ISSN - 2175-6058
DOI: https://doi.org/10.18759/rdgf.v24i3.2304

REALIDADE VIRTUAL E CRIMINALIDADE: TENSÕES E DESAFIOS

VIRTUAL REALITY AND CRIME: TENSIONS AND CHALLENGES

Rogerio Gesta Leal

RESUMO

O objeto deste trabalho é avaliar que desafios a realidade virtual está impondo ao enfrentamento da criminalidade contemporânea, razão pela qual o problema que buscamos aclarar diz em saber em que medida o Estado hodiernamente é capaz de dar conta de tais demandas, sugerindo, como hipóteses exemplificativas de respostas, algumas medidas preventivas e curativas para tanto. Para cumprir tal objeto vamos: (i)demarcar algumas dimensões simbólicas, físicas e virtuais da criminalidade atual; (ii) identificar alguns pontos de confluência entre o ciberespaço e comportamentos criminosos; (iii) avaliar e propor meios de enfrentamento da cibercriminalidade em especial para o Brasil.

Palavras-chaves: Inteligência Artificial. Criminalidade Virtual. Responsabilidade Penal.

ABSTRACT

The object of this work is to evaluate what challenges the virtual reality is imposing on the confrontation of contemporary criminality, and the problem that we seek to clarify concerns knowing to what extent the State today is capable of dealing with such demands, suggesting, as illustrative hypotheses of responses, some preventive and curative measures for this purpose. To fulfill this objective, we will: (i) demarcate some symbolic, physical and virtual dimensions of current

criminality; (ii) identify some points of confluence between cyberspace and criminal behavior; (iii) evaluate and propose means of combating cybercrime, especially in Brazil.

Keywords: Artificial Intelligence. Virtual Crime. Criminal Responsibility.

NOTAS INTRODUTÓRIAS

Historicamente o mundo todo tem experimentado períodos de grande progresso e ilustração. Desde a Revolução Industrial a ciência e o conhecimento contam com evolução surpreendente, amplificando novos sistemas de informação e dados, automatizando atividades comuns e complexas, radicalizando a velocidade das relações profissionais, familiares e institucionais, pela via de tecnologias ainda não experimentadas, bem como das comunicações, o que impacta inúmeras atividades essenciais no quotidiano de pessoas físicas e jurídicas, do setor público (serviços públicos de saúde, segurança, transportes, educacionais, dentre outros) e privado (comércio, indústria, políticas de relacionamentos entre fornecedores e consumidores).

Paralelo a isto – e de forma paradoxal - igualmente aumentaram os níveis de letargia psíquica, obesidade, complacência, banalização de comportamentos de baixa empatia com interesses e temas difusos e coletivos, fomentando em maior escala projetos individuais e setoriais da Comunidade.[1] E por que paradoxal? Pelo fato destas transformações terem potencial amplíssimo de servir ao desenvolvimento do bem estar das pessoas, aumentando suas qualidades de vida digna em Sociedade (mais do que individualmente).

O surgimento da realidade virtual por meio da internet e das redes sociais – por conta das revoluções tecnológicas que temos assistido -, objetificam muito bem os cenários referidos, criando oportunidades sem paralelo na história, seja para comércio, pesquisas, educação, entretenimento, emergindo dai espaços públicos e mercados globais nos quais ideais inovadoras a todo tempo florescem, tanto para o bem como para o mal.

Em face disto, o objeto deste trabalho é avaliar que desafios a realidade virtual está impondo ao enfrentamento da criminalidade contemporânea, razão pela qual o problema que buscamos aclarar diz em saber em que medida o Estado hodiernamente é capaz de dar conta de

tais demandas, sugerindo, como hipóteses exemplificativas de respostas, algumas medidas preventivas e curativas para tanto.

Elegemos desenvolver este texto a partir dos seguintes objetivos específicos: (i) demarcar algumas dimensões simbólicas, físicas e virtuais da criminalidade atual; (ii) verificar, de modo mais tópico, pontos de confluência entra o ciberespaço e comportamentos criminosos; (iii) propor algumas definições do que entendemos por crimes cibernéticos; (iv) avaliar e propor meios de enfrentamento da cibercriminalidade, em especial para o Brasil.

Utilizamos na pesquisa o método dedutivo, testando nossas hipóteses com os fundamentos gerais a serem declinados, bem como a técnica de pesquisa com documentação indireta, nomeadamente bibliográfica.

DIMENSÕES SIMBÓLICAS, FÍSICAS E VIRTUAIS DA CRIMINALIDADE

As possibilidades mutacionais da criminalidade tem crescido progressivamente em termos de história da civilização, sendo que o século XX foi marcado pela maior organização de pessoas e instituições voltadas para estes intentos, a começar pela experiência das chamadas máfias à moda *La Cosa Nostra* italiana, espalhadas por todo o globo com o passar do tempo.[2] E sobre isto Catania (2016, p. 21) nos refere:

> *Duas espadas cruzadas sob uma mão negra eram o emblema da organização criminosa chamada "Mão Negra", que em Nova York, a partir da década de 1880, passou a cometer crimes e extorsões, assustando até o tenor Enrico Caruso. Foi um tipo de crime tão sutil e ambíguo quanto covarde e sanguinário para com aqueles que não aceitavam a "proteção" de qualquer atividade comercial. O costume de impor o medo, como já era então definido o suborno, imposto pela Mão Negra em formas cada vez mais modernas e organizadas, tornou-se caractere primordial e traço distintivo não só da Cosa Nostra, a muito poderosa máfia siciliano-americana, mas de todas as máfias, que replicou seus mecanismos criminosos.*[3]

Susan Brener (2002, p. 12) registra que imigrantes italianos, que começaram a chegar nos Estados Unidos na década de 1860, trouxeram a *Mão Negra*, ou a Máfia, com eles, sendo que em 1890 a polícia de Nova Orleans estimou que a máfia siciliana havia cometido mais de cem as-

sassinatos na cidade entre 1870 e 1890.[4] Já na década de 1930, a autora refere o surgimento de gangs lideradas por personagens carismáticos como Dillinger, Bonnie e Clyde, e outros, alterando-se o cenário a partir da década de 1960, quando as percepções sociais e das instituições públicas se modificaram, dando-se conta dos riscos e perigos que as máfias representavam à toda a sociedade:

> *Embora estas gangues representassem um tipo de atividade criminosa organizada, eram operações de pequena escala envolvidas numa atividade com a qual muitos americanos simpatizavam numa era de execuções hipotecárias bancárias. Na década de 1960, entretanto, os esforços combinados do Senador Kefauver, do Comitê McClellan, e do Procurador-Geral Robert Kennedy, aumentaram a conscientização americana sobre o crime organizado do tipo da Máfia e geraram a percepção de que era um fenômeno que ameaçava o modo de vida americano.*[5]

A partir da segunda metade do século XX é possível identificar a formatação de certo senso comum internacional no sentido de que as máfias representavam grandes ameaças à ordem e paz social – e aos negócios formais do mercado -, pois grupos organizados de bandidos atacavam *pessoas de bem* por razões puramente comerciais. Ao contrário da percepção das gangues das décadas de 1920 e 1930, os grupos daquele período provocavam danos e vitimização com o objetivo de ganhar dinheiro. Por isto as décadas de 1970 e 1980 serão momentos de proliferação de leis e medidas de enfrentamento do crime organizado a partir das experiências com as máfias (não somente de origem italiana, mas da Yakuza japonesa, da China, da Jamaica, Rússia).[6]

Mas todos estes movimentos de criminalidade ainda eram predominantemente físicos, e por isto inculcavam tantos receios na população em geral e nas autoridades públicas de segurança, pois as consequências de seus atos se faziam sentir imediatamente e a olhos nus, provocando comoções tremendas em todos. Mas o surgimento das tecnologias virtuais de relações públicas e privadas vai alterar drasticamente estes cenários, nomeadamente os de delinquência e criminalidade.

Os avanços das redes conectadas de computadores, com bilhões de dados e informações virtuais em bancos e repositórios, gerando consórcios internacionais de cooperação industrial, comercial, de pesquisa e ensino, têm trazido aprimoramentos imensos às pessoas (físicas e jurídicas), a despeito de que isto não tenha se dado de forma equilibrada em

termos sociais, haja vista o número de excluídos destes processos. Ou seja, a realidade virtual e a internet vem sendo utilizadas como janelas para o mundo, permitindo que pessoas saciem suas curiosidades, demandas, problemas, desejos, enquanto ferramenta de alta eficácia, mas, ao mesmo tempo, também ensejam seu uso para a prática de ilícitos os mais diversos, de múltiplas espécies (administrativos, cíveis, criminais, tributários, fiscais, etc), agora com impactos imensos, justamente porque potencializados por ambientes virtuais.

Também os sistemas jurídicos neste aspecto vem tendo benefícios, pois é possível acessar junto a realidade virtual plataformas com informações sobre direitos e deveres a serem observados no âmbito comercial, industrial, das relações de trabalho, da sustentabilidade ambiental, dos direitos do consumidor, dentre tantos outros; assim como os sistemas de segurança pública e privada obtiveram ganhos significativos, tanto na prevenção como responsabilização sobre riscos, perigos e danos provocados por quem quer que seja (lembremos somente da integração virtual entre polícias e instituições judiciárias em nível global, e os meios de integração transnacional da proteção de crédito no Mercado hoje vigentes).

Os recursos daquelas tecnologias de inteligência artificial têm possibilitado que descrições textuais e imagens gráficas de suspeitos procurados, ou pessoas desaparecidas, possam ser vistas na internet, assim como é possível reportar, virtualmente, atividades suspeitas de maneira mais eficiente às autoridades. Todavia, o crescimento da confiança nas tecnologias digitais e de comunicação provocam igualmente repercussões negativas, criando obstáculos por vezes intransponíveis para o cumprimento da lei, e isto porque as mesmas tecnologias que permitem acesso a receitas favoritas vindas de Madagascar, podem ser utilizadas para baixar informações sobre armas de destruição em massa. Indivíduos que surfam na web em busca de informações para suas férias podem perseguir e assediar vitimas enquanto usufruem os frutos de suas pesquisas. Em verdade, as várias vantagens proporcionadas pela internet (*wireless technologies, smart phones*) são tão atrativas quanto podem produzir riscos e perigos os mais diversos a indivíduos e comunidades inteiras enquanto ferramentas disponíveis no mercado.[7]

Podemos afirmar, pois, que os níveis e a prevalência de experiências criminais e intercâmbios informacionais daí decorrentes nunca estiveram tão altos como nestes tempos de revolução das tecnologias virtuais, o que complexifica os cenários de investigação ainda mais, ra-

zão pela qual autoridades do mundo todo estão reunindo esforços para criar normativas, práticas e colaborações efetivas para o enfrentamento de tais situações.[8]

Mas, afinal, no que consiste o ciberespaço e como ele tem se relacionado com ambientes os mais diversos de criminalidade?

CIBERESPAÇO E COMPORTAMENTO CRIMINOSO

O ciberespaço pode ser compreendido como local indefinido onde pessoas físicas e jurídicas realizam comunicações de inúmeras naturezas (afetivas, comerciais, industriais, educacionais, etc), podendo ser chamado de o lugar entre os lugares (DERY, 2018, p.213).[9] A despeito desta categoria, em tese, ter sido criada em 1984, pelo escritor de ficção científica William Gibson (2018, p. 41)[10], ela não é tão inédita assim, eis que comunicações eletrônicas tradicionais sempre estiveram presentes no imaginário e mesmo nas relações sociais ordinárias, basta lembrarmos dos sistemas de telefonia, telégrafos e rádios utilizados ao logo de todo o século XX.[11]

Nenhum outro método de comunicação converge áudio, vídeo e dados de forma tão efetiva como no ciberespaço. Diferentemente de outras ferramentas, a internet combina e-mails, telefones, e mídias sociais, expondo indivíduos e instituições a miríades de novas experiências, servindo ainda como local de encontros sociais, bibliotecas, espaço de trabalho e lazer, e tudo isto convivendo com as dimensões físicas da realidade quotidiana. Por outro lado, como nos adverte Sara Davies, a realidade virtual frequentemente é tomada, ingenuamente, como alternativa indolor de problemas do mundo corpóreo, na qual as pessoas abandonam seus problemas, transformando suas vidas em *perfis perfeitos* (DAVIES, 2019, p.51).

O curioso é que as modalidades de crimes de rua que deixam rastros e trilhas físicas de evidências, todavia, não são muito distintas das formas tecnológicas de delinquência existentes que, ingenuamente, confiam na promessa de anonimato total sugerida pela vastidão do ciberespaço para assegurar a não detecção por parte das forças de segurança pública. Ao mesmo tempo, pessoas físicas e jurídicas de ambos os universos (físico e virtual) tem procurado impedir/embaraçar estas forças de descobrir e perseguir as responsabilidades de atos criminosos através de subterfúgios como a *deep-web* e a *dark-web*.[12]

As tecnologias wireless e os bancos de dados e informações em nuvem melhoram ainda mais o uso das ferramentas tecnológicas, assim como tem operado simplificações radicais à realização e gestão de negócios – lícitos e ilícitos -em todo o mundo. Entretanto, tais avanços não tem se dado sem efeitos colaterais significativos, como o incremento de ferramentas criminais e *modus operandi* de associações delinquentes, dificultando as políticas de repressão e prevenção do Estado, evidenciando seus déficits de velocidade (ativa/reativa) e eficiência neste campo particular. Como nos diz Margaret Wertheim:

> *Infelizmente, o mundo real não acompanhou o ritmo da sua contraparte virtual. Assim, o sistema de justiça criminal em geral e os administradores policiais em particular foram forçados a confrontar problemas contemporâneos (por exemplo, a falta de fisicalidade criminal e a intangibilidade e vulnerabilidade das provas criminais) com ferramentas antiquadas.*[13]

Muitos países tem se tornado paraísos para pessoas físicas e jurídicas que intencionalmente burlam normas de regulação do espaço virtual, por certo que cobrando exorbitantes taxas e honorários, até porque as protegem de investigações e persecuções as mais diversas por negarem colaboração aos locais de origem a que pertencem. Tome-se, por exemplo, atividades criminosas que são realizadas por meios eletrônicos, de um país para outro; ou ilícitos virtuais perpetrados em determinados locais, mas pela via de provedores localizados em outros países, e assim por diante, fazendo com que as colaborações entre autoridades (nacionais e internacionais) sejam cada vez mais importantes.

A promessa de anonimato veiculada por inúmeros mecanismos de comunicação e transmissão de dados virtuais, associados com a escassez de colaboração investigativa e de persecução de ilícitos praticados nestes ambientes, faz com que inúmeros usuários destas redes se sintam protegidos, fomentando assim atividades desviantes. Tais cenários aumentam a potencialidade de danos provocados. Assim que assédios *on line*, manipulação de mercados e ações, pornografia infantil, tráfico de armas, órgãos humanos, pessoas, tem tido exponencial crescimento em todo o mundo (DENNING, 2018, p. 71).

Os chamados postadores anônimos nas redes virtuais têm aumentado a suscetibilidade e vulnerabilidade dos navegadores, frustrando, não raro, os esforços de cumprimento da lei, na medida em que se ocupam em esconder informações sobre as fontes de endereços dos quais

provem aquelas postagens, a despeito das ferramentas de encriptação de ponta a ponta que foram desenvolvidas para aumentar os níveis de segurança.[14]

Apesar de inúmeros governos estarem propondo legislações que poderiam constituir chaves criptografadas passiveis de serem acessadas por ordem judicial, investigações estatais são seguidamente bloqueadas por conta da ausência destas. Não bastasse isto, faltam a algumas agências de cumprimento de leis adequados recursos para, inclusive, identificar a presença de atividades criminais *on line*; e quando conseguem fazê-lo, por vezes, é tarde demais (LONG; MULLEN; RUSSEL, 2017, p. 39).

Diferentemente dos crimes tradicionais, onde a vitimização é costumeiramente óbvia, a detecção de cibercrimes e suas vítimas é frequentemente atrasada devido ao mascaramento dos instrumentos e meios com que se realizam, e embora investigadores especializados possam geralmente identificar o tempo e a localização do crime cibernético perpetrado, as tecnologias vão mudando em níveis cada favoráveis às mentes criminosas.

De fato, o exponencial incremento em termos de usuários de recursos/instrumentos virtuais, e mesmo em face dos diversos tipos de telecomunicações existentes, associado com o advento do acesso universal via wireless, tem dificultado em muito investigações responderem adequadamente – e em tempo ajustado – à coleta eficaz das voláteis evidências digitais.[15]

A investigação de crimes cibernéticos é frequentemente acompanhada por obstáculos recorrentes, pois enquanto investigadores tem se esforçado para se manterem a par das recentes tecnologias, ao mesmo tempo encontram certas dificuldades com a falta de interesse e iniciativas de determinados setores importantes, como o próprio poder legislativo, que deveria estar aperfeiçoando a legislação consectária; o poder executivo, que igualmente deveria se aperfeiçoar; e também o judiciário, que deveria estar se atualizando diante destas demandas.

Em verdade, o potencial de suporte das tecnologias de atividades criminais está sempre em franca expansão, enquanto que as formas de contenção e responsabilização por parte dos Estados anda em ritmo muito menor. Ou seja, a experiência tem revelado constantemente: (i) avanços e recuos em termos de normativas reguladoras destas matérias; (ii) o incremento de políticas públicas de prevenção e responsabilização de tais temas, bem como (iii) aumento das ações

institucionais de persecução penal aos responsáveis – diretos e indiretos – pelo cometimento de delitos cibernéticos.[16]

O surgimento do telefone, por exemplo, permitiu as pessoas aprimorarem já seus comportamentos desviantes, o planejamento de atividades criminais, bem como conspirar contra os limites jurídicos de suas ações quotidianas, criando com isto pletora de desrespeito a lei para as autoridades e o sistema de justiça. E em face disto, as estruturas institucionais de segurança pública precisaram lançar mão de novos mecanismos e procedimentos para alcançar crimes praticados por esta via, como o *Wire Act*.[17] A partir de experiências como estas, restou claro que o poder público deveria estar sempre atento a novas modalidades de riscos e perigos oriundos de inéditos meios de criminalidade com a utilização de recursos tecnológicos, os quais vão dar origem ao que conhecemos por cibercriminalidade, conceito que temos de aclarar de modo mais particular para os fins deste trabalho.

DEMARCAÇÕES CONCEITUAIS DO CRIME CIBERNÉTICO

A categorização de crimes cibernéticos não é simples em um mundo no qual as relações humanas e institucionais se complexificam cada vez mais pela via também da realidade virtual. Contudo, podemos identificar de pronto três categorias gerais de crimes cibernéticos mais recorrentes nos dias atuais: (i) **alvos**, situação em que estruturas e sistemas cibernéticos são vítimas de ataques e defraudações as mais diversas como objeto finalístico, visando justamente causar danos ao seu funcionamento; (ii) **meios**, quando ferramentas cibernéticas são utilizadas para o cometimento de ilícitos os mais distintos em face de bens e interesses alheios; (iii) **incidentes**, quando mecanismos, estruturas e sistemas cibernéticos são perifericamente manejados em operações criminosas, visando dar cabo de demandas maiores (WEBB, 2020, p. 59).

Em verdade, nem todos os ilícitos envolvendo computadores e realidade virtual podem ser caracterizados como crimes cibernéticos. Não seria correto categorizarmos, por exemplo e óbvio, um assalto residencial no qual fora subtraído computador como crime cibernético, tampouco o sequestro de remessas de drives físicos de computadores.

Mas o roubo de milhões de reais através de tecnologias de inteligência artificial é apropriadamente configurado como crime cibernético.

A despeito da ameaça global e permanente de atividades criminais cibernéticas se aperfeiçoarem e ampliarem com o tempo, os Estados têm de certo modo negligenciado na ação/reação a tais fenômenos, ao menos até elas defraudarem inúmeros sistemas de dados e informações – bancários, públicos e privados, dentre outros -, gerando cenários de insegurança muito perigosos, os quais, todavia, até por falta de políticas de prevenção eficazes, foram dando ensejo a reações severas em termos legislativos, políticos e jurisdicionais.

Um dos principais eventos que sinalizaram tais conjunturas, agudizando os cataclismas que crimes cibernéticos poderiam produzir, ocorreu em 1986, quando um erro contábil envolvendo valor menor do que um dólar foi investigado por servidor da Universidade da California, Clifford Stoll, revelando que um hacker alemão, Markus Hess, a serviço da KGB, tinha conseguido invadir banco de dados militares norte-americanos, obtendo informações sensíveis (mas não classificadas), usando somente um computador pessoal e modem simplificado. Uma vez conectado, o hacker conseguiu invadir o chamado sistema MILNET com notável facilidade e impunidade relativa (STOLL, 2023, p.28).

Veja-se que, não fosse a iniciativa daquele funcionário da Universidade, seria muito difícil detectar o ocorrido; e a despeito dos esforços terem sido dirigidos fundamentalmente às discrepâncias contábeis referidas, seus achados resultaram no reconhecimento de riscos de informações associados com os sistemas abertos da Universidade.

Entidades governamentais, tradicionalmente negligentes em termos de segurança cibernética, começaram a desenvolver, a partir de violações como esta, mecanismos de proteção eletrônica de seus bancos da dados, especialmente militares.

Em 1988, somente dois anos após o ocorrido no caso MILNET, legisladores norte-americanos foram forçados a reconhecer ameaças adicionais à segurança cibernética após o programa desenvolvido por estudante da Universidade de Cornell, Robert Morris, ter danificado mais de seis mil computadores, causando entre cinco e cem milhões de dólares de danos pelo ocorrido. Este programa, chamado de *Morris Worm*, atacou os computadores via internet, o que ensejou estudos intensos sobre as falhas de segurança nos sistemas informáticos das instituições – muitos usando o *Unix Operating System* -, sendo que os estragos provocados em cadeia sequer foram imaginados por seu criador.[18]

A partir de ocorrências como estas, a possibilidade de que hackers possam prejudicar ou mesmo interromper demandas ou serviços essenciais ao setor público e privado fizeram com que politicas de segurança (pública e privada) fossem aprimoradas e criadas, nomeadamente para os efeitos de identificar e responsabilizar diversos grupos organizados de hackers, como o já lendário *Legion of Doom*, criado na década de 1980 para abrigar ações de vários hackers - intelectuais, lícitas e ilícitas -, chegando a ser processados alguns de seus membros, o que deu maior sistematicidade de reflexões e deliberações envolvendo os riscos e perigos de movimentos como estes (MIDDLETON, 2017).

A raiz do termo *hacking* tem sido postulada pelo MIT, nos anos de 1960, quando o termo era usado por seus estudantes quando se referiam ao desenvolvimento de novas técnicas para identificar falhas computacionais, as quais eram perseguidas por fortes competitividades entre os alunos visando, justamente, superar uns aos outros, sendo que, nos anos 1980, o termo restou popularizado no filme *War Games*, período em que se deu também a explosão do que conhecemos por subcultura hacker e comunidade de hackers (THOMAS, 2015, p. 41).[19]

A emergência deste termo nas mídias, associado ao crescimento da acessibilidade e conectividade global, a partir dos anos 1980, deu impulso impressionante às atividades de hackers, sendo que cada vez mais jovens e adolescentes se ocupavam destas questões, nomeadamente motivados – inicialmente - por curiosidade e diversão. O problema destes jovens a época é que a viabilização de jogos computadorizados (games) reclamavam excessivos downloads através de acessos remotos discados, via modem telefônico, o que era muito caro, razão pela qual hackeavam linhas telefônicas para jogar.[20]

Hackers destes primeiros tempos referidos compartilhavam o sentimento de empoderamento baseado na possibilidade de deterem todo o conhecimento armazenado no ciberespaço, ao mesmo tempo em que elaboravam certa retórica *antiestablishment*, voltada contra o excessivo individualismo do neoliberalismo emergente da década de 1980 – de Ronald Reagan e Margareth Thatcher -, postulando acesso universal à informação e comunicação entre as pessoas. Lembremos de Loyd Blankenship, conhecido hacker e escritor norteamericano da década de 1980, tendo sido membro do *Legion of Doom*, e que defendia abertamente, em seu manifesto *the conscience of a hacker*:

> *Este é o nosso mundo agora... o mundo do elétron e do interruptor, a beleza da transmissão. Fazemos uso de um serviço já existente sem pagar por aquilo que poderia ser muito barato se não fosse administrado por glutões aproveitadores, e vocês nos chamam de criminosos. Nós investigamos... e vocês nos chamam de criminosos. Buscamos conhecimento... e vocês nos chamam de criminosos. Existimos sem cor de pele, sem nacionalidade, sem preconceitos religiosos... e vocês nos chamam de criminosos. Vocês constroem bombas atômicas, travam guerras, assassinam, trapaceiam e mentem para nós e tentam nos fazer acreditar que é para o nosso próprio bem, mas somos os criminosos. Sim, sou um criminoso. Meu crime é o da curiosidade. Meu crime é julgar as pessoas pelo que elas dizem e pensam, não pela sua aparência. Meu crime é ser mais esperto que você, algo que você nunca me perdoará. Sou um hacker e este é o meu manifesto. Você pode impedir esse indivíduo, mas não pode impedir todos nós.*[21]

Poderíamos dizer que estes primeiros hackers constituíram aos poucos certa subcultura, com ritos de iniciação, ética e estilos de vida, promovendo conferências anuais, encontros na Web, e solidificando suas relações e escopos. Tradicionalmente esses indivíduos se proclamavam buscadores de conhecimento, com a obrigação ética de relatar falhas de segurança aos administradores de sistemas informatizados e rejeitar quaisquer pessoas que usassem suas habilidades para fins nefastos. Embora alguns criminosos tenham sido encontrados em seu meio, a história revelou significativa relutância por parte da comunidade hacker em abrigar esses tipos de atividades, havendo registros de terem sido muito duros com aqueles que buscavam, pela cultura hacker, o cometimento de ilícitos os mais diversos.[22]

Inúmeras comunidades-hacker contemporâneas, todavia, tem perdido estas preocupações libertárias e ideológicas, até em face da tentação do dinheiro fácil que pode advir pela via práticas ilícitas, assim como de escopos distintos que a invisibilidade virtual fomenta, como a vingança, perseguições, ataques, transformando parte daquelas comunidades em agências de interesses os mais diversos, proliferando o surgimento de ferramentas de software especializadas em invasão de privacidade, intimidade e patrimônio.[23]

Por outro lado, também situações existenciais de tédio tem fomentado ações de voyeurismo informativo virtual (*technological thrill seekers*)[24]; desafios intelectuais provocam por vezes ações ilícitas para vencer barreiras cibernéticas de acesso a dados e informações; sen-

timentos de vingança por conta de ocorrências envolvendo relações familiares, afetivas, de trabalho, dão ensejo a medidas telemáticas de agressão institucional e pessoal; de igual sorte os fenômenos de satisfação sexual a qualquer custo tem se proliferado nas redes sociais; isto sem falarmos dos lugares já comuns envolvendo ilícitos econômicos (tráfico de drogas, armas, pessoas, terrorismos), políticos (*hacktivists, terrorists, spies*, etc.), de discriminação cultural, religiosa, étnica e racial espalhados pelo globo.

Instituições financeiras também são responsáveis por déficits de segurança cibernética em suas atividades ordinárias, falhando em apreciar os riscos e danos que podem ser infligidos por pessoas que inclusive são ou foram seus colaboradores, conhecedores de seus códigos de acesso e operação em sistemas de dados/informações virtuais. Daí porque a necessidade de se desenvolver políticas – públicas e privadas – de gestão destes dados/informações, preventiva e curativamente, a todo tempo.

A despeito da evolução cibernética e da comunicação global terem dramaticamente ampliado a população da criminalidade virtual – e das pessoas envolvidas com isto -, a tendência em categorizá-los em face dos níveis de sofisticação ou motivação tem sido recorrente, dentre os quais podemos citar:

(i) *Script kiddies*, também conhecidos como a forma mais baixa de exercício do cibercrime, pelo fato de serem hackers inexperientes que empregam scripts ou outros programas criados por terceiros para explorar vulnerabilidades de segurança ou comprometer os sistemas de computadores. Tecnologicamente os menos sofisticados de todos os cibercriminosos, geralmente não são capazes de escrever seus próprios programas e não entendem completamente os programas que estão executando. Assim, eles geralmente não conseguem atingir sistemas informáticos específicos, mas estão limitados aos alvos que possuem vulnerabilidades identificadas. Os menos avançados desta categoria até empregam software como *Deep Throat*.[25] As motivações para suas ações podem variar de brincadeiras simples, como quando estudantes universitários usam cavalos de Tróia para "esconder" remotamente os trabalhos de conclusão de curso de seus amigos; até lucro criminoso, como quando os usuários capturam informações de contas bancárias e senhas para acessar a conta da vítima.[26]

(ii) *Cyberpunks*, termo advindo da literatura de ficção científica e utilizado por oficiais da lei para identificar, de forma mais geral, pesso-

as que buscam causar danos a terceiros pela via da internet, nomeadamente em nome de radicais transformações da ordem social, associados também a vandalismos e programas destrutivos envolvendo vírus computacionais que causam danos, mas sem necessária intenção de ganho econômico.[27]

(iii) *Hackers* ou *Crackers*, são considerados os sofisticados criminosos virtuais capazes de criar programas, escrever códigos-fontes, e invadir complexos sistemas de inteligência artificial, sendo que os *hackers* identificam e exploram vulnerabilidades de sistemas de tecnologias da informação e de dados, geralmente sem interesse econômico, enquanto que os *crackers* utilizam seus conhecimentos da mesma forma, todavia, para alcançar objetivos econômicos pessoais.[28]

(iv) *Cybercriminal organizations*, por sua vez, são aqueles grupos compostos por indivíduos que se valem da internet para se comunicarem, colaborarem e facilitarem a prática de cibercrimes, sendo que suas motivações nunca são ingênuas, pois normalmente associadas com extremismos políticos, religiosos e ganhos econômicos. A sofisticação de seus métodos empregados, e a expertise técnica de seus membros, variam desde ações elementares até altamente complexas, atingindo pessoas físicas e jurídicas, do setor público e privado.[29] Importante ter presente que, a despeito de muitas fontes reportarem que estes grupos organizados tenham ultrapassado os amplos confins da WEB, na maioria dos casos mapeados por autoridades de segurança pública internacionais tem-se a informação de que, enquanto grupos tradicionais de crime organizado tem incorporado nas suas ações mecanismos de cibercrime, a maior parte das atividades criminosas cometidas na e pela WEB tem sido feitas por aquelas chamadas *cybercriminal organizations*, não envolvendo necessariamente delitos praticados por grupos organizados tradicionais. [30]

Muito especialmente no mercado da guerra as tecnologias avançam imensamente, tanto na direção de políticas de defesa como ataque, lícitas e ilícitas, a ponto de Arquilla e Ronfeldt assentarem que: *a ascensão do ciberespaço e de outras tecnologias de informação está a alterar a forma como as pessoas vivem, melhorando o poder e o desempenho das pequenas unidades e favorecendo o surgimento de formas de organização, doutrina e estratégia em rede, ao mesmo tempo que dificulta as grandes formas hierárquicas tradicionais*.[31] E isto efetivamente ocorre, pois grandes batalhas travadas hoje em termos globais não se dão fundamentalmente entre exércitos tradicionais dos Estados-Nação ou

aliados, com suas armas físicas enormes (tanques e bombas), aviões e frotas de forças armadas regulares, mas a partir de unidades virtuais pequenas e dispersas, que podem se posicionar com agilidade — em qualquer lugar, a qualquer hora. Eles sabem como penetrar e perturbar, assim como iludir e evadir, nomeadamente pela via das tecnologias da informação e inteligência artificial.[32]

É assim que se desenvolvem atividades de cibercrimes como contrabando de mercadorias e de materiais radioativos, órgãos humanos, lixos orgânicos e inorgânicos, prostituição adulta e infantil, organização de jogos de azar, compra e venda de assassinatos, extorsão, falsificações das mais diversas espécies, nomeadamente a de moedas em curso ou cartões de crédito, de identidades civis, tráfico de informações, de tecnologias, objetos de arte, dentre outros.[33]

Estas unidades estão operando em ambientes de redes que garantem pontos de contato capazes de constituir ações colaborativas, isto é, coalizões para realizar empreendimentos criminosos específicos e, se necessário, tomar medidas retaliativas contra rivais ou agências governamentais de segurança, daí porque *esta mudança para um modelo organizacional difuso, fluido, geografica e culturalmente diversificado, colocará desafios para a aplicação da lei, que mantém uma estrutura organizacional tradicional e hierárquica*.[34]

Ou seja, potencialmente, na criminalidade virtual vamos encontrar ameaças oriundas tanto de indivíduos isolados como de grupos organizados, e ambos com capacidade de danos imensos. Aliás, na percepção de Arquilla e Ronfeldt: *estruturas semelhantes a gangues online serão transitórias e situacionais. Ou seja, os cibercriminosos realizarão associações por períodos de tempo, talvez para se concentrarem em atingir determinados objetivos ilícitos, e depois irão se separar, cada um seguindo seu próprio caminho*.[35]

Assim, há certo consenso na literatura especializada que nem o compromisso pessoal nem a filiação estável e de longo prazo a grupos são características necessárias da organização criminosa online, e isto porque ela pode se constituir para o cumprimento de projetos específicos, imprimindo natureza transitória a pactos de composição de interesses e associações para fins ilícitos, nas quais os indícios tradicionais de comprometimento e filiação das antigas e novas máfias perdem importância. Em vez de empresas criminosas multigeracionais, a organização cibercriminosa enfatizará alianças associativas instrumentais e distantes. O que importa é se alguém está disposto e disponível para

unir forças em cumprir determinado empreendimento ilícito; quais são suas qualificações e se exibem o nível de confiabilidade necessário para a colaboração transitória.[36]

Também a organização criminosa online tende a não enfatizar as estruturas organizacionais hierárquicas formais, preferindo as contextuais e laterais mais amplas, sem circunscrever suas operações a fronteiras nacionais, territoriais, ou por diferenças culturais. Assim, ao contrário das organizações criminosas hierárquicas localizadas, rígidas e muitas vezes provinciais, os cibercriminosos costumam desenvolver coalizões regionais ou mesmo globais para suas ações delinquentes.

Costumamos associar, modo geral, a criminalidade praticada por meios virtuais à macrocriminalidade organizada e empresarial, de âmbito transnacional. Entretanto, no anuário de segurança pública brasileiro do ano de 2022, temos dados que evidenciam o crescimento vertiginoso da criminalidade eletrônica em delitos de baixa complexidade, como nos mostra o quadro abaixo[37]:

Brasil e Unidades da Federação	Estelionato por meio eletrônico								
	Ns. Absolutos				Taxas [2]				Variação 2018-2021 (%)
	2018	2019	2020	2021	2018	2019	2020	2021	
Brasil	**7.591**	**14.677**	**34.713**	**60.590**	**10,8**	**20,8**	**43,7**	**64,7**	**497,5**
Acre	5	3	1	53	0,6	0,3	0,1	5,8	916,0
Alagoas	205	452	1.003	3.248	6,2	13,5	29,9	96,5	1.464,4
Amapá [1] [4]	...	...	3	59	...	...	0,3	6,7	...
Amazonas	...	...	...	...	...	...	...	...	...
Bahia	...	...	...	...	...	...	...	...	...
Ceará	...	...	...	...	...	...	...	...	...
Distrito Federal	1.799	3.084	7.524	9.813	60,5	102,3	246,3	317,1	424,4
Espírito Santo [5]	...	...	...	...	...	...	...	...	...
Goiás	4	11	12	112	0,1	0,2	0,2	1,6	2.589,1
Maranhão	...	...	...	1.114	...	...	...	15,6	...
Mato Grosso	345	547	1.839	2.232	10,0	15,7	52,2	62,6	524,2
Mato Grosso do Sul	...	...	...	876	...	...	...	30,9	...
Minas Gerais	4.343	8.547	18.892	28.581	20,6	40,4	88,7	133,5	546,7
Pará [6]	561	1.305	1.838	2.764	6,6	15,2	21,1	31,5	377,9
Paraíba	-	-	-	70	...	...	...	1,7	...
Paraná	-	3	21	1.850	...	0,0	0,2	16,0	...
Pernambuco	...	...	...	...	...	...	...	...	...
Piauí	-	-	-	48	...	...	...	1,5	...
Rio de Janeiro	...	...	...	...	...	...	...	...	...
Rio Grande do Norte	...	...	...	39	...	...	...	1,1	...
Rio Grande do Sul	...	...	...	...	...	...	...	...	...
Rondônia [6]	...	...	...	...	...	...	...	...	...
Roraima	40	95	470	840	6,9	15,7	74,5	128,7	1.755,0
Santa Catarina	...	...	2.429	7.174	...	...	33,5	97,8	...
São Paulo [7]	...	...	...	...	...	...	...	...	...
Sergipe	20	14	8	73	0,9	0,6	0,3	3,1	255,6
Tocantins	269	616	673	1.644	17,3	39,2	42,3	102,3	491,3

Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Polícia Civil do Distrito Federal; Polícia Civil de Minas Gerais; Instituto de Segurança Pública/RJ (ISP); Instituto Brasileiro de Geografia e Estatística (IBGE); Fórum Brasileiro de Segurança Pública.

Por conta disto, progressivamente a legislação nacional tem levado a cabo algumas reformas da legislação penal sobre estes temas, como o caso do furto qualificado pela fraude eletrônica, nos termos do atual art.155, §4º-B, do Código Penal - CP[38]; o estelionato eletrônico, disposto no art.171, §2º-A, do mesmo estatuto[39]; também o crime de interrupção do processo eleitoral (art.359-N), do CP[40].

Ao nosso sentir andou mau o legislador aqui quando demarcou os dois primeiros delitos com expressões distintas, na medida em que, no furto eletrônico previu sua ocorrência em redes de computadores, enquanto que no estelionato eletrônico amplia o espectro de incidência para redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, não havendo sentido algum à diferença de tratamento.[41]

Já nos crimes contra a honra, descritos no capítulo V, do CP (calúnia, difamação e injuria (arts.138, 139 e 140)), tivemos igualmente o avanço no que tange as suas práticas pelas **redes sociais**, já que restou determinada majoração da pena em três vezes em tais situações.[42] Mas cumpre questionarmos se este conceito de redes sociais alcança, por exemplo, os espaços institucionais da intranet (enquanto rede privada de comunicação corporativa, gestão de dados e recursos internos), ou do WhatsApp, Telegram, etc. Pelos termos gramaticais da norma sob comento, em tese, não, o que evidencia déficits de compreensão e conceituação de tipos penais adequados para o enfrentamento destes fenômenos.

Outro passo importante dado recentemente no país foi a internalização oficial no sistema jurídico nacional da Convenção de Budapeste sobre crime cibernético, em face da publicação do Decreto Presidencial nº11.491/2023, realizada em 13/04/2023, comprometendo-se o país a adotar mecanismos legais eficazes à responsabilização de pessoas físicas e jurídicas beneficiadas diretamente por aqueles crimes, desde que praticados, no caso das empresas, por seus diretores, representantes legais ou agentes investidos de poderes decisionais. Por certo que esta responsabilidade penal corporativa, até então atacada pelos defensores do Direito Penal Liberal, ganha reforço com a adesão do Brasil a Convenção de Budapeste, tanto em sua vertente ativa como omissiva, pois a falha institucional na supervisão e fiscalização de seus operadores pode ser causa preponderante no cometimento de crimes cibernéticos. Mas de novo, há que se regulamentar melhor tal possibilidade, outra luta a ser empenhada pelas autoridades públicas nacionais.[43]

CONSIDERAÇÕES FINAIS

As capacidades e oportunidades oferecidas pela realidade virtual e internet têm transformado radicalmente muitas atividades individuais e de mercado legítimas, aumentando a velocidade, a facilidade e o alcance com que as relações e transações podem ser realizadas, ao mesmo tempo em que reduziram muitos dos seus custos.

Por outro lado, como na realidade física, também no mundo virtual tem surgido inéditas formas de lesões a interesses privados e públicos, desde o terrorismo, a pedofilia, o *bulyng*, piratarias, racismos, xenofobias, furtos, dentre outros. Isto tem se alastrado tanto que os órgãos de segurança pública e privada em todo o mundo tem desenvolvido estratégias e treinamentos para o seu enfrentamento, a despeito de que a legislação no ponto ainda seja deficitária.[44]

Sem sombra de dúvidas que os criminosos *on line* são de todos os tipos, e podem minar a segurança de nações inteiras, como é o caso do terrorismo, o tráfico de armas, pessoas e órgãos, além do que o comercio eletrônico tem igualmente provocado danos individuais e coletivos, drenando recursos financeiros de consumidores menos avisados e atentos; a própria representação política e as eleições são atingidas – direta ou indiretamente – por comportamentos virtuais de duvidosa licitude.

A partir da WEB pessoas aliciam crianças, arregimentam fundamentalistas religiosos, racistas, fomentam o preconceito étnico e de gênero, divulgam propagandas de ódio e violência, alimentam os extremismos políticos e ideológicos, compram e vendem o que pudermos imaginar, roubam dados de pessoas físicas e jurídicas, e os utilizam no mercado virtual. Ainda se opera, a partir da rede virtual de relações, o que os especialistas chamam de desinformação, ora entendida como difusão de informações falsas e distorcidas que, transitando de um lado a outro, é capaz de condicionar a opinião pública.

Autores como David Johnson e David Post, no ano de 1996, já chamavam a atenção para o fato de que as comunicações baseadas em inteligência artificial atravessam as fronteiras territoriais, criando novo domínio da atividade humana e minando a viabilidade – e legitimidade – da aplicação de leis baseadas em fronteiras geográficas. Enquanto essas comunicações eletrônicas destroem tais limites, surge outro, formado pelas telas e senhas que separam o mundo virtual do mundo real. Essa nova fronteira define o ciberespaço que precisa criar novas leis e instituições legais próprias.[45]

Por certo que ambientes virtuais não podem ser vistos ou demonizados como lugares propícios à criminalidade por excelência, isto porque é tão somente mais um espaço que pode, ou não, ser ocupado para o cometimento de ilícitos por indivíduos e grupos, e isto tem de ser dito justamente para não criar posições fundamentalistas justificadoras de controles radicais da vida das pessoas na realidade virtual.

Em verdade, assim como empresas lícitas migram seus negócios para a rede mundial em busca de novas oportunidades de lucro, empresas criminosas estão fazendo a mesma coisa. As organizações criminosas não são os únicos atores nos mercados ilícitos, mas muitas vezes são os mais importantes, principalmente por causa da "competitividade" adicional que é fornecida pela ameaça da violência organizada. Além disso, organizações criminosas tendem a ser excepcionalmente boas em identificar e aproveitar oportunidades para novos empreendimentos e atividades ilegais, tanto que têm cada vez mais contratado especialistas financeiros para conduzir suas transações de lavagem de dinheiro. Ou seja, o crime organizado não precisa desenvolver conhecimentos técnicos sobre a Internet, vez que pode contratar profissionais – dentre eles, hackers - que possuem experiência, garantindo, por meio de recompensas e ameaças, que eles executem suas tarefas de forma eficaz.

Para além disto, o sigilo costuma ser parte fundamental da estratégia do crime organizado, e a Internet oferece excelentes oportunidades para sua manutenção, já que suas ações podem ser ocultadas por inúmeros véus de anonimato. Citemos os casos recorrentes de extorsão cibernética envolvendo altos retornos aos delinquentes, e que são, muitas vezes, subnotificados, já que evidenciam inéditas vulnerabilidades que surgem com o aumento da dependência de sistemas em rede.

Por conta destes cenários vários tratados bilaterais de cooperação entre países nesta área têm surtido efeitos para fins de assistência legal e troca de informações e dados que contribuem em muito para o controle e responsabilização das ações criminosas, principalmente porque ampliam o poder instrutório e probatório das investigações e processos administrativos e jurisdicionais. Tais iniciativas inclusive possibilitam convergir compatibilidades de cooperação ou criar outras que são necessárias à eficácia das medidas de enfrentamento destas ameaças (como termos sistemas jurídicos com tipos penais idênticos ou análogos e ferramentas processuais adequadas, principalmente para cooperação internacional).[46]

Por conta disto é que se impõem o desenvolvimento, por parte de Estados e Governos, de conhecimentos especializados na área de crimes cibernéticos, bem como o compartilhamento eficaz de informações entre as agências dentro dos países e além das fronteiras nacionais. Além disso, esse compartilhamento deve ultrapassar os órgãos tradicionais de aplicação da lei para incluir as agências nacionais e internacionais de segurança e inteligência.

Também é essencial criar unidades de aplicação da lei especializadas para lidar com questões de crimes cibernéticos em nível nacional e internacional. Essas unidades podem fornecer bases tanto para a cooperação formal quanto para a cooperação informal baseada em redes de confiança entre agentes da lei.

O outro componente importante de estratégia de combate ao cibercrime é a parceria entre governos e a indústria, especialmente o setor de tecnologia da informação. A cooperação governo-setor privado desse tipo nem sempre é fácil, mas é claro que certo grau de confiança mútua pode fazer a diferença. Para que a cooperação seja efetiva, as agências de aplicação da lei devem ter muito cuidado e discrição para não expor as vulnerabilidades das empresas que cooperam, enquanto estas devem estar dispostas a denunciar qualquer atividade criminosa dirigida contra seus sistemas de informação e comunicação.

O Supremo Tribunal Federal - STF brasileiro vem dando sinais de preocupação com estas questões, nomeadamente no que toca as plataformas digitais e suas responsabilidades envolvendo publicações sobre pedofilia, pornografia infantil, permitindo ainda a veiculação e disseminação de discursos de ódio (nazistas, homofóbicas e racistas), e ataques às instituições democráticas, como as que ocorreram no dia 08 de janeiro de 2023, em Brasília, quando milhares de pessoas se articularam pelas redes sociais para invadir o planalto e prédios públicos os mais diversos (Congresso Nacional, STF), depredando bens da República de diversas naturezas.[47]

O Ministro Alexandre de Moraes, do STF, recentemente, sustentou a tese de que aquelas plataformas digitais devem ser consideradas empresas mistas, de tecnologia e de comunicação e publicidade, até em face dos milhões que arrecadam pelos serviços que vendem, e também porque possuem ferramentas de inteligência artificial para impedir a divulgação de conteúdos ofensivos, o que deveria ser estendido a discursos de ódio e antidemocráticos impulsionados e monetizados com o uso de algoritmos.[48]

Há muito ainda o que fazer.

NOTAS

[1] Como nos mostram os estudos de: (i) Lipovetsky, 2006, 2003, 1993; (ii) Han, 2012.

[2] Lembremos dos casos cinematográficos de Al Capone e suas operações em Chicago, na década de 1920. Neste sentido ver o texto de Hendley, 2021, p.19 et seq.

[3] CATANIA, 2016, p.21. – Tradução livre.

[4] BRENNER, 2002, p.12.

[5] BRENNER, 2012, p.03 – tradução livre. Por outro lado: *A imagem do crime organizado que surgiu durante esta época foi pensada para causar preocupação entre o público americano das décadas de 1950 e 1960. Por um lado, a Máfia foi denominada, muitas vezes em termos sinistros, como um grupo composto por "estrangeiros" (ou imigrantes recentes, que eram vistos da mesma forma) que não partilhavam os valores americanos.* (p.06). – Tradução livre.

[6] Conforme CRITCHLEY, 2019, pp.14/35.

[7] Documento das Nações Unidas advertem para isto: *A internet não é mais uma nova fronteira. Para muitos, o mundo digital tornou-se uma extensão natural da vida quotidiana. A pandemia da COVID-19 e as suas restrições apenas reforçaram esta realidade. Embora o crescimento do espaço digital tenha proporcionado muitas oportunidades legítimas, também expôs novos riscos. Com os criminosos e os terroristas a utilizarem cada vez mais a Internet para cometer e facilitar as suas ações ilícitas, o combate à utilização da Internet para fins terroristas tornou-se uma prioridade particularmente urgente*. – Tradução livre. UNITED NATIONS. The use of the internet. Disponível em: <https://www.unodc.org/unodc/en/terrorism/expertise/the-use-of-the-internet.html>. Acesso em: 22/05/2023.

[8] Como nos alerta BRENNER, 2012, vol.77, pg. 461, ao dizer que: *No mundo cibernético, a força física é insignificante; um hacker supera as defesas da vítima, não convocando esforços combinados de dez ou vinte hackers, mas usando tecnologia, técnicas automatizadas que permitem contornar as defesas eletrônicas. No mundo cibernético, a força está no software, não no número de indivíduos*. – Tradução livre.

[9] DERY, 2018, p.213.

[10] Ver no texto GIBSON, 2018, p.41 e seguintes.

[11] Nos EUA, já em 2009, aproximadamente 78% das pessoas utilizavam meios eletrônicos para comunicação, comparado com 10% no ano de 1995, conforme pesquisa do PEW RESEARCH CENTER. Social Media Fact Sheet. 07/04/2021. Disponível em:<https://www.pewresearch.org/internet/fact-sheet/social-media/>. Acesso em: 19/05/2023. Da mesma forma no Reino Unido, o crescimento de utilização destes mecanismos ainda resta mais evidente, pois oscilou de 1.9%, em 1995, para 83.2%, em 2009, conforme dados publicados no WORLD BANK GROUP PUBLICATIONS. World Development Indicators. 04/04/2011. Disponível em: <http://issuu.com/world.bank.publications/docs/9780821387092>. Acesso em: 19/05/2023.

[12] A pesquisa de Flaviano Alves demonstra que informações públicas na *Deep Web* são comumente de 400 a 500 vezes maiores que as definidas da *World Wide Web*. A *Deep Web* contém 7.500 *terabytes* de informações comparadas a 19 *terabytes* da *Surface Web*. Contendo aproximadamente 550 bilhões de documentos individuais (comparados com 1 bilhão da *Surface Web*). Na mesma investigação o autor diz que 06 das maiores enciclopédias da *Deep Web* contém cerca de 750 *terabytes* de informação, o suficiente para exceder o tamanho da *Surface Web* em 04 vezes. Em média, estes *sites* mais reservados recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral, sendo a categoria que mais cresce no número de novas informações sobre a Internet, e a profundidade de conteúdo de qualidade total deles é de 1.000 a 2.000 mil vezes maior que a da internet ordinária e de superfície. ALVES, 2018, p. 131.

[13] WERTHEIM, 2019, p.252. – Tradução livre.

[14] O problema é que meios de encriptação têm sido também utilizados por agentes criminosos para suas atividades rotineiras de quebra da lei.

[15] Lembremos que até há pouco tempo, modo geral, os provedores de internet não precisavam manter registros de suas operações.

[16] Conforme demonstra a pesquisa de REAGLE, 2019. O autor lembra que muitas vezes restou comprovado que violações de segurança institucional resultaram mais de práticas descuidadas de login do que de ataques direcionados; também por conta de funcionários que postam senhas em locais visíveis, permitindo que outras pessoas naveguem em seus computadores, usem nomes comuns para senhas, ou as divulguem para estranhos, o que tem representado igualmente riscos significativos à integridade das informações. E mais: *Deve-se notar que ignorar o perigo representado por ex-funcionários ou insatisfeitos não é um fenômeno novo. Muitos empregadores raramente mudam seus bloqueios depois que alguém se demite ou é demitido, contando com mecanismos de backup ou secundários. Outros não conseguem alterar os códigos de segurança ou, mais provavelmente, os padrões de códigos, alegando que as despesas associadas à reconversão profissional e a elevada taxa de rotatividade tornam impraticável a mudança de práticas sistêmicas. Muitas universidades, por exemplo, não alteram os códigos dos sistemas de registros dos alunos, baseando-se em senhas individuais e excluindo contas de usuários após o encerramento*. (p.48) – Tradução livre.

[17] O INTERSTATE WIRE ACT foi criado em 1961, nos EUA, com o fim especifico de proibir a operação de certos tipos de empresas de apostas, prevendo expressamente que quem estivesse envolvido em negócio de apostas utilizando conscientemente meio de comunicação por fio para a transmissão de comércio interestadual ou estrangeiro, ou informações que auxiliam na realização de apostas, em qualquer evento ou concurso esportivo, ou para a transmissão de comunicação eletrônica que dá direito ao destinatário de receber dinheiro ou crédito como resultado de apostas, ou por informações que auxiliam na realização de apostas, seria multado ou preso por não mais de dois anos, ou ambos. PLAYUSA. A guide to understanding the wire act. 23/08/2022. Disponível em: < https://www.playusa.com/us/wireact/#:~:text=The%20Interstate%20Wire%20Act%20of,the%20use%20of%20electronic%20wires>. Acesso em: 20/05/2023.

[18] Ver o artigo de DALY, 1993. Diz o artigo que quando Robert Morris reconheceu as possíveis implicações de suas ações divulgou mensagem anônima para vários programadores, dando instruções de como desativar o *worm*, mas seguramente isto não chegou a tempo e para todos os que foram atingidos por suas ações. Morris foi condenado judicialmente por ter violado o *Computer Fraud and Abuse Act* (CFAA), com sentença de 03 anos e liberdade condicional, 400 horas de serviços comunitários e multas de mais de U$10.000,00. Atualmente ele é professor do *Massachussetts Institut of Technology - MIT*, e membro do *Computer Science and Artificial Intelligence Laboratory* desta mesma instituição.

[19] *War Games* foi um filme dirigido por John Badham, em 1983, com roteiro de Lawrence Lasker e Walter Parkes, apresentando a trajetória de David Lightman (Matthew Broderick), jovem estudante que se conecta acidentalmente com o sistema de Defesa dos Estados Unidos e provoca um alerta acerca da possibilidade de conflito global entre os estadunidenses e russos.

[20] Lembremos que a chamada *culture hacking* não contempla somente aspectos negativos voltados ao cometimento de ilícitos para fins econômicos, políticos, ideológicos, etc., mas também está associado à cultura inovadora de empreendimentos lícitos inseridos no mercado de trabalho, como nos mostra a matéria CULTURE AMP. What is Culture Hacking? Disponível em: <https://www.cultureamp.com/blog/culture-hacking>. Acesso em: 20/05/2023. Ver também o excelente estudo de ALLEYNE, 2018, que faz dura crítica a tais temas.

[21] BLANKENSHIP, 2023. – Tradução nossa.

[22] Como nos informa COLEMAN, 2018, p.41e seguintes.

[23] Conforme a pesquisa de CHIESA, RAOUL; DUCCI; CIAPPI, 2018, p.34 e seguintes.

[24] Ver a interessante matéria no GLOBALSPEC. Teenagers'thrill seeking impulses can lead to cybercrime. Disponível em: <https://insights.globalspec.com/article/13352/teenagers-thrill-seeking-impulses-can-lead-to-cyber-crime>. Acesso em: 25/04/2023.

[25] Ver o interessante texto SECURITYWEEK. Edward Snowden: the geek turned deep throat. 29/06/2013. Disponível em: <https://www.securityweek.com/edward-snowden-geek-turned-deep-throat/>. Acesso em: 22/05/2023.

[26] REVERON, 2019, p.57 e seguintes.
[27] HAFNER; MARKOFF, 2020, p.13.
[28] Lembremos que, em 2012, a gigante do software de segurança Symantec foi vítima de tentativa de extorsão por hackers relacionados ao grupo *Anonymous*, que exigiam US$ 50.000 da empresa para não liberar o código-fonte do *pcAnywhere* e do *Norton Antivirus*. COMPUTERWORLD. Anonymous claims to have released source code of symantec's pcAnywere. 07/02/2012. Disponível em: <https://www.computerworld.com/article/2732196/anonymous-claims-to-have-released-source-code-of-symantec-s-pcanywhere.html, acesso em 19/05/2023.
[29] Ver as informações do escritório das Nações Unidas sobre Drogas e Crimes, no UNODC. Criminal groups engaging in cyber organized crime. Disponível em: <https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html>. Acesso em: 19/05/2023
[30] Ver as informações disponíveis no site do FBI, nos Estados Unidos da América -EUA. FBI. The cyber threat. Disponível em: <https://www.fbi.gov/investigate/cyber>. Acesso em: 19/05/2023.
[31] ARQUILLA & RONFELDT, 2017, p.35. – Tradução livre. Na sequência os autores lembram que: *ao contrário dos modos de conflito anteriores, as tensões ocorrem num espaço de batalha não linear, que é caracterizado não por um confronto concentrado entre grupos opostos homogéneos e claramente delineados, mas por um campo de conflito amplamente distribuído no qual forças amigas e inimigas estão misturadas*. (p.42). – Tradução livre. Na mesma direção ver o texto de ARQUILLA, 2021, p.55.
[32] Neste sentido ver o texto de ARQUILLA & RONFELDT, 2011, p. 56.
[33] Ver o texto de CASTELLS, 1999.
[34] ARQUILLA & RONFELDT, 2011, p.61. – Tradução livre.
[35] Idem, p.69. – Tradução livre.
[36] BRITZ, 2019, p.51.
[37] Pesquisa divulgada no documento do Fórum Brasileiro de Segurança Pública, Ano 16, 2022, conforme site: https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf?v=5. Acesso em: 20/04/2022, p.111.
[38] Art.155, §4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
[39] Art.171, §2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
[40] Art. 359-N. Impedir ou perturbar a eleição ou a aferição de seu resultado, mediante violação indevida de mecanismos de segurança do sistema eletrônico de votação estabelecido pela Justiça Eleitoral.
[41] Podemos indagar se tais delitos, como outros, poderia se dar pela via do WhatsApp, já que ferramenta de comunicação altamente utilizada para fins ilícitos também. E nos parece que é possível, pela via de *qualquer outro meio fraudulento análogo*, descrito no art.171, §2º-A, do CP.
[42] Esta alteração se deu em face do chamado Pacote Anticrime (Lei nº13.964/2019), e, nos termos do §2º, do art.141, do CP, restou consignado que, se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.
[43] Lembremos, todavia, que se revela imperioso à concretização real desta possibilidade a deliberação legislativa própria do Congresso Nacional brasileiro, em face de disposição expressa do art.5º, XXXIX, da Constituição Federal de 1988.
[44] Informações que estão disponíveis no site do FBI norteamericano sobre estes temas, identificando quem são as pessoas que costumam estar por trás de ações neste campo: *Quem está por*

trás de tais ataques? Eles abrangem múltiplos protagonistas - desde geeks de computador em busca de direito de se gabar... até empresas que tentam obter vantagem no mercado hackeando sites concorrentes, desde redes de criminosos que querem roubar suas informações pessoais e vendê-las no mercado negro... até espiões e terroristas procurando roubar informações vitais de nossa nação ou lançar ataques cibernéticos.- Tradução livre. In https://www.fbi.gov/investigate/cyber, acesso em 21/11/2017.

[45] POST; JOHNSON, 1996, p.1370. Aduzem os autores ainda que: *O ciberespaço mina radicalmente a relação entre fenómenos juridicamente significativos (online) e localização física. A ascensão da rede informática global está a destruir a ligação entre a localização geográfica e: (1) o poder dos governos locais para exercerem controle sobre o comportamento online; (2) os efeitos do comportamento online sobre indivíduos ou coisas; (3) a legitimidade dos esforços de um soberano local para fazer cumprir regras aplicáveis aos fenómenos globais; e (4) a capacidade da localização física de informar quais conjuntos de regras se aplicam.* – Tradução livre.

[46] Neste sentido ganham relevo as iniciativas e projetos do Grupo de Ação Financeira (GAFI), órgão fiscalizador global da lavagem de dinheiro e do financiamento do terrorismo, atividades estas que se valem, e muito, da realidade virtual, razão pela qual o órgão internacional tem estabelecido normas que visam prevenir estas atividades ilegais e os danos que causam à sociedade, conforme site https://www.fatf-gafi.org/en/home.html, acesso em 17/10/2023.

[47] Ver a matéria publicada em O GLOBO. Cronologia do terror: como golpistas promoveram um ataque histórico a República. Disponível em: <https://infograficos.oglobo.globo.com/politica/cronologia-golpistas-atacam-congresso-planalto-stf-brasilia.html>. Acesso em: 25/05/2023.

[48] Conforme informa noticia publicada em CONJUR. Redes sociais devem ser equiparadas a veículos de comunicações, diz Alexandre. 13/03/2023. Disponível em: <https://www.conjur.com.br/2023-mar-13/rede-social-considerada-veiculo-comunicacao-alexandre>. Acesso em: 25/05/2023.

BIBLIOGRAFIA

ALLEYNE, Brian. **Geek and Hacker Stories** – code, culture and storytelling from the technosphere. London: Palgrave Macmillan, 2018.

ALVES, Flaviano de Souza. **A criminalidade na Deep Web***.* In Revista da Escola Superior de Guerra, v.33, nº67, p.123/141, jan./abr. 2018.

ARQUILLA John & RONFELDT, David. **In Athena's Camp**: preparing for conflict in the information age. Washington: RAND, 2017.

ARQUILLA John & RONFELDT, David. **Networks and Netwars** – the future of terror, crime and militancy. Washington: RAND, 2011.

ARQUILLA, John. **Bitskrieg** – the new challange of cyberwarfare. Cambridge: Polity, 2021.

BLANKENSHIP, Loyd. **The conscience of a hacker**. Disponível em: <http://phrack.org/issues/7/3.html>. Acesso em: 31/03/2023.

BRENNER, Susan W. **Cybercrime, cyberterrorism anda cyberwarfare**. In Revue Internationale de droit pénal, 2012, vol.77.

BRENNER, Susan W. **Organized cybercrime**? How cyberspace may affect the structure of criminal relationships. In North Carolina Journal of Law & Technology, V.4 (1), 2002.

BRITZ, Marjie T. **Computer forensics and cybercrime**. New York: Pearson Education, 2019.

CASTELLS, Manuel. **Fim do milênio**: a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999.

CATANIA, Enzo. **Dalla Manno Nera a Cosa Nostra** – l'origine di tutte le máfia e dele organizzazioni criminali. Roma: Boroli Editore, 2016.

CHIESA, RAOUL; DUCCI, Stefania; CIAPPI, Silvio. **Profiling hackers** – the science of criminal profiling as applied to the world of hacking. New York: CRC Press, 2018.

COLEMAN, Gabriella. **Coding Freedom**. The ethics and aesthetics of hacking. Princeton: Princeton University Press, 2018.

COMPUTERWORLD. **Anonymous claims to have released source code of symantec's pcAnywere**. 07/02/2012. Disponível em: <https://www.computerworld.com/article/2732196/anonymous-claims-to-have-released-source-code-of-symantec-s-pcanywhere.html, acesso em 19/05/2023.

CONJUR. **Redes sociais devem ser equiparadas a veículos de comunicações, diz Alexandre**. 13/03/2023. Disponível em: <https://www.conjur.com.br/2023-mar-13/rede-social-considerada-veiculo-comunicacao-alexandre>. Acesso em: 25/05/2023.

CRITCHLEY, David. **The origin of organized crime in America**. New York: Routledge, 2019.

CULTURE AMP. **What is Culture Hacking?** Disponível em: <https://www.cultureamp.com/blog/culture-hacking>. Acesso em: 20/05/2023

DALY, Joseph P. **The computer fraud and abuse act** – a new perspective: let the punishment fit the damage. 12 J. Marshall J. Computer & Info. L. 445 (1993). Disponível em: <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1377&context=jitpl>. Acesso em: 24/05/2023.

DAVIES, Sarah R. **Hackerspaces**: making the maker movement. Malden, MA: Polity Press, 2019.
DENNING, Dorothy E. **Information Warfare and Security**. Toronto: Addison-Wesley, 2018.

DERY, Mark. **Escape Velocity**: cyberculture at the end of the century. New York: Grove Press, 2018.

FBI. **The cyber threat**. Disponível em: <https://www.fbi.gov/investigate/cyber>. Acesso em: 19/05/2023.

GIBSON, William. **Burning Chrome**. New York: Arbor House Pub.Co., 2018.

GLOBALSPEC. **Teenagers'thrill seeking impulses can lead to cybercrime**. Disponível em: <https://insights.globalspec.com/article/13352/teenagers-thrill-seeking-impulses-can-lead-to-cyber-crime>. Acesso em: 25/04/2023

HAFNER, Katie, MARKOFF, John. **Cyberpunk** – outlaws and hackers on the computer frontier. New York: Simon & Schuster, 2020.

https://www.fbi.gov/investigate/cyber, acesso em 17/10/2023.

https://www.fatf-gafi.org/en/home.html, acesso em 17/10/2023.

HAN, Byung-Chul. **La sociedade del cansacio**. Barcelona: Herder, 2012.

HENDLEY, Nate. **Al Capone** – Chicago's king of crime. Toronto: Dundurn Press, 2021.

LEAL, Rogério Gesta. **Criminalidade econômica e responsabilidade penal da pessoa jurídica: debates inconclusos**. São Paulo: Tirant lo blanch, 2022.

LIPOVETSKY, Gilles. **La era del vacío**. Barcelona: Anagrama, 1993.

LIPOVETSKY, Gilles. **La Societé de Déception**. Paris: Éditions Textuel, 2006.

LIPOVETSKY, Gilles. **Metamorfosis de la cultural liberal**. Barcelona: Anagrama, 2003.

LONG, Johnny Long; MULLEN, Tim and RUSSEL, Ryan. **Stealing the Network**—How to own a shadow. Rockland (MA): Syngress Publishing, 2017.

MIDDLETON, Bruce. **A history of cyber security attacks**. New York: Auerbach Publications, 2017.

MIDDLETON, Bruce. **Cyber Crime Investigator's** – field guide. New York: Auerbach Publications, 2012.

O GLOBO. **Cronologia do terror**: como golpistas promoveram um ataque histórico a República. Disponível em: <https://infograficos.oglobo.globo.com/politica/cronologia-golpistas-atacam-congresso-planalto-stf-brasilia.html>. Acesso em: 25/05/2023.

PLAYUSA. **A guide to understanding the wire act**. 23/08/2022. Disponível em: < https://www.playusa.com/us/wireact/#:~:text=The%20Interstate%20Wire%20Act%20of,the%20use%20of%20electronic%20wires>. Acesso em: 20/05/2023.

PEW RESEARCH CENTER. **Social Media Fact Sheet**. 07/04/2021. Disponível em:<https://www.pewresearch.org/internet/fact-sheet/social-media/>. Acesso em: 19/05/2023

POST, David G. and JOHNSON, David R. Law and Borders – the rise of law in cyberspace. In **Stanford Law Review**, vol.48, pp.1367/1402, 1996.

REAGLE, Joseph. **Hacking Life**. Systematized living and its discontents. Cambridge Mass.: MIT Press, 2019.

REVERON, Derek S. **Cyberspace and national security** – threats, opportunities, and power in a virtual world. Washington: Georgetown University Press, 2019.

SECURITYWEEK. **Edward Snowden**: the geek turned deep throat. 29/06/2013. Disponível em: <https://www.securityweek.com/edward-snowden-geek-turned-deep-throat/>. Acesso em: 22/05/2023.

STOLL, Clifford. **Stalking the wily hacker**. Disponível em: <http://pdf.textfiles.com/academics/wilyhacker.pdf>. Acesso em: 17/5/2023.

THOMAS, Douglas. **Hacker Culture**. Minneapolis: University of Minnesota Press, 2015.

UNITED NATIONS. **The use of the internet**. Disponível em: <https://www.unodc.org/unodc/en/terrorism/expertise/the-use-of-the-internet.html>. Acesso em: 22/05/2023.

UNODC. **Criminal groups engaging in cyber organized crime**. Disponível em: <https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html>. Acesso em: 19/05/2023

WEBB, Maureen**. Coding Democracy**. How hackers are disrupting power, surveillance and authoritarianism. Cambridge Mass. MIT Press, 2020.

WERTHEIM, Margaret. **The Pearly Gates of Cyberspace**. New York: W. W. Norton, 2019.

WORLD BANK GROUP PUBLICATIONS. **World Development Indicators**. 04/04/2011. Disponível em: <http://issuu.com/world.bank.publications/docs/9780821387092>. Acesso em: 19/05/2023.

Recebido em: 23-5-2023
Aprovado em: 18-10-2023

Rogerio Gesta Leal
Doutor em Direito do Estado, pela Universidade Federal de Santa Catarina, Brasil. Doutor em Direitos Humanos pela Universidad Nacional de Buenos Aires, Argentina. Mestre em Desenvolvimento Regional, pela Universidade de Santa Cruz do Sul, RS, Brasil. Mestrado em Direito. Desembargador do Tribunal de Justiça do Estado do Rio Grande do Sul, junto à Quarta Câmara Criminal, especializada em Crimes de Prefeitos e

Vereadores e Crimes contra a Administração Pública. Professor Titular da Universidade de Santa Cruz do Sul e da Fundação Escola Superior do Ministério Público do Rio Grande do Sul, nos cursos de Graduação. Especialista em Direito Constitucional pela Universidade de Santa Cruz do Sul, RS, Brasil. E-mail: rleal@unisc.br

Universidade de Santa Cruz do Sul
Av. Independência, 2293
Universitário, Santa Cruz do Sul – RS
96815-900