fins – um deles sendo o criminal, como a própria Delegacia da Criança e Adolescente afirmou (DCAV, 2023). Assim, ao manipular o servidor a sua vontade, às vezes fazendo com que as conversas com conteúdo ilegal ficassem de três a quatro horas no ar (G1, 2024), pensando que estão fora do alcance das autoridades e que podem usar o anonimato ao seu favor (TJRJ, 2024), o efeito de desinibição de Suler (2004) se mostra visível e a agressão às vítimas começa diante da presença da tríade de Cooper (1998) intitulada "Triple A" (ou, em tradução livre, "A Triplo"), a qual converge as experiencias de sexualidade na internet em 3 pilares: *acessibility* (acessibilidade técnica), *affordability* (acessibilidade econômica) e *anonymity* (anonimato) que podem ser encontradas durante todo o caso, em um modo fácil de conseguir pornografia online. De maneira análoga, os servidores amplificavam a possibilidade de se conseguir presenciar abuso de mulheres e animais.

Rimer (2017), em sua pesquisa sobre a antropologia do abuso sexual online, contempla que os agressores não compreendem a internet como um lugar "real", o qual requer adesão a normas sociais, mas apenas um lugar rápido no qual a oportunidade é criada (Wortley, 2012 apud Rimer, 2017). Kurek (2018) acrescenta que alguns jovens cujas necessidades de gratificação se baseiam em "motivos obscuros", quando expostos a um ambiente amplamente descontrolado e não monitorado, podem tender a desenvolvimentos pouco saudáveis. Kurek (2018) também cita que alguns adolescentes optam por procurarem redes sociais específicas para estabelecerem um sentido de comunidade fora de seu ambiente imediato e que jovens com traços de personalidade antissocial também podem o fazer, porém seguindo suas próprias motivações – o que deve ser estudado de maneira aprofundada em momentos futuros, avaliando se os agressores lidam com personalidade antissocial, sádica ou se foram comportamentos aprendidos durante o uso da internet.

As máscaras citadas na decisão judicial se referem tanto à questão de anonimidade da internet quanto às máscaras físicas que os integrantes do grupo utilizavam. Conhecidas como "máscaras siege", o pano que esconde metade do rosto e tem desenho de caveira humana em sua parte inferior tem relação com movimentos fascistas e de extrema direita, como observado

por Fürstenberg (2022), em que seguidores a utilizam em atentados, invasões políticas e em vídeos de propaganda, ostentando-as como brasões e identificadores. Olshaker e Douglas (2021) apontam como os grupos de ódio racistas podem ser atrativos, ao ponto de se tornarem alvos não apenas pessoas negras ou judias, mas qualquer minoria que lhes agradem ferir, inclusive as mulheres, como explícito no trecho:

> Eles proporcionam um senso de propósito e missão - embora errôneos - para uma vida sem grandes objetivos. [...] Talvez o mais importante, vinculado a todo o resto, seja a mensagem de que existem pessoas hereditariamente inferiores. Negros, judeus, imigrantes, muçulmanos e, para alguns, as mulheres são os alvos favoritos, mas pode ser simplesmente qualquer 'outro' (Olshaker; Douglas, 2021).

A máscara identificadora também foi utilizada por um dos assassinos do massacre de Suzano em 2019 e por outro no massacre de Aracruz em 2022. O interesse dos usuários em tiroteios escolares vai além de apenas o uso de máscaras, tendo havido mentoria em um dos servidores para que um dos integrantes realizasse o ataque armado à Escola Estadual de Sapopemba em 23 de outubro de 2023. O autor do ataque compartilhou fotos da escola em que realizaria o atentado e outros usuários mandaram dicas sobre como executar o crime; os integrantes do servidor pediram, inclusive, para que o garoto transmitisse os assassinatos em uma chamada de vídeo, que aconteceu durante poucos minutos, no banheiro da escola, antes do atentado. Após o ocorrido, usuários queixaram-se pela morte de uma pessoa, chamando o garoto de "merda" por não ter assassinado pelo menos cinco (Investigação Criminal, 2024; Metrópoles, 2023).

Segundo a jornalista Carla Albuquerque, até maio de 2024 haviam sido feitas 80 detenções de diversos grupos criminosos da plataforma Discord. Entre eles, até mesmo um garoto português foi preso por diversos crimes, entre eles o de terrorismo internacional por mentoria intelectual[15] ao ataque armado à Escola Estadual de Sapopemba (Investigação Criminal, 2024). Na mesma ocasião, o psicólogo criminal Dr. Christian Costa atesta que os acontecimentos não são eventuais desafios entre jovens e sim uma rede e associação criminosa que precisa ser controlada (Investigação Criminal, 2024), acrescentando a declaração da promotora de justiça de São Paulo, Maria Fernanda Balsalobre, que afirmou na reportagem do

[15]A mentoria intelectual é vista por Wall (2005) como um cibercrime assistido.

Fantástico (2023) serem criminosos que utilizam a insegurança da plataforma quanto a crianças e adolescentes para praticar os crimes.

CONCLUSÃO

O caso trata de um exemplo de crimes cibercapacitados, em que os agressores utilizam as redes informáticas tanto para se unirem em organização criminosa dentro da plataforma quanto para o amplo alcance de vítimas.

A Operação Darkroom, realizada entre março e julho de 2023, trata de acontecimentos relativamente recentes, com alguns arquivos em segredo de justiça para sigilo da identidade de menores e de processos que ainda estão em julgamento. O julgamento da associação de criminosos gera precedentes jurídicos em torno da área de direito cibercriminal e auxilia os policiais em suas próximas investigações, compreendendo o M.O. entre os criminosos junto às características psicológicas atreladas ao uso dos computadores na comunicação entre pares, sendo possível até adaptar o modo de precaução de aplicativos e desmantelar outras associações criminosas que utilizam esse meio antes, durante ou após os crimes.

Assim, pode-se perceber claramente como os estudos relacionados tanto ao comportamento de jovens na rede de internet quanto o comportamento influenciado por essas próprias redes se mostram incipientes e demonstram potencial para outros estudos. Em um futuro próximo, a descrição dos psicólogos jurídicos atrelados ao caso e pesquisadores da área poderão contribuir nas buscas assertivas para demonstrar se o caso se trata de um sadismo aprendido, compensatório ou inato.

REFERÊNCIAS

AGÊNCIA BRASIL. **Polícia apreende jovens que praticavam violência sexual pela internet.** Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2023-06/policia-apreende-jovens-que-praticavam-violencia-sexual-pela-internet. Acesso em: 22 jul. 2024.

ALVES TOMAZ SILVA, J. P.; ARRUDA MARINHO, L. E. **O aumento dos crimes virtuais na pandemia e os limites da liberdade de expressão.** Trabalho de Conclusão de Curso (Bacharelado em direito) - Universidade de Potiguar, Natal, 2022.

BRENNER, S. Is there such a thing as "virtual crime"? **California Criminal Law Review**, v.4, n. 1, p. 69, 2001.

CGI.br. (2021). **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros** – TIC Domicílios 2020.

CGI.br. (2023). **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**: TIC Domicílios 2023.

COHEN, L. E.; FELSON, M. Social change and crime rate trends: A routine activity approach**. American sociological review**, v. 44, n. 4, p. 588, 1979.

COOPER, A. **Cybersex and sexual compulsivity:** The dark side of the force. Sexual addiction & compulsivity, v. 7, n. 1–2, p. 1–3, 2000.

COOPER, A. **Sexuality and the internet:** Surfing into the new millennium. Cyberpsychology & behavior: the impact of the Internet, multimedia and virtual reality on behavior and society, v. 1, n. 2, p. 187–193, 1998.

DATA REPORTER. **Digital around the world.** Disponível em: https://datareportal.com/global-digital-overview. Acesso em: 16 abr. 2024.

DOUGLAS, J. E., & DOUGLAS, L. K. **Modus operandi and the signature aspects of violent crime**. Em: DOUGLAS J. E. *et al*, Crime classification manual: A standard system of investigating and classifying violent crimes. 2006.

FANTÁSTICO. **Rede sem lei:** no Discord, criminosos violentam e humilham meninas menores de idade**.** Globoplay, 2023. Disponível em: https://globoplay.globo.com/v/11729798/. Acesso em: 18 abr. 2024.

FINN, E. **What algorithms want:** Imagination in the age of computing**.** Londres, England: MIT Press, 2018.

FortiGuard Labs apresenta relatório sobre ciberataques no Brasil. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acessado em: 11/04/2024.

FÜRSTENBERG, M. **Communities of hateful practice: the collective learning of accelerationist right-wing extremists, with a case study of the Halle synagogue attack**. Max Planck Institute for Social Anthropology Working Papers, n. 210, 2022.

G1. **Condenado por criar grupo no Discord para cometer crimes monetizava conteúdo e instigou adolescente a se cortar, diz investigação**. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/07/05/condenado-por-criar-grupo-no-discord-para-cometer-crimes-monetizava-conteudo.ghtml. Acesso em: 28 jul. 2024.

GOLDSMITH, A.; WALL, D. S. The seductions of cybercrime: Adolescence and the thrills of digital transgression. **European journal of criminology**, v. 19, n. 1, p. 98–117, 2022.

HINDELAND, M. J., GOTTFREDSON, M. R., e GAROFALO, J. **Victims of Personal Crime:** an Empirical Foundation for a Theory of Personal Victimization**.** Cambridge, Mass.: Ballinger. 1978.

INVESTIGAÇÃO CRIMINAL. **MAIS UM CRIMINOSO DO DISCORD PRESO! - INVESTIGAÇÃO CRIMINAL.** Disponível em: https://www.youtube.com/watch?v=aOnKwWWyTD4. Acesso em: 26 jul. 2024.

JESUS, D. E. **Manual de Crimes Informáticos**. São Paulo: Saraiva, p. 48, 2016.

JONES, R. **Review of Crime in the Digital Age by P. Grabosky and R. Smith**. International Journal of Law and Information Technology, n. 11, p. 98. 2003.

KATZ, J. Seductions of crime: Moral and sensual attractions in doing evil**. The journal of criminal law & criminology**, v. 80, n. 1, p. 352, 1989.

KIRWAN, G.; POWER, A. **Cybercrime:** The psychology of online offenders**.** Cambridge University Press, 2013.

KUBOTA, L. C. **Uso de tecnologias da informação e comunicação pelos jovens brasileiros.** In: SILVA, E. (org.). Dimensões da experiência juvenil brasileira e novos desafios às políticas públicas. Brasília: IPEA, p. 199–220, 2016.

KUREK, A. **Understanding online disinhibition:** An investigation of the relationship between information and communication technology and adolescent personality, identity and behai-ior. Tese (Doutorado em Filosofia) - Victoria University of Wellington, New Zealand, 2018.

DPE-CE - Defensoria Pública do Estado do Ceará**. Lei Carolina Dieckmann:** 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual. Disponível em: https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/. Acessado em: 11 abr. 2024.

LEINER, B. M. et al. **A brief history of the internet**. Computer communication review, v. 39, n. 5, p. 22–31, 2009.

LLOYD, B. **How Has the Internet Affected the Way We Communicate Within This New Era? Can We Use This to Our Advantage?** New Zealand Association for Cooperative Education Annual Conference. 2005.

MCDOWELL, S. D. **Telecommunications, cities, and geographic and social space**. The Journal of communication, v. 47, n. 1, p. 136–143, 1997.

MCGUIRE, M; DOWLING, S. **Cyber crime:** A review of the evidence. Chapter 4: Improving the cyber crime evidence base. Home Office Research Report 75, 2013.

METRÓPOLES. **Exclusivo: mensagens mostram que aluno foi instruído a atacar escola.** Disponível em: https://www.metropoles.com/sao-paulo/exclusivo-mensagens-mostram-que-aluno-foi-instruido-a-atacar-escola. Acesso em: 29 jul. 2024.

MPRJ - Ministério Público do Estado do Rio de Janeiro. **MPRJ denuncia homem por utilizar plataforma online para cometer crimes sexuais**. Disponível em: https://www.mprj.mp.br/visualizar?noticiaId=128001. Acesso em: 26 jul. 2024.

O DIA. **Operação mira adolescentes que praticavam estupro e estimulavam suicídio através do Discord.** Disponível em: https://odia.ig.com.br/rio-de-janeiro/2023/06/6660138-operacao-mira-adolescentes-que-praticavam-estupro-e-estimulavam-suicidio-atraves-do-discord.html?. Acesso em: 26 jul. 2024.

OELERMANS, J.J., & VAN DER WAGEN, W. **Types of cybercrime and their criminalisation.** In *Essentials in cybercrime: A criminological overview for education and practice*. Eleven International Publishing, p. 53-98. 2022.

OLSHAKER, M.; DOUGLAS, J. E. **The killer's shadow:** The FBI's hunt for A white supremacist serial killer. Nova Iorque, NY, USA: HarperCollins, 2021.

PHILLIPS, W. **This is why we can't have nice things:** Mapping the relationship between online trolling and mainstream culture. Londres, England: MIT Press, 2016.

PHILLIPS, W.; MILNER, R. M. **The ambivalent internet:** Mischief, oddity, and antagonism online. Oxford, England: Polity Press, 2018.

RIMER, J. R. Internet sexual offending from an anthropological perspective: analysing offender perceptions of online spaces. **The journal of sexual aggression**, v. 23, n. 1, p. 33–45, 2017.

SHAY, H. Virtual edgework: Negotiating risk in role-playing gaming. **Journal of contemporary ethnography**, v. 46, n. 2, p. 203–229, 2017.

STEINMETZ, K. F. Hacked: **A radical approach to hacker culture and crime.** Nova Iorque, NY, USA: New York University Press, 2016.

SULER, J. **The online disinhibition effect.** Cyberpsychology & behavior: the impact of the Internet, multimedia and virtual reality on behavior and society, v. 7, n. 3, p. 321–326, 2004.

TJRJ - TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. **Jovem que promovia estupros ao vivo pelo aplicativo Discord é condenado a 24 anos de prisão**. Disponível em: https://www.tjrj.jus.br/noticias/noticia/-/visualizar-conteudo/5111210/402515326. Acesso em: 29 jul. 2024.

TJRJ - TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. **Processo Nº 0000634-52.2023.8.19.0012**

UNODC - United Nations Office on Drugs and Crime. **Comprehensive Study on Cybercrime 2013.** Disponível em: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf Acessado em: 15 nov. 2023.

VALKENBURG, P. M.; PIOTROWSKI, J. T. **Plugged in:** How media attract and affect youth. New Haven, CT, USA: Yale University Press, 2017.

VIRILIO, P. **The Aesthetics of Disappearance**. Cambridge, MA: MIT Press. 1991.

VAN DER WAGEN, W.; PIETERS, W. The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory**. European journal of criminolog***y*, v. 17, n. 4, p. 480–497, 2020.

WALL, D. S. **The internet as a conduit for criminal activity**. Em: Information Technology and the Criminal Justice System. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2005. p. 77–98. (revised 2010, 2015)

WILLIAMS, J. **Stand Out of the Light:** Freedom and Resistance in the Attention Economy. Cambridge University Press. 2018.

WILLIAMS, M. **Virtually criminal:** Crime, deviance and regulation online. Londres, England: Routledge, 2006.

YEPES, R. **The Art of Profiling in a Digital World. The Police Chief 83**. Disponível em: https://www.policechiefmagazine.org/the-art-of-profiling-in-a-digital-world/. Acesso em: 23 out. 2023.

X.COM. Disponível em: https://x.com/MerDarte/status/1635663238166728704. Acesso em: 14 mar. 2024.