PUCRS

FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CRIMINAIS
DOUTORADO EM CIÊNCIAS CRIMINAIS

LEANDRO AYRES FRANÇA

CRIMINOLOGIAS CYBER:
O QUE É PROPRIAMENTE CRIME NO CIBERESPAÇO

Porto Alegre
2017

PÓS-GRADUAÇÃO - *STRICTO SENSU*

Pontifícia Universidade Católica
do Rio Grande do Sul

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CRIMINAIS

LEANDRO AYRES FRANÇA

CRIMINOLOGIAS *CYBER*:
O QUE É PROPRIAMENTE CRIME NO CIBERESPAÇO

PORTO ALEGRE
2017

LEANDRO AYRES FRANÇA

CRIMINOLOGIAS *CYBER*:
O QUE É PROPRIAMENTE CRIME NO CIBERESPAÇO

Versão definitiva para depósito da tese apresentada como requisito para a obtenção do grau de Doutor pelo Programa de Pós-Graduação em Ciências Criminais da Faculdade de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientadora: Profª. Dra. Ruth M. Chittó Gauer

PORTO ALEGRE
2017

LEANDRO AYRES FRANÇA

CRIMINOLOGIAS *CYBER*:
O QUE É PROPRIAMENTE CRIME NO CIBERESPAÇO

Versão definitiva para depósito da tese apresentada como requisito para a obtenção do grau de Doutor pelo Programa de Pós-Graduação em Ciências Criminais da Faculdade de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovado em: 10 de julho de 2017.

BANCA EXAMINADORA:

_____
Profª. Dra. Ruth M. Chittó Gauer - PUCRS

_____
Prof. Dr. Claudio Brandão - UFPE

_____
Prof. Dr. Gabriel Antinolfi Divan - UPF

_____
Prof. Dr. Ricardo Jacobsen Gloeckner - PUCRS

_____
Prof. Dr. Augusto Jobim do Amaral - PUCRS

PORTO ALEGRE
2017

Catalogação na Publicação (CIP)
Ficha Catalográfica feita pelo autor

F814c França, Leandro Ayres.
Criminologias cyber: o que é propriamente crime no ciberespaço / Leandro Ayres França. – Porto Alegre, 2017.
193 f.

Orientadora: Ruth Maria Chittó Gauer.

Tese (Doutorado) – Pontifícia Universidade Católica do Rio Grande do Sul, Faculdade de Direito, Programa de Pós-Graduação em Ciências Criminais, 2017.

1. Criminologia. 2. Tecnologia. 3. Ciberespaço. 4. Atuante. 5. Cybercrime. I. Gauer, Ruth Maria Chittó, orient. II. Título.

RESUMO

Vinculada à linha de pesquisa de *Violência, Crime e Segurança Pública* do Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul, a presente tese analisa a arquitetura do ciberespaço e as violações estruturadas e condicionadas por essa nova tecnologia, colocando em questão o que é propriamente *cyber* naquilo que chamamos de *cybercrimes*. A primeira parte da tese descreve, em linhas gerais, as diferentes perspectivas do debate sobre a (des)continuidade das criminologias tradicionais, questionando se são justificáveis criminologias alternativas para os crimes, desvios e ameaças *cyber*. Para isso, e com fundamento em recursos intelectuais diversos, são apresentados pressupostos fáticos e filosóficos que permitem uma nova proposição de definição e critérios criminológicos. A partir daí, a tese assume o pressuposto de que o desenvolvimento de um ambiente social novo e distinto, o ciberespaço, com suas próprias estruturas ontológica e epistemológica, formas de interação, funções e possibilidades, oportunizou a emergência de fenomenologias criminais inéditas, e que estas demandam, o que se convencionou chamar de, criminologias *cyber*. Uma vez que esta tese tem como objeto o estudo de crimes, desvios e ameaças desenvolvidos a partir de, e condicionados por, um novo ambiente (ciberespaço), a segunda parte do trabalho dedica-se às teorias criminológicas que tiveram como objeto principal o fator espacial na análise do fenômeno criminal e explica duas questões fundamentais do ciberespaço: sua neutralidade e sua arquitetura. No terceiro capítulo, explica-se como algumas teorias criminológicas tradicionais sobre a etiologia do comportamento desviante são adaptáveis ao contexto *cyber*, mas é destacada a necessidade de uma reconfiguração dos atores individuais em *atuantes*, tornando possível que sejam desenvolvidas novas formas de compreender conjuntos técnicos de humanos/objetos. Por fim, e para reforçar o argumento central da tese, é apresentada uma taxonomia geracional dos *cybercrimes*, acompanhada de explicações e críticas, permitindo, assim, uma compreensão mais clara e prática dos motivos, formas e impactos dos *cybercrimes*.

Palavras-chave: Criminologia. Tecnologia. Ciberespaço. Atuante. Cybercrime.

ABSTRACT

Linked to the *Violence, Crime and Public Security* research line of the Pontifícia Universidade Católica do Rio Grande do Sul's Graduation Program in Criminal Sciences, this thesis analyzes the cyberspace's architecture and the violations structured and conditioned by this new technology, questioning what is properly *cyber* about cybercrimes. The first part of the thesis describes, in broad lines, the different perspectives of the debate on the (dis)continuity of traditional criminologies, inquiring the need of alternative criminologies for the cyber crimes, deviations and threats. Therefore, and based on various intellectual resources, factual and philosophical assumptions are presented allowing a new proposition of criminological definition and criteria. From this, the thesis takes on the argument that the development of a new and distinct social environment, cyberspace, with its own ontological and epistemological structures, forms of interactions, functions and possibilities, enabled the emergence of unprecedented criminal phenomenologies, and that the latter require, what has been conventionally called, cyber-criminologies. Once this thesis has as object the study of crimes, deviations and threats developed from, and conditioned by, a new environment (cyberspace), the second chapter is dedicated to the criminological theories that were focused on space when analyzing the criminal phenomena and it explains two fundamental matters of cyberspace: both its neutrality and architecture. The third chapter explains how some traditional criminological theories on the etiology of deviant behavior are adaptable to the cyber context, though it is emphasized the need of a reconfiguration of individual actors into *actants*, making possible that new ways of understanding technical assemblages of humans/objects are developed. Lastly, and to undergird the thesis' main argument, a cybercrimes' generational taxonomy is presented, followed by explanations and critics, enabling then a clearer and more practical comprehension of cybercrimes' motives, forms and impacts.

Keywords: Criminology. Technology. Cyberspace. Actant. Cybercrime.

SUMÁRIO

INTRODUÇÃO

O maior desafio de escrever uma tese criminológica sobre um fenômeno que emerge exponencialmente é resistir aos cantos das sereias e prosseguir na rota previamente planejada. No trajeto, correm-se riscos de encanto com a novidade, de distração com as maravilhas de um novo horizonte, de sedução pelas notícias, de infinitos desvios que se apresentam, de tentação para a ação imediata. Por mais que a pesquisa e a redação tenham sido animadas por uma curiosidade sem fim, por mais que se tenha recorrido a argumentos filosóficos, jurídicos, sociológicos e de tantos outros campos, por mais que muitas veredas tenham se apresentado como possíveis, procurou-se manter a tese centrada na sua proposta de ser um trabalho criminológico. Simples assim.

Por isso, talvez a melhor introdução para esta tese seja o esclarecimento sobre o que ela não é. Primeiro, ela não apresenta um prelúdio histórico. As origens das tecnologias de informação, tal como seus impactos na sociedade, já foram bem documentados e examinados. O presente estudo reconhece essa distinta fenomenologia como de conhecimento geral. Segundo, ela não se concentra na identificação e na explicação das várias formas dos *cybercrimes*, e nas possibilidades de controle, seja por meio da regulação, da prevenção ou da responsabilização. A bibliografia sobre os *cybercrimes* é vasta e tem aumentado nos recentes anos, o que é compreensível porque ela indica que há problemas importantes a serem resolvidos, e eles são fluidos, mutáveis e estão em constante complexificação. Assim, a literatura taxonômica dos tipos de crimes não foi utilizada aqui, salvo para reforçar o argumento central da tese (das gerações dos *cybercrimes*). Terceiro, ela tampouco é sobre engenharia eletrônica, ciência da computação e segurança da informação. Por mais fundamentais que sejam essas ciências na discussão dos *cybercrimes*, suas explicações não cabem numa tese vinculada a um programa de ciências criminais.

Desde sua origem, o *cybercrime* carrega consigo um aspecto dramatizado; sua imagem primordial foi construída num período em que o desenvolvimento da tecnologia da informação e de rede estava intimamente ligado às narrativas de ficção científica. Mas, esse aspecto explodiu em espetacularização com a sociedade consumerista contemporânea, quando o crime se tornou também objeto consumível e essa realidade alterou o modo como o público em geral percebe o *cybercrime*. A ansiedade pública com relação aos crimes tornou-se norma e passou a pautar a vida cotidiana. Isso explica

porque singulares incidentes de *cybercrimes* têm o potencial de formatar a opinião pública e de fomentar a ansiedade geral, o que resulta em demandas políticas por soluções simples e imediatas para situações extremamente complexas. Considerado um risco atual, ubíquo e impessoal, a verdadeira natureza do *cybercrime* se ocultou diante de projeções emotivas que sobrepõem expressões de pânico dos riscos potenciais à avaliação ponderada dos riscos reais. Essa reação que interpreta equivocadamente a tecnologia em rede como criminogênica abre espaço a um modelo de administração pública que utiliza o crime como argumento e justificativa para seus atos (o que Jonathan Simon chama de *governo através do crime*) e incita duas consequências de ordem prática: a produção legislativa irracional e a aceitação de contramedidas tecnológicas, formatando, assim, uma ideologia da regulação.

Porque esta é uma tese criminológica, a minha preocupação foi iniciar – e, nesse aspecto, isso ainda é novidade – uma análise sobre a arquitetura do ciberespaço e as violações estruturadas e condicionadas por essa nova tecnologia, colocando em questão o que é propriamente *cyber* naquilo que chamamos de *cybercrimes*.

*

O problema inicial desta pesquisa buscava investigar criminologicamente o fenômeno do coletivo *Anonymous*, em prol da melhor compreensão dos anseios e conflitos sociais, no contexto ciberneticamente globalizado. O anteprojeto intitulava-se *Inimigos Anônimos*. No decorrer da pesquisa, entretanto, foi necessário um passo-atrás, foi necessária a ampliação do universo de investigação para um maior aprofundamento dos argumentos criminológicos empregados e uma análise crítica da arquitetura do ciberespaço e das ações potencialmente criminosas, desviantes ou ameaçadoras nesse ambiente. A tese, mantendo-se fiel ao seu compromisso criminológico original, assumiu, então, um objeto maior de pesquisa que pode contribuir para o esboço de teorias criminológicas alternativas.

A tese encontra-se dividida em quatro partes. A primeira delas se concentra na definição do objeto de pesquisa: a possibilidade de criminologias alternativas *cyber*. E inicia com três questões: como devemos chamar o estudo do novo fenômeno criminal (item 1.1); quais as diferentes perspectivas do debate sobre a (des)continuidade das criminologias tradicionais para os crimes, desvios e ameaças *cyber* (item 1.2); e, se o que se pretende é o desenvolvimento de uma nova teoria, com suas próprias formas de investigação, apta a compreender esse novo fenômeno com uma linguagem autêntica e contemporânea, e responder ao desafio de mudança e irrompimento, quais são os

pressupostos fáticos e científicos que permitem uma nova proposição de critérios e de definição (item 1.3)? Nesse terceiro ponto, é evidenciado como as tecnologias da informação provocaram transformações sobre nossas tradicionais percepções de espaço e tempo; de identidade, autonomia, poder e vitimização dos atuantes; de jurisdições para controle, regulação e responsabilização. A partir disso, a tese assume o pressuposto de que o desenvolvimento de um ambiente social novo e distinto, o ciberespaço, com suas próprias estruturas ontológica e epistemológica, formas de interação, funções e possibilidades, oportunizou a emergência de fenomenologias criminais inéditas, e que estas demandam, o que chamarei aqui de, criminologias *cyber*.

Uma vez definido que as criminologias *cyber* têm como objeto o estudo de crimes, desvios e ameaças desenvolvidos a partir de, e condicionados por, um novo ambiente (ciberespaço), a segunda parte do trabalho dedica-se, num primeiro momento, às teorias criminológicas estabelecidas que tiveram como objeto principal o fator espacial na análise do fenômeno criminal. Por sua relevância científica – aqui avaliada em razão da revolução paradigmática que mostraram, da qualidade de seus trabalhos e da influência que marcou nas criminologias contemporâneas e posteriores –, são resgatadas duas correntes criminológicas principais: as criminologias ecológicas (item 2.1.1), com suas pesquisas sobre a morfologia da criminalidade em meio ao desenvolvimento da urbe, e as criminologias culturais (item 2.1.2), com uma específica abordagem sobre a importância da geografia cultural. Se essas duas correntes demonstram como o espaço pauta as relações humanas e evidenciam o seu relevante papel na etiologia e no controle dos comportamentos desviantes, é possível considerar também o ciberespaço como um dispositivo que estrutura e condiciona os comportamentos dos atuantes? Para responder a isso, o item 2.2 traz um apresentação do ciberespaço: sua etimologia, seus sentidos de virtualidade, sua essência e suas características. E, na sequência, explica duas questões fundamentais do ciberespaço: sua (aparente) neutralidade e sua arquitetura (codificada).

No terceiro capítulo, são retomadas algumas correntes criminológicas derivadas da Escola de Chicago e de influência cultural, nas suas vertentes que exploraram o comportamento desviante, tais como as teorias sobre o conflito cultural (Sykes e Matza), a associação diferencial (Sutherland), as técnicas de neutralização (Sykes e Matza), a ação situacional (Pérez Suárez) e as criminologias culturais (Caldeira, Ferrell, Hayward, O'Brien, Young). Explica-se como algumas dessas teorias criminológicas tradicionais sobre a etiologia do comportamento desviante são adaptáveis ao contexto

cyber; mas, a partir de outros teóricos preocupados com o conjunto homem-máquina (Agamben, Brown, Dant, Latour), é destacada a necessidade de uma reconfiguração dos atores individuais em *atuantes*.

Por fim, e para reforçar o argumento central da tese, é apresentada uma taxonomia geracional nos *cybercrimes*: (*cyber*)crimes tradicionais ou de primeira geração, nos quais os computadores são utilizados no estágio preparatório do crime, para assistir violações tradicionais; *cybercrimes* híbridos ou de segunda geração, caracterizados como crimes tradicionais para os quais surgiram novas oportunidades globalizadas com as tecnologias da informação (hacking, ciberespionagem, ciberextorsão, ciberterrorismo, ciberfraude, golpe virtual, apropriação e pirataria de propriedade intelectual, pornografia infantil, veiculação de conteúdo violento ou perigoso); e *cybercrimes* próprios ou de terceira geração, produtos das oportunidades criadas pela internet e que somente podem ser perpetrados dentro do ciberespaço (hacktivismo, ciber-bloqueio, *botnets*, *spamming*, distribuição de *malware*, *leaking*). A referência a cada um desses tipos de *cybercrimes* é acompanhada de explicações e críticas, permitindo, assim, uma compreensão mais clara e prática de seus motivos, formas e impactos. O quarto capítulo se encerra com uma análise específica do caso do coletivo Anonymous, objeto original de investigação do anteprojeto, com o propósito de ilustrar a necessidade de novos paradigmas criminológicos para interpretar a evolução do fenômeno e de suas atividades, seus conflitos inéditos e as reações de controle.

Acompanha a tese um glossário (Anexo I) para elucidar o inevitável léxico *cyber* recorrente no texto e também uma lista de vocábulos com o morfema *cyber* dicionarizados (Anexo II) para justificar os argumentos apresentados no item 1.1 (Terminologia). No que se refere às traduções presentes nas páginas que seguem: quando não indicado tradutor na referência da obra, foram feitas pelo autor da tese.

*

O Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul registra dois outros trabalhos sobre *cybercrimes*, que foram de grande valia para a presente pesquisa.

Moreira de Oliveira defendeu, em 2002, uma dissertação dedicada a conceituar os delitos informáticos, como espécie do gênero da criminalidade contemporânea. O autor parte do pressuposto comum e bastante compartilhado que, desde o fim da década de 1980, tem ocorrido uma inflação penal – também descrita por outros autores como uma expansão do direito penal – como resposta aos anseios sociais.

(Esse fenômeno não pode ser contestado facilmente. Todavia, é preciso questionar, sem a intenção de maior aprofundamento nesta breve provocação[1], se essa expansão penal não é mero reflexo do processo de democratização do país – que demandou a elaboração de novos estatutos, adequados à nova Constituição –, e se essa expansão também não traduz o acompanhamento – talvez até insuficiente – da complexificação das relações sociais. Pense-se na rotina de um indivíduo em meados do século XX comparada às práticas sociais contemporâneas. Quantos serviços e contratos o indivíduo do século passado ativava em seu caminho de casa ao trabalho? Quantos serviços e contratos o indivíduo contemporâneo ativa quando, após solicitar um transporte privado urbano, é levado ao destino selecionado, previamente traçado por mapas GPS, sendo cobrado a partir de uma autorização anterior para o débito do valor no seu cartão de crédito, vinculado a uma instituição financeira, num intervalo de tempo que lhe permite trocar mensagens instantâneas, ler as notícias do dia e os posts de amigos, manifestar-se sobre eles com curtidas ou respostas, verificar arquivos mantidos em nuvens, tudo isso através de um aparelho celular, cuja comunicação é mantida por uma operadora telefônica, num conjunto de múltiplos contatos e contratos ativados por toques de dedos na tela de um aparelho que viaja com seu proprietário no banco traseiro de um automóvel – sem falar de todos os outros contratos ocultos à experiência direta deste que viaja, mas que sustentam todo esse processo de comunicação, como direitos autorais, publicidade, serviços de criptografia etc. De qualquer modo, deve-se concordar que o direito penal tem sido utilizado como recurso imediato para casos que poderiam ter outras soluções jurídicas.)

A preocupação de Moreira de Oliveira é relevante porque estabelece uma exigência da técnica legislativa para evitar excessos no controle social e no poder de punir, ou, como justifica o autor, para evitar que o "descaso conceitual [acarrete] como consequência prática a edição de mais leis penais, cujos bens jurídicos já estão devidamente tutelados dentro do ordenamento jurídico".[2] Seu recurso fundamental é, então, a identificação de um bem jurídico que justifique as criminalizações de condutas no ciberespaço, que é "a capacidade funcional dos sistemas informáticos".[3] E é a partir dessa identificação que o autor explora, então, as diversas atividades desviantes

[1] Provocação feita originalmente pelo professor Paulo César Busato ao autor da tese, há alguns anos, em conversa no seu gabinete.
[2] MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*. 2002. 160 f. Dissertação (Mestrado em Ciências Criminais) – Programa de Pós-Graduação em Ciências Criminais, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2002. p. 60.
[3] *Ibid.*, p. 95.

praticadas na atividade informática, já apresentando uma crítica à possibilidade da "redundância inoperante de uma tipificação assistemática" desses desvios.

A ideia é semelhante àquela trazida por esta tese, mas Moreira de Oliveira elabora suas críticas a partir da análise dogmática do bem jurídico – enquanto aqui se argumenta a partir da distinção geracional das condutas no ciberespaço e na defesa de que alguns crimes podem ser chamados propriamente de *cyber* porque são estruturados e condicionados pela tecnologia da informação. A principal distinção entre esses estudos – que se combinam em muitos pontos – repousa nas diferentes perspectivas adotadas: dogmática ou criminológica. Fato é que a criminologia ignora o conceito de bens jurídicos. A criminologia pode até estar atenta aos interesses e valores protegidos pela norma, mas ela se propõe a explicar as práticas e os processos em torno da criminalização: atores, vítimas, motivos, reações, controles, punições.

No segundo trabalho, apresentado em 2009, Colli defendeu uma dissertação (excelente, diga-se de passagem) sobre os limites e as perspectivas para a investigação preliminar policial brasileira de *cybercrimes*. Nela, Colli conceituou o *cybercrime* como sendo "aquele no qual um ou mais computador(es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais, conduta(s) criminalizada(s), ou são alvo(s) desta(s)".[4]

Tal como no trabalho de Moreira de Oliveira, a pesquisa de Colli possui um viés mais político-criminal (quando se concentra na investigação policial) e dogmático (porque limita seu escopo às condutas criminalizadas), e não muito criminológico (o que permitiria uma reflexão sobre a própria matriz do *cybercrime*, assim compreendido no seu sentido genérico de crime, desvio ou ameaça) – o que de forma alguma desqualifica o estudo. E há ainda uma segunda distinção entre a dissertação de Colli e esta tese: a categorização dos *cybercrimes* (que ele prefere denominar *crimes informáticos*). Tornando manifesta sua opção dogmática, Colli os divide da seguinte forma, *ipsis litteris*:

[4] COLLI, Maciel. *Cibercrimes*: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009. 172 f. Dissertação (Mestrado em Ciências Criminais) – Programa de Pós-Graduação em Ciências Criminais, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2009. p. 37.

> a) quando o computador é *utilizado* como *meio-fim* para a consecução de um crime, seja ele um *crime informático comum* ou um *crime informático específico*;
> b) quando o computador, ou algo nele constante ou inerente – armazenamento, transmissão e processamento de dados, acessórios ou instrumentos essenciais ao seu funcionamento –, é o próprio *objeto material* da conduta criminalizada, estando por detrás dessa proteção algum *bem jurídico* previsto pela norma jurídico-penal incriminadora.[5]

Em contraposição – mas sem que isso indique um juízo de maior ou menor acerto –, a categorização proposta nesta tese tem um motivo geracional e fundamento no quão condicionado é o *cybercrime* com relação à tecnologia da informação vigente.

Com esta tese, os *cybercrimes* voltam à pauta do PPGCCRIM/PUCRS. E se espera, como foi o caso dos trabalhos anteriormente apresentados, seja ela fonte de esclarecimento e reflexão, inspiração e contestação, para futuros estudos.

A presente pesquisa adota uma abordagem qualitativa, com objetivo exploratório e explicativo sobre o fenômeno criminal *cyber*. A partir de uma análise bibliográfica, o estudo questiona a *possibilidade* de criminologias alternativas para a compreensão dos *cybercrimes* estruturados e condicionados pela tecnologia da informação, trabalhando com a hipótese de que, enquanto para muitos casos um conjunto de saberes tradicionais permanecem válidos ao ciberespaço, podendo ser transposto ao novo ambiente, para comportamentos inéditos (*cybercrimes* próprios) há necessidade de uma articulação criminológica nova.

[5] *Ibid.*, grifos no original.

1 DEFINIÇÃO DO OBJETO

Três questões iniciais se apresentam: se os *cybercrimes* distinguem-se das formas tradicionais de crimes como uma nova categoria de atividade criminosa, (1.1) como devemos chamar o estudo do novo fenômeno criminal; (1.2) há teorias criminológicas ou adjacentes à criminologia já existentes e suficientes ou passíveis de adaptação; ou, (1.3) se o que se pretende é o desenvolvimento de uma nova teoria, com suas próprias formas de investigação, apta a compreender esse novo fenômeno com uma linguagem autêntica e contemporânea, e responder ao desafio de mudança e irrompimento, quais são os pressupostos científicos e recursos intelectuais atuais que permitem uma nova proposição de critérios e de definição?

1.1 TERMINOLOGIA

> Então, marcou-as com o nome respectivo, de modo que bastava ler a inscrição para identificá-las. [...] Pouco a pouco, estudando as infinitas possibilidades do esquecimento, percebeu que podia chegar um dia em que se reconhecessem as coisas pelas suas inscrições, mas não se recordasse a sua utilidade. Então foi mais explícito. [...] Assim, continuaram vivendo numa realidade escorregadia, momentaneamente capturada pelas palavras, mas que haveria de fugir sem remédio quando esquecessem os valores da letra escrita.[6]

O título desta tese é um neologismo introduzido pelo autor, sem qualquer pretensão de rotular o estudo acadêmico dos *cybercrimes* como uma criminologia inteiramente nova. Ele é utilizado tanto para indicar uma das possíveis criminologias alternativas, quanto como um modo de destacar o ponto principal deste ensaio: que a distinção dos crimes originados das – em vez de meramente facilitados pelas – tecnologias da informação engendra novas formas de compreender controles, crimes e punições. Enquanto alguns criminologistas têm oferecido explicações sobre os *cybercrimes* emergentes com base nos cânones criminológicos já existentes, este texto enfatiza que alguns *cybercrimes* não apenas são essencialmente novos, mas também que novas criminologias são necessárias para conceituá-los e os explicar.

Em sua origem, o verbo grego *kubernáō* (κυβερνώ) denotava a ação de dirigir, conduzir, guiar; o substantivo *kubérnēsis* (κυβέρνησις) identificava a pilotagem e o

[6] GARCÍA MÁRQUEZ, Gabriel. *Cem anos de solidão*. trad. Eliane Zagury. 58. ed. Rio de Janeiro: Record, [1967] 2005. p. 50-51.

governo; e a substantivação *kubernētikḗ tékhnē* (κυβερνητική τέχνη) definia a arte da pilotagem, ou, por conotação, o saber do governo. (Como será explicado adiante, no sentido grego original, *tékhnē* significava um modo de saber.) O étimo latino parece-nos mais familiar: *gubernator*.

Esse resgate etimológico oferece uma interessante reflexão e um primeiro indício de critério científico para a definição do objeto das criminologias *cyber*: a composição *cybercrime* indica que como tal deve ser definido aquele crime que é governado – ou seja: criado, mediado, controlado, dirigido – por uma técnica, por um saber próprio que emergiu com a própria tecnologia da informação.

O primeiro registro moderno do elemento de composição *cyber-* (ou *cybernet-*) somente apareceu em francês (1834), tendo *cybernetique* a acepção de "estudo dos meios de governo", em correspondência com o sentido grego.[7] Na língua inglesa, o matemático Norbert Wiener (1894-1964) atribuiu um novo sentido ao termo, definindo cibernética como "o estudo científico de controle e comunicação no animal e na máquina".[8] Colli explica melhor esse conceito:

> A *cibernética* possui como um de seus fundamentos a interatividade entre sistemas de controle e processamento de informações entre máquinas, seres vivos e sociedade. Em um modelo matemático-reducionista, WIENER pretendeu atribuir às leis gerais da matemática a possibilidade de prever-se, controlar-se e compreender-se a interatividade *retroalimentadora* existente entre homens, natureza e máquinas. A tarefa desempenhada pelo timoneiro frente ao leme de uma embarcação corresponderia claramente à alusão dessa interatividade em prol de um mesmo objetivo: a navegação (*finalidade*) orientada pelo homem (*controlador*), possibilitada pela nau (*máquina*).[9]

No discurso mais contemporâneo, *cyber* tornou-se um morfema lexical antepositivo a substantivos, utilizado para formar vocábulos compostos referentes à cultura da tecnologia da informação, computadores, realidade virtual e, mais especificamente, referente à internet, ou para denotar conceitos futurísticos.[10] A maioria dos vocábulos compostos já dicionarizados teve o seu estabelecimento a partir da década de 1990 e as composições já somam mais de meia centena (Anexo II), numa

---

[7] HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da Língua Portuguesa*. Rio de Janeiro: Objetiva, 2001.
[8] WIENER, Norbert. *Cybernetics, or control and communication in the animal and the machine*. Cambridge: MIT Press, 1948.
[9] COLLI, Maciel. *Cibercrimes*, *op. cit.*, p. 17, grifos no original.
[10] *OED Online*. Oxford: Oxford University Press, 2014.

representação tão onipresente que Pfohl referiu-se a uma *ciber-hifenização*[11]. É essa facilidade de composição de *cyber-* com outros vocábulos (ciberisso, ciberaquilo) e a sua direta conotação com a cultura de tecnologia de informação, computadores, realidade virtual e com a internet, que permite propor o título de *cibercriminologias* (ou, criminologias *cyber*) ao estudo científico da natureza, dos atores, das formas de expressão, do controle e da punição do comportamento delinquente no contexto telemático. Além disso, em inglês, *cyber* tem também uma função adjetiva, o que possibilita a melhor qualificação ou especialização de entes; nessa tese, farei empréstimo dessa aptidão declinativa da língua inglesa para o português e a palavra *cyber* terá aqui também a função caracterizadora.

Outros termos semelhantes já foram propostos. Jaishankar, em defesa de uma nova "subdisciplina" acadêmica, dentro do extenso âmbito da criminologia, que explique e analise os crimes na internet, propôs que ela fosse chamada de *cyber criminology*.[12] Para ele, "[o] campo da cibercriminologia cristaliza, para muitos cientistas e sociólogos uma área de pesquisa na interface entre a ciência da computação, o estudo da internet e a criminologia".[13] O criminólogo apresenta duas razões por que ele decidiu cunhar academicamente o termo: primeiro, o saber que lida com os *cyber crimes* não deve ser confundido com investigação criminal e, assim, imerso no conteúdo da *cyber forensics*; segundo, deveria haver uma disciplina independente para estudar e explorar os *cybercrimes* a partir de uma perspectiva das ciências sociais.[14] Mas, importante: enquanto Jaishankar empreende esforços para a elaboração de uma disciplina acadêmica, tendo inclusive já desenvolvido uma teoria a causação de crimes no ciberespaço[15], o objeto desta tese é a elaboração de uma teoria criminológica. Brown, com um entendimento semelhante ao apresentado no decorrer deste texto, prefere a denominação *criminologia virtual*.[16]

---

[11] "Da vigilância, das compras e do sexo cibernético à ciberfilosofia e mesmo aos sonhos utópicos da rebelião dos cyborgs – seja por diversão, ou por desespero, por desejo ardente ou por querer conexões mais apaixonadas e politicamente efetivas –, o mundo ao redor e dentro de mim aparece cada vez mais mediado por uma espécie de ciber-hifenização delirante da realidade." (PFOHL, Stephen. "O delírio cibernético de Norbert Wiener", *Revista FAMECOS*, n. 15, ago 2001. p. 106)

[12] JAISHANKAR, K. "Cyber Criminology: Evolving a novel discipline with a new journal", *International Journal of Cyber Criminology*, v. 1, n. 1, 2007, p. 1-6.

[13] *Ibid*., p. 1.

[14] *Ibid*., p. 1; *Idem*. "The Future of Cyber Criminology: Challenges and Opportunities", *International Journal of Cyber Criminology*, v. 4, n. 1&2, 2010. p. 26.

[15] *Idem*. "Establishing a Theory of Cyber Crimes", *International Journal of Cyber Criminology*, v. 1, n. 2, 2007, p. 7-9.

[16] BROWN, Sheila. "Virtual Criminology" In MCLAUGHLIN, Eugene; MUNCIE, John. *The SAGE dictionary of criminology*. 3. ed. London: SAGE, 2013. p. 486-488.

Como argumentado, defenderei que a distinção, a complexidade e a novidade do emergente fenômeno *cyber* justificam uma variedade de perspectivas plurais e alternativas, capazes de discutir o rápido surgimento de crimes previamente não conhecidos e não conhecíveis.

Quando se opta por utilizar o plural para designar um campo de estudo, já se parte do pressuposto que esse campo tem a capacidade de se adaptar às realidades que o inspiram e que são por ele desveladas. A criminologia tem essa capacidade de mudança e declinação? Ao que indica sua história, com as pequenas revoluções que ocorreram nos instrumentos conceituais e teóricos empregados, e sua diversidade temática, manifesta nas perspectivas alternativas contemporâneas, a criminologia tem demonstrado a habilidade de responder às "alterações sísmicas em seu terreno substancial"[17] e de atender à diversidade por meio do desenvolvimento de enquadramentos caleidoscópicos. Talvez, prossegue Zedner, a criminologia tenha maior facilidade adaptativa porque é uma disciplina intersticial: ela habita espaços de outras ciências sociais mais estabelecidas, distinguindo-se delas por seu interesse substancial com um tema específico (o crime), porém lhes subtraindo os estilos intelectuais, conceitos e ferramentas explicativas, com voraz capacidade de absorver novas ideias; e porque a criminologia, podendo desenvolver as ferramentas analíticas emprestadas conforme seus propósitos, mas livre dos grilhões da institucionalização disciplinar, é capaz de redefinições de seus pressupostos, valores e métodos, o que a possibilita a se adaptar à "topografia cambiante" do que é novo e do que precisa ser explicado.[18] É possível, então, falarmos em criminologias e, como afirmam Graham e McNeill, essa diversidade de alternativas é saudável e não precisa excluir potenciais sinergias ou o desenvolvimento de uma visão compartilhada.[19]

As criminologias *cyber* exemplificam hoje um conjunto de alternativas, construções e neologismos – sempre cambiantes – originados de novas experiências e reflexões. Ainda assim, nem todos os teóricos que se dedicam ao *cybercrime* concordam que um novo conceito é necessário para descrever o terreno e as atividades aqui referidas como criminologias *cyber*.

---

[17] ZEDNER, Lucia. "Pre-crime and post-criminology?", *Theoretical Criminology*, v. 11, i. 2, 2007, p. 261-281.
[18] *Ibid*., p. 268-269, 275.
[19] GRAHAM, Hannah; McNeill. "Desistência: Prevendo Futuros" In CARLEN, Pat; FRANÇA, Leandro Ayres. *Criminologias alternativas*. Porto Alegre: Canal Ciências Criminais, 2017. p. 573-593.

1.2 A (DES)CONTINUIDADE DAS CRIMINOLOGIAS TRADICIONAIS

Nas recentes três décadas, período em que houve uma revolução nas tecnologias de informação, as seguintes questões têm sido apresentadas. Haveria uma implícita presunção, promovida como reação a um inédito fenômeno, de que há algo novo, distinto da compreensão tradicional de crime? Essa presunção não esconderia que há muito "vinho velho em novas garrafas"? Ou há, de fato, algo como *cybercrime*, que exige articulações criminológica, dogmática e político-criminal próprias?

As respostas a essas perguntas podem ser classificadas num matiz que varia entre a ideia (tradicionalista) de que os *cybercrimes* são fundamentalmente crimes tradicionais executados por meio da tecnologia da informação e a ideia (adaptacionista) de que os *cybercrimes* marcam uma descontinuidade com os crimes tradicionais. Nesse intervalo, é ainda possível que autores adotem ambas as perspectivas. Siegel, por exemplo, define *cybercrime* como "qualquer ato criminoso que envolve redes de comunicação, de computador e de internet" (continuidade), no entanto, alguns parágrafos antes da definição, descreve-o como "uma nova espécie de infrações" (descontinuidade).[20] Os posicionamentos intermediários, todavia, não respondem aos questionamentos feitos. Por isso, aqui são tratadas as perspectivas mais polares.

1.2.1 Tradicionalistas (ou céticos[21])

Num plano geral, quanto à necessidade de uma articulação criminológica própria para o fenômeno *cyber*, alguns autores concluem que não há necessidade – ao menos, no presente momento – de uma nova criminologia que compreenda o fenômeno dos *cybercrimes*, sendo suficientes para entendê-los, analisá-los e explicá-los os conceitos e teorias criminológicos já estabelecidos. Na análise mais específica do fenômeno, o que pode ser extraído em comum dos argumentos desses autores é que a tecnologia é reduzida a um mero meio, através do qual indivíduos utilizam máquinas para atacar outras máquinas e outras pessoas. Em outras palavras, a criminalidade virtual é basicamente a mesma do crime terrestre com o qual estamos acostumados, diferenciando-se aquela somente em termos do meio.

---

[20] SIEGEL, Larry J. *Criminology*: theories, patterns, and typologies. 10. ed. Belmont: Wadsworth, 2010. p. 468.
[21] YAR, Majid. "Online Crime", *Oxford Research Encyclopedia of Criminology*, 2016.

Brenner, por exemplo, questiona se há uma implícita presunção, promovida como reação a um inédito fenômeno, de que há algo novo, distinto da compreensão tradicional de crime, e se essa presunção não esconderia que *há muito vinho velho em novas garrafas* – ou seja, que os *cybercrimes* contêm os elementos constitutivos dos crimes tradicionais.[22]

Partindo do pressuposto tradicional da *commom law* anglo-saxã de que o crime compõe-se de quatro elementos – estado mental (*mens rea*), conduta (*actus reus*), circunstâncias presentes (semelhante à avaliação de antijuridicidade em nosso ordenamento) e resultado ou dano proibido –, Brenner realizou uma análise empírica de diversos crimes com o propósito de verificar se eles se apresentavam como novas variedades de conduta ilícita ou se eles indicavam meramente o cometimento de um crime tradicional em um novo espaço (ciberespaço); nesse caso, sendo o ciberespaço simplesmente um meio utilizado para o cometimento de crimes tradicionais, não haveria, pois, necessidade de se reconhecer uma distinta categoria *cybercrime*.[23]

A primeira anotação que precisa ser feita é que a existência de um agente causador é um elemento incontestável: tanto os crimes tradicionais quanto os *cybercrimes* só se realizam a partir de um comportamento, ativo ou omissivo, de um ou mais indivíduos. Essa é uma constatação óbvia, contudo fundamental porque, em razão dela, estabelece-se um novo elemento de análise: os atuantes dos *cybercrimes*. Brenner entende, porém, que, sendo a figura do agente uma constante dos crimes tradicionais e dos *cybercrimes*, e que não parece haver motivo para se estabelecer diferentes níveis de culpabilidade entre as duas categorias, poder-se-ia eliminar esse elemento como ponto de distinção entre os dois fenômenos.[24] Assim, Brenner concentra-se nos outros três elementos: conduta, circunstância e resultado. Segundo ela, são esses elementos hipoteticamente distintos que constituem duas categorias de atividade criminosa a partir de uma divergência empírica: o espaço no qual os crimes são cometidos.[25]

Crimes admitidos como tradicionais são aqueles cometidos no assim chamado mundo real: as condutas para o cometimento do crime, as circunstâncias envolvidas no ato e os resultados dele ocorrem em espaços concretos. Essa concepção é pautada pelo

---

[22] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?" *California Criminal Law Review*, v. 4, i. 1, 2001. A publicação original solicita que as citações façam referência aos parágrafos do artigo, devendo ser indicado o seu número acompanhado da marca de parágrafo (¶), sinal gráfico pouco utilizado em português para esse fim. Nas referências subsequentes, seguiu-se essa recomendação.
[23] *Ibidem*.
[24] *Ibid*., ¶ 8.
[25] *Ibid*., ¶ 9.

próprio modelo de direito penal moderno, o qual, como premissa fundamental, limita a responsabilização às condutas, ativas ou omissivas, que ocorram no mundo físico, excluindo de sua alçada as ações não externalizadas, como os pensamentos.[26]

A hipótese de Brenner é que crimes tradicionais também podem ocorrer nos dois espaços – na realidade *física* compartilhada e na realidade *conceitual* compartilhada –, sem que sejam distintos em seus elementos constitutivos. Crimes de furto de valores, por exemplo, podem correr no espaço físico e no espaço virtual, preservados os mesmos elementos de conduta, circunstâncias pertinentes e resultado de dano. Nesses casos, o ciberespaço é somente o meio pelo qual o crime é realizado.[27] O furto de informações, por sua vez, é um pouco mais complexo: no caso em que a vítima se vê privada da informação subtraída, trata-se de uma clara variação do tradicional crime de furto; quando o criminoso copia as informações (ou um software), o resultado deixa de ser uma "soma zero" que identifica a clássica subtração, então, ocorre uma indevida diluição da propriedade porque a vítima já não é a única em posse das informações. De qualquer forma, os elementos constitutivos restam preservados.[28]

O mesmo raciocínio, segundo ela, aplica-se aos crimes de fraude[29], de falsificação[30], de pornografia[31], de *stalking*[32], de vandalismo (extensível à propagação de programas maliciosos e *denial of service attacks*)[33], invasão de propriedade (por extensão, *hacking*) e invasão de propriedade com intenção de cometer crime subsequente (por extensão, *cracking*)[34], e de vigilantismo e terrorismo (por extensão, hackitivismo ou ciberterrorismo)[35]. Em todos esses casos, conclui Brenner, princípios tradicionais do direito penal podem ser utilizados para responsabilizar essas variedades de crimes, o que torna desnecessário uma nova criminalização da conduta como *cybercrime*, sendo, porém, possível e aconselhável a extensão da redação típica para abranger os novos meios.[36]

Seria possível que houvesse, então, crimes autenticamente identificados como *cybercrimes*, cujos elementos constitutivos se manifestariam exclusiva ou quase

---

[26] *Ibid*., ¶ 10.
[27] *Ibid*., ¶ 41-43.
[28] *Ibid*., ¶ 44-47.
[29] *Ibid*., ¶ 51-55.
[30] *Ibid*., ¶ 56-58.
[31] *Ibid*., ¶ 59-60.
[32] *Ibid*., ¶ 61-68.
[33] *Ibid*., ¶ 69-76.
[34] *Ibid*., ¶ 77-86.
[35] *Ibid*., ¶ 95-98.
[36] *Ibid*., ¶ 39-50, 99.

exclusivamente no ciberespaço? Brenner cita o incidente ocorrido na comunidade virtual LambdaMOO, no ano de 1993, quando um participante da comunidade, Mr. Bungle, utilizando um subprograma, forçou avatares de outros usuários a realizarem atos sexuais. Na época, questionou-se se a ação do usuário por trás de Mr. Bungle teria alguma adequação legal; de pronto, foram descartadas as possibilidades de tipificação do ato como crimes de estupro, pornografia e *stalking*. Para Brenner, este foi o único exemplo relatado de um crime essencialmente virtual (interpretação da qual discordo, como se verá adiante), em que quase todos os elementos constitutivos ocorreram no ciberespaço – salvo, ressalta ela, o pressionar das teclas e o sofrimento das vítimas. Nesse caso, seria impossível uma extensão legislativa ou uma interpretação que revisasse as normas penais, sob risco de alteração da natureza das prescrições normativas ou seu esvaziamento por vagueza em decorrência de uma ampliação demasiada.[37]

Como não é possível impor a responsabilização penal para uma variedade de injustos que emergem no ciberespaço somente expandindo as definições legais existentes para que envolvam as atividades físicas e virtuais, Brenner indica duas soluções para os *cybercrimes*: primeiro, a utilização de princípios existentes para definir (criar) novos crimes que compreendam esse tipo de injusto; segundo, o estabelecimento de novos princípios para a responsabilização penal voltada aos *cybercrimes*.[38] "Para o presente," argumenta ela, "parece que nós podemos responder adequadamente a novas variedades de más condutas situadas no ciberespaço utilizando tradicionais princípios de direito penal para instituir novos crimes que compreendam esses comportamentos".[39] Mas, como essa proposta apresenta uma sequência predeterminada, pode-se recorrer à segunda solução na eventualidade de insatisfação da primeira, isto é, a criação de uma nova e autêntica *cyberlaw*[40], o que também se justificaria por razões simbólica ("para deixar claro que embora o ciberespaço seja um novo mundo, nós esperamos que ele se conforme aos padrões que aplicamos em nosso velho mundo (físico)"[41]) e pragmática (tratamento diferenciado para crimes com "maior magnitude potencial de dano causado pelo cibercriminoso" ou que apresentem "maior possibilidade de que ele ou ela evite ser

[37] *Ibid*., ¶ 102-111.
[38] *Ibid*., ¶ 113.
[39] *Ibid*., ¶ 120.
[40] *Ibid*., ¶ 113, 120.
[41] *Ibid*., ¶ 121.

processado"[42]) – apesar de essas razões adicionais serem facilmente contestáveis[43]. Contudo, defende a autora que esse tempo de tratamento diferenciado a infratores virtuais, de criação de um conjunto de prescrições normativas que envolvam novos tipos de atividade criminal, de implementação de um novo sistema de responsabilização penal, algo como, escreve ela, uma *responsabilização supercriminal*, é um tempo que pode vir, mas não chegou, ainda no domínio da especulação.[44]

Apoiando-se na teoria criminológica da atividade rotineira, Grabosky afirma sucintamente que a teoria, inicialmente derivada para explicar crimes convencionais "de rua", é igualmente aplicável aos crimes no ciberespaço.[45] Essa teoria pode ser compreendida como a síntese das explicações *dispositiva* e *situacional* do desvio e do crime.

As *teorias dispositivas* analisam mecanismos causais (biológicos, psicológicos, sociais, econômicos, culturais) que explicam por que alguns indivíduos ou grupos apresentam tendência ao comportamento delinquente. Cesare Lombroso, Émile Durkheim, Robert K. Merton, William Chambliss *et al.* são exemplos de criminólogos que, com suas respectivas peculiaridades, buscaram compreender essa disposição criminosa.

As *teorias situacionais* não negam que motivações pessoais podem ser incitadas por esses mecanismos, no entanto, essas incitações não oferecem condições suficientes para que alguém cumpra a tendência em uma atividade infratora; assim, seriam as situações sociais que medeiam decisões sobre agir ou não conforme a inclinação.

Aproveitando ambas as perspectivas, a teoria da atividade rotineira busca examinar o modo como a organização espaço-temporal de atividades sociais contribuem para que os indivíduos traduzam suas tendências criminais em ações. (Por essa razão, considera-se uma abordagem ecológica.) Tal como outras abordagens teóricas, a teoria traz consigo diferentes formas, variados conceitos e distintos níveis de análise, os quais se constituíram a partir de orientações específicas de criminologistas e também do natural processo de revisão e reconstrução teóricas; ainda assim, para o momento, é possível descrevermos a teoria tomando como base a sua hipótese original: atos

[42] *Ibid*., ¶ 122.
[43] *Ibid*., ¶ 123-125.
[44] *Ibid*., ¶ 126-127.
[45] GRABOSKY, Peter N. "Virtual Criminality: Old Wine in new Bottles?", *Social & Legal Studies*, v. 10, n. 2, 2001, p. 243-249.

criminosos exigem a convergência, no espaço e no tempo, de *pretensos infratores*, *alvos aptos* e a *ausência de protetores capazes*. Ou pela fórmula:

motivação + oportunidade – guardião capaz

Grabosky é cauteloso: "Enquanto a tecnologia de implementação, e particularmente sua eficiência, podem ser sem precedentes, o crime é fundamentalmente conhecido."[46]

Primeiro, as motivações criminosas não são novas; segundo ele, as tecnologias podem mudar rapidamente, mas não a natureza humana: "Os Dez Mandamentos são tão relevantes hoje quanto o foram nos tempos bíblicos. A animação pelo engano caracterizou não menos a inserção do Cavalo de Troia original do que o fez a criação de seus descendentes digitais."[47]

Segundo, o crescimento exponencial na conectividade da computação e das comunicações criaram paralelas oportunidades para possíveis infratores, assim como paralelos riscos para possíveis vítimas: "Conforme a internet se torna, cada vez mais, um meio de comércio, ela se tornará, também de modo crescente, um meio de fraude."

E, terceiro, levando em consideração a evolução histórica da guarda capaz (do feudalismo ao surgimento do Estado e a proliferação de instituições públicas de controle social, até o momento presente de muitas democracias em que empregados de serviços de segurança privados ultrapassam em números os agentes policiais), o policiamento no ciberespaço é um esforço pluralístico tanto no espaço virtual quanto no espaço terrestre: "As responsabilidades pelo controle dos *cybercrimes* será similarmente compartilhado entre agentes do Estado, especialistas em segurança da informação no setor privado, e os usuários individuais." E ele prossegue: "No ciberespaço, hoje, como no espaço terrestre, há dois milênios, a primeira linha de defesa será a autodefesa."

Tendo aqueles paradigmas criminológicos como fundamento, Majid Yar, por sua vez e de modo mais aprofundado, propôs-se a testar a aplicação da teoria da atividade rotineira ao fenômeno dos *cybercrimes*.[48] Seria essa teoria, já parcialmente validada para os crimes tradicionais, também aplicável no ciberespaço? Como a existência de *pretensos infratores* é dada como pressuposto certo para a hipótese, tanto no mundo

[46] *Ibidem*.
[47] *Ibidem*.
[48] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *European Journal of Criminology*, v. 2, i. 4, 2005, p. 407-427.

físico quanto no virtual, Yar preocupa-se em analisar os outros elementos da teoria: *espaço, tempo, alvos* e *protetores*.

O primeiro passo para responder ao texto hipotético, pois, é verificar se o ciberespaço apresenta uma ontologia espaço-temporal congruente com aquela do mundo físico. Yar acredita que é exagerada a defesa de que não é possível reconhecer uma topologia espacial no ciberespaço, argumento que estabelece uma separação absoluta entre ambientes real e virtual, como ordens ontologicamente distintas.[49] Aproveitando a ideia de Manuel Castells, Yar defende que o ciberespaço, melhor do que uma *realidade virtual*, deve ser entendido como uma *virtualidade real*, um ambiente interacional sócio-tecnicamente gerado enraizado no mundo real das relações políticas, econômicas, sociais e culturais. Nesse sentido, o ciberespaço traduziria ou reproduziria características do mundo real ao espaço virtual.[50]

Outro argumento apresentado por Yar contesta a ideia de equidistância do ciberespaço. A maior distância, nesse caso, não seria medida pela extensão física, mas pelo dispêndio de tempo e esforços para alcançar determinada informação, pessoa ou *site*, em uma atividade que poderia ser também medida por cliques.[51] Exemplo prático disso seria a diferença entre o acesso de um conteúdo que carregue *hyperlink* (o que o torna prioritário num mecanismo de busca) e o acesso a um conteúdo não indexado (que integra a chamada *deep web*).

No entanto, há uma diferença qualitativa importante entre o mundo físico e o espaço virtual: a estabilidade. E é exatamente esse fator que permite que uma abordagem ecológica como a da teoria da atividade rotineira realize correlações entre o espaço e o fenômeno criminal.[52] Como, porém, aplicar essa teoria num contexto volátil e facilmente transmutável como o do ciberespaço?

O outro pressuposto teórico analisado por Yar é a questão da temporalidade: para que a teoria criminológica seja aplicável, ela exige uma regular periodicidade da ocorrência dos eventos (*rhythm*) e uma coordenação de diferentes atividades (*timing*). Sem essa ordenação temporal, infratores não poderiam antecipar quando e onde alcançar suas vítimas (o crime resultaria sempre de eventos inesperados), e analistas não poderiam identificar situações criminogênicas. E isso é um problema no ciberespaço, onde, apesar de se possível identificar picos de atividade virtual, o tempo não pode ser

[49] *Ibid*., p. 416.
[50] *Ibid*., p. 416.
[51] *Ibid*., p. 416-417.
[52] *Ibid*., p. 417.

pensado em termos de atividades rotineiras. A internet permanentemente conecta todos os fusos horários, no chamado *24/7*.[53]

O *alvo apto*, para a teoria, é constituído por quatro propriedades: valor, inércia, visibilidade e acessibilidade. Primeiro, tal como os alvos dos crimes tradicionais, os alvos dos *cybercrimes* variam amplamente e atraem avaliações diferentes; são essas avaliações que impactam na aptidão do alvo, a partir da perspectiva subjetiva do pretenso infrator.[54]

No que toca à segunda propriedade, a teoria das atividades rotineiras dita que há uma relação inversa entre a inércia do alvo e a sua aptidão em se tornar objeto de crime: um objeto grande e pesado é difícil de ser subtraído; uma pessoa grande e pesada é difícil de ser atacada. No ciberespaço, porém, as propriedades físicas de volume e massa inexistem, excluindo assim qualquer análise de resistência do alvo. Ainda assim, argumenta Yar, mesmo os alvos virtuais conservam, em algum nível, a propriedade de inércia: o volume de informações (tamanho do arquivo) e especificações tecnológicas (configurações de sistema) impactam na portabilidade do alvo. Assim, "embora alvos informacionais ofereçam *relativamente* menos resistência inercial, sua leveza não é absoluta".[55]

Quanto à visibilidade, a teoria estabelece que a relação é direta: quanto mais visíveis as pessoas ou os objetos, maiores as chances de se tornarem alvos. Esse aspecto é de difícil mensuração para o contexto do ciberespaço, pois nele, em especial na internet, os entes são globalmente visíveis.[56]

Por fim, a propriedade da acessibilidade é compreendida pela teoria como a habilidade de um infrator alcançar o alvo e, posteriormente, poder deixar a cena do crime. Aqui também ocorre uma relação direta: quanto maior a acessibilidade, maior a aptidão do alvo. Daí, a conhecida conclusão dos criminólogos ecologistas de que uma casa situada em uma rua sem saída tem menor probabilidade de ser alvo de um crime do que uma residência próxima a diversos acessos para fuga. Tal análise de trajeto linear, porém, é imprópria para o ciberespaço. O único ponto em que convergem as realidades físicas e virtuais no que importa à acessibilidade é quanto aos mecanismos de segurança que evitam acesso não autorizado. Em ambos os contextos, há dispositivos que evitam a violação dos alvos (fechaduras, travas, senhas, exigências de autenticações) e

[53] *Ibid*., p. 418.
[54] *Ibid*., p. 419.
[55] *Ibid*., p. 420.
[56] *Ibid*., p. 420-421.

instrumentos para quebrá-los (chaves micha, pés-de-cabra, *crackers*, programas de decriptografia).[57]

Em suma: das quatro propriedades, somente a primeira (valor) pode ser tranquilamente transposta ao ciberespaço, e isso pode ser explicado pelo fato de que a avaliação não emana do ambiente físico ou virtual, mas de atribuições econômicas e simbólicas. As outras três propriedades (inércia, visibilidade e acessibilidade) apresentam profundas divergências quando analisadas em um ou outro contexto.

A existência de *protetores capazes* é a última variável da hipótese de causação de crime da teoria das atividades rotineiras. A proteção refere-se à capacidade de pessoas e objetos evitarem a ocorrência do crime, seja pela presença física de um impeditivo, seja sob forma de uma ação direta. E sua presença junto ao alvo apto, no momento em que o infrator motivado converge a ele, é um importante fator no exame criminogênico da situação. Yar argumenta que essa variável transita bem entre os mundos real e virtual: nos dois contextos, protetores oficiais (exemplo: a polícia) não estão ubiquamente presentes, prestando proteção geralmente de forma reativa ao evento criminoso; também nos dois contextos, são as proteções informais e privadas que exercem uma constante vigilância das situações, através de ações diretas ou dispositivos de segurança.[58]

A proposta da análise de Yar era a de examinar se e até que ponto etiologias do crime tradicional poderiam ser transpostas ao contexto do ciberespaço. Tendo focado exclusivamente na teoria da atividade rotineira, em razão de constantes referências de que essa abordagem era a mais apta para adaptar-se à realidade virtual, Yar encontrou ambas continuidade e descontinuidade na configuração de crimes tradicionais e virtuais. (A continuidade refutaria a novidade; a descontinuidade reclamaria uma nova criminologia.) A teoria da atividade rotineira, tal como outras teorias de causação criminal ecologicamente orientadas, conclui ele, "parece, então, de utilidade limitada em um ambiente que desafia muitas de nossas presunções dadas como certas sobre como é configurado o arranjo sócio-interacional das atividades rotineiras".[59] Havendo distinções de níveis e não de tipos, a demanda dos *cybercrimes* seria de uma adaptação conceitual, e não de uma rejeição de concepções tradicionais. Ou, como ele mesmo explica: talvez não seja o caso de um velho vinho em novas garrafas, mas sim de um

[57] *Ibid*., p. 421.
[58] *Ibid*., p. 422-423.
[59] *Ibid*., p. 424.

velho vinho sem garrafas ou um velho vinho em garrafas de formatos variáveis e fluidos.

Um ponto positivo dessas perspectivas tradicionalistas é que elas evidenciam uma sobrevalorização do meio cibernético. Como bem ressalta Lévy: gângsteres, terroristas, pedófilos e pornógrafos estão na internet, assim como estão em outros lugares; porém, apesar de eles também utilizarem aeronaves, rodovias e telefones, para obviamente expandirem seus campos de ação, ninguém pensou em identificar essas outras redes tecnológicas como ferramenta para criminosos.[60] O mesmo se diga sobre quem utiliza um telefone para ameaças (que responde pelo crime comum de ameaça) ou para fazer apostas (que vai enfrentar uma clássica contravenção), ou sobre aquele que subtrai um celular ou um automóvel (que vai responder por furto de objeto). Daí se infere que as categorias criminológicas convencionais seriam válidas ao ciberespaço e que parte do saber criminológico atual poderia ser transposta à realidade virtual ou aplicada às tecnologias de informação.

No entanto, enquanto cautelosas, essas perspectivas também são descuidadas por sua generalização, que torna todos os *cybercrimes* versões de crimes terrestres, ignorando a capacidade das tecnologias *cyber* de criarem crimes que não podem existir fora do ciberespaço.

1.2.2 Adaptacionistas (ou alternativos)

Sem argumentar por uma criminologia inteiramente nova, alguns autores reclamam uma adaptação da criminologia para justificar a análise de fenômenos emergentes que podem ou não atrair um rótulo criminal. Capeller[61], Brown[62] e Wall[63] defendem uma revisão de conceitos criminológicos e enquadramentos teóricos, e o desenvolvimento de um vocabulário criminológico correspondente e inovador[64], com fundamento na ideia de que o universo criminológico se tornou incapaz de explicar os novos desvios que provocaram demandas para a criação de novos (*cyber*)crimes.

---

[60] LÉVY, Pierre. *Cyberculture*. trad. Robert Bononno. Minneapolis: University of Minnesota Press, 2001. p. 185.
[61] CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", trad. Serena Barkham-Huxley, *Social & Legal Studies*, v. 10, n. 2, 2001, p. 229-242.
[62] BROWN, Sheila. "The criminology of hybrids: Rethinking crime and law in technosocial networks" *Theoretical Criminology*, v. 10, i. 2, 2006, p. 223-244; *Idem*. "Virtual Criminology", *op. cit.*
[63] WALL, David S. *Cybercrime*: the transformation of crime in the information age. Cambridge: Polity, 2007.
[64] YAR, Majid. "Online Crime", *op. cit.*

Central aos seus argumentos, há uma noção explícita ou implícita de descontinuidade com o velho e de emergência do novo.

Em 2001, Capeller defendeu a necessidade de uma revisão dos modelos criminológicos em prol de um paradigma que explique o movimento em direção ao imaterial e que acentue uma filosofia criminológica moderna para o século XXI.[65] Segundo ela, ocorreu uma mudança na compreensão do ciberespaço: visto antes como um meio ou suporte, o espaço virtual passou a ser entendido como um contexto no qual formas variadas de interação podem acontecer, um verdadeiro ambiente autônomo.[66] Assim, a criminologia tornou-se incapaz de explicar as novas formas de desvio que têm o potencial de serem legalmente definidas como *cybercrimes*.[67] Capeller, assim, utiliza explicitamente o critério da *(des)continuidade*: enquanto há uma *continuidade* das formas tradicionais de atividades criminosas, inclusive com uma crescente utilização do espaço virtual como suporte para elas, a emergência de uma nova fenomenologia criminal própria da tecnologia da informação estabelece uma *descontinuidade* com relação aos fenômenos tradicionais.[68]

Com uma diferente hipótese adaptativa – mas ainda implicitamente baseada na descontinuidade –, Brown defende uma criminologia de *híbridos* (humano e técnica) que se preocupe com o mapeamento de redes tecno-sociais[69], seus atuantes e seus agrupamentos.[70] A autora relata que a criminologia já se dedicou à tecno-socialidade, porém limitou-se a analisar a tecnologia como *tecnologia de controle social* (teorias que relacionam instrumentos com exclusão social) ou como *tecnologias sociais de controle* (teorias da governamentalidade), tratando "o técnico" como uma especialidade deixada de lado do cerne da criminologia e deixando inexploradas as implicações de suas interfaces – e, assim, valendo-se de, em vez de construindo, uma teoria geral.[71] Para ela,

---

[65] CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", *op. cit.*, p. 241.
[66] *Ibid*., p. 229, 234.
[67] *Ibid*., p. 230.
[68] *Ibid*., p. 230.
[69] O ambiente tecno-social é aquele criado pela intervenção tecnológica no qual passam a se desenvolver novas formas de relações sociais; essa tecno-socialidade caracteriza a combinação entre materialidade e imaterialidade, sujeito e objeto, senciência e insenciência, intencionalidade e automação, em redes de crime e controle (BROWN, Sheila. "The criminology of hybrids: Rethinking crime and law in technosocial networks", *op. cit.*, p. 227). A rede tecno-social se distingue do ciberespaço na medida em que este se refere exclusivamente às relações midiatizadas pelas tecnologias digitais.
[70] BROWN, Sheila. "The criminology of hybrids: Rethinking crime and law in technosocial networks", *op. cit.*
[71] *Ibid*., p. 225-227.

não é suficiente aplicar velhas leis para novas tecnologias, nem suscitar analogias simples entre "crime incorporado" e *cybercrime*.[72]

Em artigo mais recente, Brown denominou *criminologia virtual* uma variedade de trabalhos que emergiu desde meados de 1990, preocupados com as implicações de tecnoculturas contemporâneas na forma em que compreendemos crime, justiça, direito e controle social.[73] De acordo com a autora, a criminologia virtual contesta dois modos (incorporados) da criminologia tradicional: primeiro, o foco no corpo e na mente desviantes como sujeito e objeto do crime e do controle; segundo, a noção de que a tecnologia é um meio, um apêndice externo, uma mera ferramenta, no empreendimento criminoso ou no controle social.

De acordo com Brown, a criminologia virtual se justifica primeiramente pelo ineditismo de seu objeto: ela permite a absorção de comportamentos que não são necessariamente definidos como criminosos e de áreas que não são tradicionalmente consideradas pela criminologia consolidada como parte de seu domínio – precisamente porque são "virtuais". Vale lembrar que as formas de ordem, controle e desvio dentro dos ambientes virtuais não são necessariamente os mesmos daqueles do mundo real ou incorporado. As ciberculturas apresentam complexos padrões e novas formas de punição informal (as punições pela infração a regras, por exemplo, variam de sanções textuais à derrubada de servidores e bombeamentos de informações).

A criminologia virtual também se justifica pela adequação de um novo sujeito, colocando em primeiro plano a simulação e as relações desimcorporadas: "O que está em jogo teoricamente, na criminologia virtual", argumenta Brown, "é a noção da *interface* entre o humano e o *software/hardware*; o sensório humano se estende para dentro da virtualidade e torna co-constituintes o ser humano e a máquina".[74] Assim, enquanto a criminologia tradicional (e o direito tradicional) se assenta na presunção de que a conduta humana, as motivações, a culpabilidade são distintas das coisas (não humanas) e da tecnologia – presumindo que a própria essência humana seja autoevidente –, a criminologia virtual, indo além do senso comum voltado aos crimes que facilmente se traduzem do real ao *cyber* (furtos, fraudes, constrangimentos), estaria atenta à fusão do humano com o técnico: a dissolução do corpo em informação, identidades desincorporadas, consciência simulada etc.

---

[72] *Ibid*., p. 236.
[73] BROWN, Sheila. "Virtual Criminology", *op. cit.*
[74] *Ibidem*.

Representante da doutrina nacional, Albuquerque também apresenta uma distinção (adaptacionista) entre duas espécies de "crimes informáticos".[75] Para ele, nos *crimes informáticos comuns* (ou *traditional computer crimes*) os recursos informáticos são utilizados como meio-fim para o cometimento de crimes já previamente tipificados no direito penal vigente; por sua vez, os *crimes informáticos específicos* (*computer-specific crimes*) caracterizam-se pelas condutas que lesam um bem jurídico ainda não tutelado por norma jurídico-penal. Para os crimes dessa segunda espécie, mesmo que a conduta resulte em dano ou em perigo (de dano) a um bem jurídico (não identificado), ela é considerada atípica por falta de previsão legal. A indicação de seu argumento se justifica pela evidência que coloca a novas expressões criminosas que demandam uma nova resposta jurídica, enquanto insuficientes as já existentes. No entanto, sua divisão possui uma fundamentação dogmática, tendo como referencial a tipificação legal como chancela para a imputação penal ao responsável pelo crime.

Wall, por sua vez, oferece oportunidade para uma análise mais matizada, ao desenvolver uma abordagem geracional para as questões referentes ao potencial das criminologias existentes em mediar os desafios e significados – histórica e culturalmente cambiantes – das atividades *cyber*.[76] Ao categorizar os *cybercrimes* por gerações, ele argumenta que diferentes desenvolvimentos tecnológicos demandam diferentes explicações criminológicas. Essa noção de transformação lhe permite (i) oferecer um aspecto geral e reconciliatório de tipos de *cybercrimes* aparentemente distintos ao categorizá-los em diferentes fases de um processo de mudança, e (ii) compreender que as mesmas tecnologias que criam os *cybercrimes* também fornecem a oportunidade para sua regulação e seu controle.[77]

Afastando a compreensão dos *cybercrimes* como uma ideia imutável, Wall identifica, no seu desenvolvimento fenomenológico, variações de sentido que podem ser categorizados cronologicamente como gerações distintas de crimes. Wall justifica sua opção por dispor os *cybercrimes* num enquadramento de tempo, ao invés de organizá-los conforme argumento de espaço, porque assim se evidencia como sucessivas gerações foram definidas por diferentes estágios de desenvolvimento tecnológico.[78] São elas:

---

[75] ALBUQUERQUE, Roberto Chacon. *Criminalidade informática*. São Paulo: Juarez de Oliveira, 2006. p. 39-41.
[76] WALL, David S. *Cybercrime*: the transformation of crime in the information age, *op. cit.*
[77] *Ibid*., p. 4.
[78] *Ibid*., p. 48.

- Na primeira geração, os *cybercrimes* aconteciam (e acontecem) em sistemas de computação distintos e se caracterizaram pela exploração criminosa de computadores *mainframes* e de seus sistemas operacionais. Trata-se de crimes *tradicionais* (Wall) ou *ordinários* (McQuade) nos quais os computadores são utilizados no estágio preparatório do crime, como uma ferramenta de comunicação, para obter informações preparatórias, enfim, para assistir violações tradicionais. Nos crimes dessa primeira geração, a extração da tecnologia da equação criminosa não evita a execução criminosa, que pode ocorrer por outros meios.[79] Pense-se no caso de criminosos que se comunicam por e-mail (o que poderia ser feito por outros meios) ou que fazem uso do Google Maps para planejar uma rota de fuga (o que pode ser traçado em mapas impressos).

- Os *cybercrimes* de segunda geração, por sua vez, são aqueles cometidos através de redes, tendo sido originalmente caracterizados como *hacking* e *cracking*. São crimes *híbridos* (Wall) ou *adaptativos* (McQuade), também passíveis de serem descritos como crimes tradicionais para os quais surgiram novas oportunidades globalizadas. Extraída a internet da equação, o comportamento infrator permanece; todavia, as novas oportunidades de infrações desaparecem e o comportamento se realiza por outros meios, em menores número e escala.[80] A título ilustrativo, tome-se o caso de fraudadores que aplicam golpes por meio da internet (o que potencializa sua atividade criminosa) ou de *haters* que propagam discursos de ódio em redes sociais (o que amplia sua audiência e o potencial número de vítimas).

- A terceira geração de *cybercrimes* foi introduzida na virada do século, com a substituição do *modem* de discagem pela banda larga, e compreende os *cybercrimes* próprios, de natureza distribuída e automatizada, quase totalmente mediados por tecnologia. Os *cybercrimes* dessa geração são literalmente *sui generis*: são produtos das oportunidades criadas pela internet e somente podem ser perpetrados dentro do ciberespaço; excluída a tecnologia que os possibilitou

[79] *Ibid*., p. 44-45.
[80] *Ibid*., p. 45-47.

> acontecer, o crime, impossível de existir como atividade, desaparece.[81] A disseminação de *malwares* e a derrubada de servidores são claros exemplos de condutas que emergiram a partir, e só podem ser executadas por meio, da internet.[82]

Tomando como pressuposto que a característica definidora do *cybercrime* é a sua mediação por tecnologias em rede, Wall propõe o *teste da transformação*, que consiste em questionar o que resta, no todo que chamamos de *cybercrimes*, se aquelas mesmas tecnologias em rede forem retiradas da equação. O teste, diz ele, não pretende ser científico; em vez disso, trata-se de um instrumento heurístico, uma regra geral (*rule of thumb*).[83]

Enquanto os *cybercrimes* tradicionais utilizam a tecnologia de informação como meio para a preparação de crimes e os *cybercrimes* híbridos utilizam-na para execução de crimes, também há crimes totalmente mediados pela tecnologia, produtos das oportunidades criadas pela internet e somente passíveis de serem perpetrados dentro do ciberespaço (os *cybercrimes* próprios). Nesse sentido, enquanto os *cybercrimes* de primeira e segunda geração podem se satisfazer com a aplicação das categorias criminológicas convencionais, os *cybercrimes* de terceira geração demandam o desenvolvimento de novas abordagens teóricas, nas quais a técnica seja compreendida como sujeito do fenômeno criminal.

No mesmo sentido, mais recentemente, Yar defendeu que a criminologia precisa começar a procurar algumas "novas ferramentas" para esses "novos crimes"[84], ao passo que Jaishankar defende o desenvolvimento e a independência da cibercriminologia, mas ele a pensa mais como disciplina acadêmica autônoma do que como uma nova perspectiva criminológica.[85]

Como já referido anteriormente, Jaishankar revela a preocupação de elaborar uma nova e independente disciplina acadêmica, que se concentre na causação dos *cybercrimes* a partir da perspectiva das ciências sociais, separando-se, portanto, da

---

[81] *Ibid*., p. 47-48.
[82] Wall faz prognósticos referentes a uma possível quarta geração de *cybercrimes*, os quais emergirão de oportunidades criminosas pelas *tecnologias ambientes*, mas ele não explica sua natureza e seus modelos. (*Ibid*., p. 48)
[83] *Ibid*., p. 34.
[84] YAR, Majid. *Cybercrime and society*. 2. ed. London: SAGE, 2013.
[85] JAISHANKAR, K. "Cyber Criminology: Evolving a novel discipline with a new journal", *op. cit.*; *Idem*. "The Future of Cyber Criminology: Challenges and Opportunities", *op. cit.*

ciência da *cyber-forensics*, a qual lida exclusivamente com a investigação criminal.[86] Ele justifica essa demanda ao apontar que, quando programas de criminologia oferecem curso/disciplina em *cybercrimes*, eles geralmente focam em questões criminais forenses e na prática investigativa (quando tecnólogos[87] ensinam), e, com menor interesse, nos aspectos teóricos do crime (quando criminólogos tradicionais o fazem) ou na legislação *cyber* (quando eles são advogados), negligenciando os fundamentos criminológicos e o conhecimento da tecnologia de informação e da internet, assim resultando num prejuízo à compreensão holística do fenômeno.[88]

Assim, Jaishankar define a cibercriminologia como "o estudo de causação de crimes que ocorrem no ciberespaço e seu impacto no espaço físico".[89] O seu estudo é pautado por uma teoria, por ele mesmo desenvolvida, chamada de *teoria da transição de espaço*. A teoria é uma explicação sobre a natureza do comportamento das pessoas que apresentam condutas conformes e não conformes no espaço físico e no ciberespaço, e argumenta que as pessoas comportam-se diferentemente quando se movem de um a outro espaço – isto é, do físico ao *cyber* e vice-versa.[90] Os postulados da teoria são os seguintes:

> 1. Pessoas com comportamento criminal reprimido (no espaço físico) têm uma propensão a cometer crime no ciberespaço, o qual, ao contrário, eles não cometeriam do espaço físico, em razão de seus status e posição.
>
> 2. Fatores de flexibilidade de identidade, de anonimato dissociativo e de falta de dissuasão no ciberespaço proporcionam ao infrator a escolha de cometer o *cybercrime*.

---

[86] *Idem*. "The Future of Cyber Criminology: Challenges and Opportunities", *op. cit.*
[87] No original, *technocrats* (*Ibid*., p. 27). Optou-se por *tecnólogos* porque a palavra inglesa original não comporta imediantamente o mesmo sentido negativo que a sua tradução.
[88] Duas observações: (i) quando faz referência aos cursos/disciplinas existentes, Jaishankar limita sua análise aos programas de criminologia de universidades dos Estados Unidos e do Reino Unido; (ii) o próprio Jaishankar reconhece o grande desafio das instituições de ensino em desenvolver programas com abordagens mais multi e interdisciplinares em razão da dificuldade em encontrar docentes e pesquisadores com formação mais holística.
[89] JAISHANKAR, K. "Cyber Criminology: Evolving a novel discipline with a new journal", *op. cit.*, p. 1.
[90] *Idem*. "Establishing a Theory of Cyber Crimes", *op. cit.*

> 3. O comportamento criminoso de delinquentes no ciberespaço é capaz de ser importado para o espaço físico, assim como, no espaço físico, pode ser exportado para o ciberespaço.
>
> 4. Intermitentes ações arriscadas de delinquentes no ciberespaço e a natureza espaço-temporal dinâmica do ciberespaço propiciam a oportunidade de escapar.
>
> 5. (a) Estranhos tendem a se unir no ciberespaço para cometer crimes no espaço físico. (b) Associados no espaço físico tendem a se unir para cometer crimes no ciberespaço.
>
> 6. Indivíduos de sociedade fechada são mais suscetíveis de cometerem crimes no ciberespaço do que pessoas de sociedade aberta.
>
> 7. O conflito de normas e valores do espaço físico com as normas e os valores do ciberespaço pode levar a *cybercrimes*.

A teoria pretende suprir a deficiência do estudo criminológico diante da emergência do ciberespaço como um novo *locus* de atividade criminal. No entanto, como o próprio proponente afirmou quando apresentou esses postulados[91], ainda é necessário testá-la para verificar se a teoria de transição de espaço explica a atividade criminal *cyber*.

[91] *Ibidem*.

1.3 PRESSUPOSTOS DAS CRIMINOLOGIAS *CYBER*

> Deveríamos nos agarrar nos procedimentos e modelos que nos deram as velhas ordens de conhecimento? Ou deveríamos, em vez disso, saltarmos adiante e mergulhar de cabeça na nova cultura, a qual nos oferece remédios específicos para os males que ela engendra?[92]

A terceira questão inicial indaga, então, quais são os pressupostos fáticos e filosóficos que informam as reflexões aqui apresentadas e que permitem uma nova proposição de definição e critérios criminológicos?

1.3.1 Pressupostos fáticos

Recentes trabalhos[93] têm reconhecido que a criminologia tem sido desafiada pelas grandes transformações de nosso tempo. – Em verdade, desde o seu surgimento no mundo urbanizado e industrializado de meados do século XIX, a criminologia foi, ou procurou ser, um estudo contemporâneo, tempestivo e mundano.[94] – Isso fica evidente para quem olha, além da realidade imediata do crime, em direção aos processos que dão forma à experiência social: as mudanças seculares na estrutura familiar, nas relações interpessoais, na ecologia espacial das cidades, nas rotinas da vida social e do controle social; a globalização, a dinâmica transformativa da produção e da troca capitalistas, a emergência do consumo em massa, a reestruturação do mercado de trabalho; a democratização da vida social e cultural, a dessubordinação dos grupos minoritários e menos favorecidos, o impacto social da mídia de massa, a disseminação dos anseios e dos medos, as novidades da forma de governo e do discurso político – esses e muitos outros fatores possíveis implicam a criminologia em uma demanda adaptativa, que constantemente exige crescente velocidade, especialização e profundidade, para compreender o fenômeno criminal e responder à prática dos índices criminais, da política criminal, da prevenção, do controle e da punição.

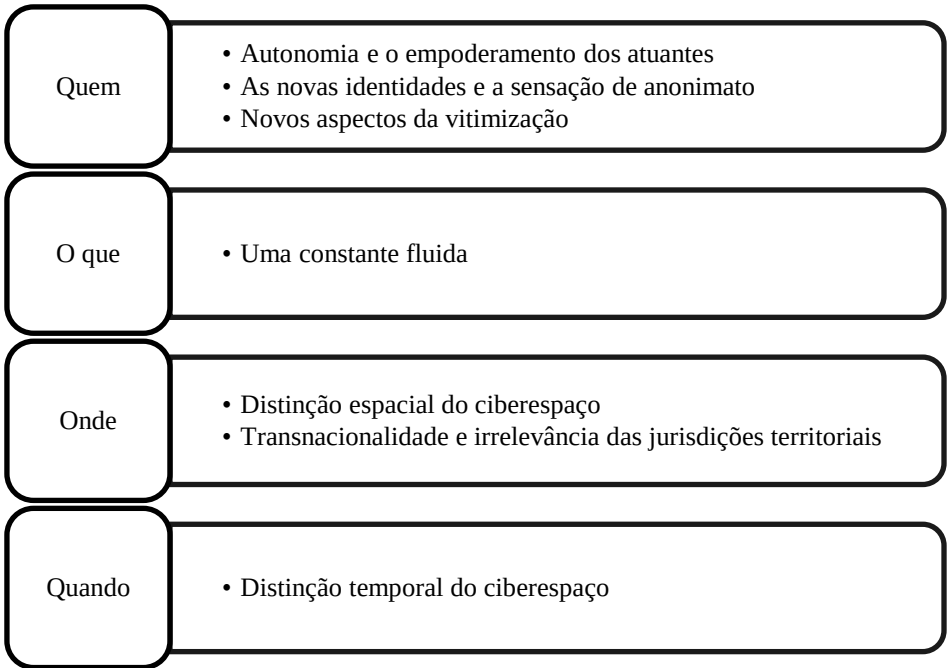
---

[92] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 147.

[93] Por todos: GARLAND, David; SPARKS, Richard. "Criminology, Social Theory and the Challenge of our Times", *The British Journal of Criminology*, v. 40, n. 2, 2000, p. 189-204; ZEDNER, Lucia. "Pre-crime and post-criminology?", *op. cit.*

[94] Essa passagem faz referência à emergência da criminologia moderna e não pretende sugerir que a criminologia – abstrata e falsamente representada no singular – tenha nascido nesse período. Existiram produções criminológicas anteriores, mas muitas delas não invocaram o rótulo da "criminologia", como é o caso dos textos demonológicos e os manuais inquisitoriais.

Esta tese assume o pressuposto de que o desenvolvimento de um ambiente social novo e distinto, o ciberespaço, com suas próprias estruturas ontológica e epistemológica, formas de interação, funções e possibilidades, oportunizou a emergência de fenomenologias criminais inéditas[95], que podem justificar o neologismo "criminologias *cyber*". Algumas novidades fenomenológicas ilustram bem esse argumento:



1.3.1.1 Prêambulo necessário sobre o espaço e o tempo

No que segue, discutirei transformações na percepção do espaço e do tempo, provocadas pela tecnologia da informação. É preciso esclarecer, contudo, que noções são essas que tínhamos e que – como tradição, inércia ou vestígio – ainda temos, justificando a nossa vertigem diante da velocidade cibernética.

Espaço e tempo são categorias básicas da existência humana. O espaço é tratado tipicamente como um atributo objetivo das coisas, que pode ser medido: o espaço tem área, forma, volume e distância. Mas, as percepções e as experiências espaciais variam entre grupos sociais: muitas criminologias já revelaram que migrantes, marginalizados, mulheres e apenados não dispõem do mesmo espaço que indivíduos privilegiados, portadores de um passaporte que lhes permite um trânsito muito mais amplo.

[95] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*

De modo semelhante, registramos a passagem do tempo – já pressupondo que ele passa – numa escala temporal objetiva. Se o tempo é um conceito difícil para a física, sendo constante objeto de contendas, se sua "relatividade" prega peças aos nossos processos e percepções mentais, se até mesmo reconhecemos o fato de que diferentes grupos sociais cultivem sentidos de tempo muito distintos, tudo isso não costuma afetar o seu sentido comum, em torno do qual organizamos nossas rotinas diárias (talvez a ideia de movimento cíclico ofereça uma sensação de segurança num contexto que parece de constante aceleração).[96]

Fato é que raramente discutimos seus sentidos. Tomamo-los por certos, num significado amplo e objetivo que todos aceitam como comum e geral. Por isso, pode-se dizer que lhos damos, ao espaço e ao tempo, atribuições do senso-comum. Partindo de uma perspectiva materialista, Harvey afirma que "as concepções do tempo e do espaço são criadas necessariamente através de práticas e processos materiais que servem à reprodução da vida social".[97] Disso decorre que, se as práticas materiais de reprodução social variam geográfica e historicamente, cada modo de formação social incorpora um agregado particular de práticas e conceitos do espaço e do tempo, o que explica por que o espaço social e o tempo social são construídos de maneiras tão diferentes.

No fim do século passado, Virilio já havia se incomodado com as transformações do espaço e do tempo:

> Se, de facto, a esfera de actividade do homem já não é limitada pela extensão, pela duração, pela própria opacidade dos obstáculos que lhe barram o caminho, onde se situa então a sua presença no mundo, a sua presença real? Tele-presente, sim, mas onde? A partir de que lugar, de que posição? Presente-vivo, ao mesmo tempo aqui e ali: *onde estou eu, se estou em toda a parte?*[98]

Virilio prefere descrever o ciberespaço como atópico, sem território, um não-lugar – atopia que vai se refletir no corpo social e no corpo humano.[99] E seus argumentos revelam que, preso à noção tradicional do espaço, o famoso dromólogo sente-se perdido na ausência de referências de localização:

---

[96] HARVEY, David. *Condição pós-moderna*: uma pesquisa sobre as origens da mudança cultural. trad. Adail Ubirajara Sobral e Maria Stela Gonçalves. 25. ed. São Paulo: Edições Loyola, 2014. p. 187-189.
[97] *Ibid*., p. 189.
[98] VIRILIO, Paul. *A inércia polar*. trad. Ana Luía Faria. Lisboa: Publicações Dom Quixote, 1993. p. 124, grifos no original.
[99] *Idem*. "Da política do pior ao melhor das utopias e à globalização do terror", *FAMECOS*, n. 16, dez. 2001. p. 7.

> Uma última constatação: se a mundialização rápida das trocas implica, como se viu, a virtualização das diversas representações estratégicas, econômicas científicas, um problema notável se coloca: o da *localização física precisa do objeto virtual*.
> Efetivamente, com a confusão que se instala a partir de então entre *o espaço real* da ação e *o espaço virtual* da retroação, todo *posicionamento* começa a cair num impasse e ocorre portanto a crise de toda previsão de posição...[100]

O que se verá a seguir revoluciona absolutamente as noções tradicionais de espaço e tempo, e, por consequência, nossas referências corológica e cronológica. Essas revoluções podem ser desestabilizantes, mas não são necessariamente tão assustadoras. O apocalíptico é mais catástrofe na adjetivação do que em essência.

1.3.1.2 A distinção espacial do ciberespaço

O ciberespaço desafia limites espaciais físicos, tornando a geografia irrelevante[101] diante de uma experiência de equidistância[102]. Ainda que sejam identificáveis constantes referências espaciais do mundo físico – navegação, sítios, portais, salas de bate-papo, envio e recebimentos de mensagens –, as expressões revelam-se como metáforas convenientes que nos auxiliam a contextualizar um ambiente que é inerentemente distinto do mundo físico.[103] São meros recursos linguísticos. Por exemplo: apesar de recorrermos à mesma palavra *página* para indicar o plano no qual se inscrevem informações, a página física, como a folha de papel, é um campo limitado no qual se fixa o conteúdo (o antepositivo latino *pag-* indica fixação: paz, pacto, pago, pagão), enquanto a página virtual é uma unidade de fluxo, sujeita somente às limitações da conexão de rede.[104] Uma decisão da Corte Distrital do Southern District of New York (S.D.N.Y.), no caso *American Library Association v. Pataki (969)*, evidenciou a mesma confusão com relação à ideia de "endereço". Em 23 junho 1997, a juíza Loretta A. Preska assim fundamentou sua decisão:

---

[100] *Idem*. *A arte do motor*. trad. Paulo Roberto Pires. São Paulo: Estação Liberdade, 1996. p. 133.
[101] JAISHANKAR, K. "The Future of Cyber Criminology: Challenges and Opportunities", *op. cit.*; LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 31.
[102] WALL, David S. *Cybercrime*: the transformation of crime in the information age, *op. cit.*, p. 37.
[103] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*
[104] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 139. O recurso metafórico à página de papel é antigo; em *Computer Machinery and Intelligence*, Turing já escrevera: "O computador [digital] inclui uma memória correspondente ao papel usado por um computador humano. Deve ser possível escrever na memória qualquer uma das combinações de símbolos que poderiam ter sido escritas no papel." (TURING, Alan Mathison. "Computing Machinery and Intelligence", *Mind*, v. LIX, n. 236, 1950, p. 441.)

> A internet é completamente indiferente a distinções geográficas. Em quase todos os casos, os usuários da internet não sabem nem se importam com a localização física dos recursos da internet que eles acessam. Os protocolos da internet foram projetados para ignorar, em vez de documentar, a localização geográfica; embora computadores na rede tenham "endereços", eles são endereços lógicos na rede, em vez de endereços geográficos no espaço real. A maioria dos endereços da internet não contém indicações geográficas e, mesmo onde um endereço da internet forneça uma tal indicação, ela pode ser enganosa.[105]

De fato, os endereços de IP referem-se a locais lógicos na rede; são endereços virtuais. Eles não se referem a um particular lugar geográfico. "Assim," afirma Lessig, "dois endereços IPs, em princípio, poderiam ser muito próximos um do outro em número, mas muito distantes um do outro em geografia. Não é assim que funciona, por exemplo, o código postal".[106] Embora os protocolos de comunicação entre computadores em rede (TCP/IP: *Transmission Control Protocol/Internet Protocol*) não possam revelar diretamente onde um atuante se encontra no espaço real, eles podem ser utilizados para revelar ao menos a origem ou o destino de um pacote de dados.

Inspirado pelas ideias de Manuel Castells, Yar contesta essa impressão de desconectividade do ciberespaço das restrições socioculturais.[107] Para Yar, embora o ciberespaço seja diferente do mundo material, aquele é um ambiente interacional sócio-tecnicamente gerado e enraizado no mundo real das relações políticas, econômicas, sociais e culturais. Assim, o ciberespaço traduz ou reproduz características do mundo real ao espaço virtual. Yar também contesta a ideia de equidistância no ciberespaço: a distância, para ele, existe e é medida pelo dispêndio de tempo e esforços para alcançar determinado conteúdo, num cálculo que deveria se pautar, por exemplo, pelo número de cliques.

O ciberespaço é um desafio especial porque parte significativa da tradição das perspectivas criminológicas fundamenta-se, implícita ou explicitamente, em teorias ecológicas – as quais relacionaram a ocorrência dos crimes, seus padrões e distribuições, com a configuração sócio-espacial de lugares específicos, e que possibilitaram respostas como mapeamento, identificação de ambientes criminogênicos, programas de prevenção.[108]

---

[105] *Apud* GEIST, Michael. "Cyberlaw 2.0", *Boston College Law Review*, n. 323, 2003. p. 327.
[106] LESSIG, Lawrence. *Code*: version 2.0. New York: Basic Book, 2006. p. 58.
[107] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*
[108] *Idem*. *Cybercrime and society*, *op. cit.*, p. 17.

Ainda que não seja minha intenção aprofundar neste tópico para o momento, é importante já sinalizar que, apesar de ser um ambiente diferente do mundo físico, o ciberespaço possui um fundamento comum (porém, peculiar) com este: a arquitetura. Ao identificar propriedades políticas na experiência tecnológica do ciberespaço, Lessig informa que há uma arquitetura própria do ciberespaço: o *código*, isto é, o conjunto de protocolos e de regras codificadas e implementadas que determinam como as pessoas interagem (ou, existem) nesse espaço.[109] Tal como uma estrutura arquitetônica sujeita o comportamento humano (e inspira a análise ecológica), o código estrutura e condiciona comportamentos, estabelece restrições e permissões – o que nos permite já vislumbrar uma cibercriminologia ecológica.

É preciso destacar, no entanto, que algumas legislações resolvem a irrelevância geográfica do ciberespaço com uma previsão de alcance extraterritorial de suas normas internas. O PATRIOT Act[110], implementado logo após os ataques terroristas às torres gêmeas do World Trade Center alterou o Computer Fraud and Abuse Act, estendendo a possibilidade de o governo estadunidense processar criminalmente ações de hacking e DDoS ao expandir a definição de "computadores protegidos" como também "um computador localizado fora dos Estados Unidos que seja utilizado de um modo que afete o comércio ou a comunicação interestadual ou internacional dos Estados Unidos" (18 U.S. Code § 1030, (e) (2) (B)), sem qualquer menção à possibilidade de que a conduta praticada não seja considerada ilícita no país dos atuantes (ou seja, sem exigência de uma dupla incriminação). O mesmo tratamento foi identificado nas legislações de Singapura e Malásia; no mesmo sentido, uma legislação promulgada na Austrália, em 2001, pretende regular sites de jogos de azar fora de suas jurisdição.[111] É obviamente questionável a capacidade desses países em aplicar esses específicos estatutos contra atuantes e provedores no exterior.

Mas, enquanto o ciberespaço despreza limitações geográficas, o mesmo não pode ser dito com relação às comunicações feitas por meio da internet (e aqui se evidencia como *ciberespaço* e *internet* são distintos). Nos recentes anos, tem se verificado que diversos serviços fazem uso de ferramentas que permitem a identificação geográfica dos atuantes de forma bastante eficaz – porém, imperfeita –, possibilitando

---

[109] LESSIG, Lawrence. *The laws of cyberspace*: draft 3. In: Taiwan Net '98, 1998, Taipei.
[110] USA PATRIOT Act é a abreviação de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*.
[111] GEIST, Michael. "Cyberlaw 2.0", *op. cit.*, p. 345-347.

ou não que se tenha, por exemplo, acesso a determinados conteúdos.[112] O Google é uma ferramenta de pesquisa global, mas alguém que acesse o serviço de dentro do território chinês terá seu resultado de busca restringido pelo que é autorizado pelo governo chinês (limitação que foi condição para que a empresa operasse no país e com a qual ela concordou). Do mesmo modo, questões regionais referentes à licitude material ou aos direitos autorais (e direitos de distribuição) também podem impactar no acesso – basta que se verifique como serviços de *streaming* audiovisuais (Youtube, Netflix) podem oferecer programações distintas para diferentes países ou como sites de conteúdo mais rigorosamente controlado (sites de jogos ou pornôs) não são acessíveis ao público comum de determinados países que os consideram ilícitos. Nas palavras de Geist:

> Embora muitos usuários da internet de fato experimentem uma internet "sem fronteiras", enquanto visitam, sem esforço, *sites* em todo o mundo ao clique do *mouse*, os próprios usuários não são sem fronteiras. Eles estão localizados em locais físicos que, com uma crescente frequência, podem ser identificados pelos *websites* que visitam.[113]

Ao filtrar conteúdos e, assim, alterar a experiência dos usuários com base nas suas origens geográficas, essas novas regulamentações codificadas iniciam um processo de fronteirização da internet. Novamente: enquanto o ciberespaço pode ser considerado um ambiente comum, a internet mostra-se, cada vez mais, um meio delimitado por jurisdições geográficas definidas por demandas políticas e/ou comerciais.

1.3.1.3 A distinção temporal do ciberespaço

O tempo também foi deformado no ciberespaço. Ao menos, se tomarmos como pressuposto a compreensão mais comum do tempo como um fluxo quantificável de eventos, que implica numa dinâmica que varia entre a expectativa (futuro), o acontecimento (presente) e a perda (passado). Diversos autores[114] já haviam relatado que a estrada de ferro, o automóvel e o avião a jato, a imprensa, a telegrafia, o rádio e a televisão já haviam acelerado consecutivamente o ritmo de uma cultura anterior,

---

[112] GEIST, Michael. "Cyberlaw 2.0", *op. cit.*, p. 332.
[113] *Ibid*., p. 335.
[114] Por todos: KERCKHOVE, Derrick de. *A pele da cultura*: uma investigação sobre a nova realidade eletrónica. trad. Luís Soares e Catarina Carvalho. Lisboa: Relógio D'Água Editores, 1997. p. 103; HARVEY, David. *Condição pós-moderna, op. cit.*, p. 212.

removendo as barreiras espaciais. O dromólogo Virilio, teórico da velocidade, preocupava-se com essa aceleração:

> Ocorre que a rapidez das novas tecnologias esmaga as distâncias tradicionais. A compressão temporal é uma poluição das grandes dimensões naturais. Trata-se de um fechamento que, em breve, tornará insuportável a convivência entre os seres. Não haverá mais espaço físico nem temporal separando as pessoas. A cibernética e as viagens supersônicas comprimem o mundo como numa prisão cujas paredes se movessem diminuindo o espaço existente.[115]

Não foi diferente com a internet. A experiência da comunicação à velocidade da luz proporciona a sensação de um imediatismo que embaraça o entendimento naturalmente acostumado a uma sequência derivada de ações físicas. Qual o intervalo, no ciberespaço, entre o momento de ação e a produção do resultado?

(Mesmo que os momentos de ação e produção de resultado sejam distintos e identificáveis, haveria ainda problemas na responsabilização criminal, em razão de adotarmos um sistema baseado na ação do indivíduo na realidade física. Moreira de Oliveira[116] apresenta uma intrigante provocação: imagine a introdução num sistema de computadores de uma *logic bomb* programada para iniciar sua atividade a partir de uma data específica, quando já estiver extinta a punibilidade do agente, ou de um *worm* disparado e espalhado por diversos computadores que venha aleatoriamente a encontrar uma vulnerabilidade somente após muitos anos de circulação e contágio, quando, então, causará o dano esperado, num momento em que o crime já estaria prescrito. Um recurso dogmático pode ser a atribuição de permanência ao crime ao longo do período em que o *malware* estiver instalado; mas sua inatividade e a ausência de lesividade, ao longo desse tempo, podem tornar inadequada a solução dogmática. Esse descompasso na imputação de responsabilidade é já indicativo de que os *cybercrimes* próprios demandam novos modelos criminológicos de atuantes, condutas e controle.)

Os horizontes temporais – escreveu Harvey[117], tratando do efeito do capitalismo – se reduzem a um ponto em que só existe o presente. Mas, este presente é um presente leve, instantâneo, volátil. Seja no domínio das ideias, dos processos e das relações sociais, ou da produção de mercadorias, as pessoas passaram a experimentar um presente imediato, manifesto na instantaneidade e na descartabilidade das opiniões, das

[115] VIRILIO, Paul. "Da política do pior ao melhor das utopias e à globalização do terror", *op. cit.*, p. 14.
[116] MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*, *op. cit.*, p. 132.
[117] HARVEY, David. *Condição pós-moderna*, *op. cit.*, p. 219.

relações laborais e afetivas, dos produtos e dos alimentos. Toda novidade já nasce obsoleta. A permanência perde espaço na compressão temporal.[118]

Além disso, a compressão temporal oferece um outro fenômeno: a aniquilação do passado (perda) pela permanente rememoração – esse sim, agora, insistente e pesado. Se o esquecimento sempre foi a consequência natural do tempo, desafiada pelos registros históricos das narrativas da escrita e das representações – ao que denominamos memória ou lembrança –, as técnicas de armazenamento e recuperação de informações digitais possibilitam hoje que o passado esteja presente, que o acontecido esteja ao alcance imediato, que a rememoração seja absoluta (sobre todos) e permanente (disponível) – a tal ponto que o esquecimento tenha sido recentemente elevado a um direito de se ter informações pessoais deletadas de registros e bancos de dados, já reclamado em tribunais pelo mundo.[119]

1.3.1.4 A autonomia e o empoderamento dos atuantes

Aparentemente livre do controle de governos ou de corporações, o usuário da internet experimenta maior autonomia. Kerckhove já havia feito um prognóstico muito certeiro:

> A mudança do controlo do produtor/emissor para o consumidor/utilizador transformará uma minoria de utilizadores nos seus próprios produtores, ou "prosumidores". A descentralização das emissões será acompanhada pela descentralização das tecnologias produtivas. A queda dos preços dos equipamentos de vídeo e dos computadores está a ser acompanhada por um aumento da qualidade e da *performance*. Hoje é possível fazer um melhor trabalho e mais rápido com um câmara semiprofissional de HI-8 ou com um editor de vídeo assistido por computador e uma simples mesa de mistura de som, do que era, há uns anos atrás, com enormes estúdios de edição vídeo. A tecnologia de transmissão, estimulada pelas redes celulares, vai contribuir para colocar o poder da difusão nas mãos dos indivíduos, em áreas cada vez maiores.[120]

---

[118] E se as teses de doutorado ainda existem, ou persistem, com a sua exigência de anos para elaboração, é porque o mercado acadêmico tornou o título um requisito importante e privilegiado de avaliação do ensino superior. O doutoramento vai perder sentido quando deixar de ser medida de importância nessa concorrência classificatória e, então inadequado, vai ceder espaço para algo mais breve, simplificado, quiçá esquematizado.

[119] SOUZA, Bernardo de Azevedo e. *Direito, tecnologia e práticas punitivas*. Porto Alegre: Canal Ciências Criminais, 2016; ver ainda HAYWARD, Keith. "Five Spaces of Cultural Criminology", *The British Journal of Criminology*, v. 52, n. 3, 2012, p. 457.

[120] KERCKHOVE, Derrick de. *A pele da cultura*, *op. cit.*, p. 95-96, grifo no original.

Nesse mesmo sentido, Lévy argumenta que o ciberespaço quebra com a ideia de *sociedade do espetáculo*, denunciada pelos situacionistas como o contexto em que as relações interpessoais são cristalizadas pela mídia, a qual se caracteriza por nós centralizados que distribuem mensagens para receptores isolados e inabilitados para responder.[121] Lessig descreve essa revolução da comunicação como uma transformação de arquiteturas de publicação um-para-muitos (mídia de massa) para um novo contexto onde todos publicam.[122] No ciberespaço, a comunicação é inerentemente livre da intervenção compulsória da mídia, porque ele é comum, não hierárquico e recíproco.[123] A internet, prossegue Lévy, é "anarquista" – não *apesar de* sua origem militar, mas *por causa* dela (a estrutura dispersa da rede foi projetada para resistir a eventuais ataques inimigos).[124]

No âmbito das manifestações criminosas, o empoderamento individual proporcionado pela internet gera um maior controle da execução criminal pelo indivíduo atuante. Esse empoderamento decorre da capacidade da tecnologia em ser multiplicadora de força, possibilitando que indivíduos com recursos mínimos gerem potencialmente enormes efeitos negativos.[125] Um único *spammer*, por exemplo, pode alcançar milhões de destinatários. Já se estimou que mais de 80% dos *spams* globais foram originados por menos de duas centenas de conhecidos *spammers* nos Estados Unidos.[126]

Esse empoderamento, no entanto, não se refere unicamente à potencialidade de danos; ele pode se referir também a um empoderamento meramente simbólico. "É claro que a internet empodera pequenos grupos e faz com que eles pareçam muito mais capazes do que eles podem ser de verdade, até tornando uma bravata num tipo de medo virtual".[127] O grupo terrorista ISIS, por exemplo, representa uma grande ameaça mundial, mas isso decorre da habilidade de seus integrantes em utilizar a internet para

---

[121] LÉVY, Pierre. *Cyberculture*, *op. cit.*
[122] LESSIG, Lawrence. *Code*: version 2.0, *op. cit.*, p. 2.
[123] LÉVY, Pierre. *Cyberculture*, *op. cit.*
[124] *Ibid*., p. 208.
[125] WALL, David S. *Cybercrime*, *op. cit.*, p. 39-40; YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*; YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 11
[126] Ver WALL, David S. *Cybercrime*, *op. cit.*, p. 145; ver ainda n. 432 desta tese.
[127] THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, v. 23, i. 1, 2003, p. 115-116.

propagar seus crimes, em estilo cinematográfico. Na realidade, o grupo Boko Haram é responsável por um número muito maior de mortes.[128]

1.3.1.5 As novas identidades e a sensação de anonimato

Reconhece-se que no mundo contemporâneo a identidade tornou-se volátil. Ao analisar a questão da identidade, Lévy escreveu que:

> Nós não nos apegamos mais a um trabalho do que a uma nação ou uma identidade qualquer. Mudamos de regime alimentar, de trabalho, de religião. Saltamos de uma existência a outra, inventamos continuamente nossa atividade e nossa vida. Somos instáveis tanto em nossa vida familiar como em nossa vida profissional. Nós nos casamos com pessoas de outras culturas e de outros cultos. Não somos infiéis, somos móveis.[129]

Suas observações são perspicazes. Ao tratar das novas identidades aqui, porém, a análise repousará nas muitas potenciais declinações identitárias de um indivíduo atuante no ciberespaço, destacando a ainda maior fluidez de modelos com relação a um mundo já bastante fluido (ou líquido, para quem o preferir).

As interações no ciberespaço oportunizam aos indivíduos a capacidade de se reinventarem, adotando novas *personæ* virtuais potencialmente muito distantes de suas identidades do mundo real.[130] Falando sobre as imagens de si que emergem dos sistemas *cyber*, Kerckhove descreve a ideia de uma *subjetividade de empréstimo* como exemplo do que ocorre nas comunicações no ciberespaço:

> O seu efeito reside na expansão do *ego* do seu espaço mental privado para o espaço partilhado *on-line*, enquanto o espaço social imediato fica dedicado à privacidade. Quando se está a ligar e a desligar da Internet essa actividade corresponde ao aumento da presença do ser no ciberespaço e fora do tempo, especialmente em modelos de transmissão assíncronos. O "eu *on-line*" não se apoia em nenhum tipo de tempo, espaço ou corpo, e é, sem dúvida, um presente.[131]

---

[128] MYTHEN, Gabe. "Criminologia e Terrorismo: rumo a uma abordagem crítica" In CARLEN, Pat; FRANÇA, Leandro Ayres. *Criminologias alternativas*. Porto Alegre: Canal de Ciências Criminais, 2017. p. 365-380.

[129] LÉVY, Pierre. *A conexão planetária*: o mercado, o ciberespaço, a consciência. trad. Maria Lúcia Homem e Ronaldo Entler. São Paulo: Ed. 34, 2001. p. 19.

[130] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*; *Idem*. *Cybercrime and society, op. cit.*, p. 11.

[131] KERCKHOVE, Derrick de. *A pele da cultura, op. cit.*, p. 267.

Mas, além dessa personificação voluntária, é necessário destacar que a *presença* virtual se constitui a partir de uma multiplicidade de informações compostas pelos perfis nas redes sociais, pelos registros em fóruns, pelas contas de compras online e pela comunicação fática das atualizações de status, dos gestos sem informações (curtidas, cutucadas, *matches*) e de outras formas de interação que priorizam a conexão e o reconhecimento sobre o conteúdo e o diálogo.[132] Esse conjunto de informações constitui uma presença digital, uma *persona* pública virtual e desincorporada, que se apresenta em vários pontos na arquitetura do ciberespaço, numa vasta e permanente reserva online de informações pessoais (de fotografias marcadas, de preferências de consumo e de hábitos de navegação).

E essa *persona* virtual – quem chamarei de *atuante*, nesta tese – nem mesmo combina, em seus movimentos, com a pessoa física que está diante dos computadores. Explicando a diferença entre o *humano de massa* e o *humano de velocidade*, Kerckhove afirma que, enquanto o primeiro modelo humano estava preso num mundo feito para ele por indústrias da consciência, restando homogeneizado e despersonalizado pela mídia de massa, o segundo modelo está em todos os lugares, mas, ainda assim, no centro das coisas, o que esclarece como, apesar de mergulhado num dispositivo comum, sejam promovidas e enfatizadas suas diferenças.[133] E mais: o novo atuante – desincorporado, onipresente e permanente – existe à velocidade da luz, enquanto seu correspondente homólogo – incorporado, limitado e passageiro – não se move. Kerckhove elucida essa distinção:

> Mesmo a polícia de província que nos apanha em excesso de velocidade num estrada secundária pode ter acesso ao nosso registro chamando a base de dados da polícia pelo seu telefone celular. (...) A sua velocidade é o acesso instantâneo que têm às coisas e à informação.[134]

E, enquanto no mundo real o anonimato tem que ser criado, no ciberespaço o anonimato é o óbvio.[135] Essa constatação não deve ser compreendida como um natural e absoluto desconhecimento de autoria ou assinatura, como tradicionalmente se deduz sobre aquilo que é considerado anônimo. As condutas podem não ser imediata e facilmente atribuíveis aos atuantes no ciberespaço, mas elas são rastreáveis – através de operações de *reverse DNS look-up* ou *cookies*. Essa rastreabilidade é um tipo de

[132] Vince Miller *apud* HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*, p. 457.
[133] KERCKHOVE, Derrick de. *A pele da cultura*, *op. cit.*, p. 186.
[134] *Ibidem*.
[135] LESSIG, Lawrence. *Code*: version 2.0, *op. cit.*, p. 45.

impressão digital, que é sem sentido a menos que seja decodificada, e, uma vez decodificada, vincula ao atuante responsável.[136] E isso é possível porque todo atuante apresenta uma concretização qualitativa (individualidade de características na rede) e uma concretização numérica (endereço) que lhe proporciona identidade e reconhecimento na rede mundial de computadores.[137] (Importante destacar que se trata da identidade do atuante – conjunto sujeito-máquina –, não revelando ela imediatamente o indivíduo que se conjunta com o computador, e que o endereço numérico é exclusivo, porém provisório.)

Mas, de qualquer modo, sua arquitetura induz uma impressão de anonimato nos usuários. E essa sensação de anonimato permite que os indivíduos empreendam comportamentos que, na realidade social tradicional, seriam limitados por níveis distintos de controle (freios psicológicos, regras sociais, normas jurídicas) e que, se executados, seriam recepcionados como ilícitos ou, no mínimo, desviantes. Um exemplo rotineiro e não criminoso retrata bem essa distinção: não é incomum que indivíduos, pelas razões mais diversas, acompanhem a vida de outrem nas redes sociais e a tal nível de dedicação que, articulado com aplicativos diversos (Facebook, Twitter, Foursquare), seja-lhes possível traçar uma rotina do sujeito observado. A mesma prática de acompanhamento e observação da vida cotidiana de uma terceira pessoa, se aplicada no mundo real (basta imaginar um observador constante à janela de casa) implicaria na identificação de uma conduta impertinente, agressiva, desviante, à qual a primeira reação do observado seria ligar para a autoridade policial.

1.3.1.6 Novos aspectos da vitimização

Novas formas de associações e intercâmbios, caracterizadas pela instantaneidade e pela aparente equidistância das interações entre usuários, tornam todos vulneráveis a uma variedade de "predadores" que podem alcançá-los instantaneamente, sem as restrições das barreiras normais da distância física.[138]

Essa percepção generalizada de vitimização real ou potencial já era uma característica da modernidade tardia e foi descrita por Garland e Sparks como o *complexo criminal*: uma formação cultural caracterizada por um distinto conjunto de

---

[136] *Ibid*., p. 70.
[137] COLLI, Maciel. *Cibercrimes, op. cit.*, p. 74.
[138] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*; *Idem*. *Cybercrime and society, op. cit.*, p. 11.

atitudes, crenças e práticas, derivado da percepção dos altos índices criminais como um fato social normal, o que tornou a evitação do crime um princípio organizador da vida cotidiana.[139] A arquitetura telemática majorou a possibilidade dessa experiência e intensificou a sensação da potencialidade de vitimização; e há claros indícios de que efeitos psicológicos e comportamentais nascidos dessa percepção dos *cybercrimes* resultaram em hábitos cotidianos de prevenção.

Grabosky não percebe isso da mesma forma.[140] Para ele, as possibilidades de vitimização são muito semelhantes, tanto no mundo físico quanto no ciberespaço. Argumenta ele que, na realidade tradicional, as pessoas também têm ciência de sua vulnerabilidade perante o fenômeno criminal; têm ciência de que, caso sejam vítimas de subtração patrimonial (furto numa residência, por exemplo), têm poucas chances de recuperar suas posses; estão cientes de que é bastante certo que os infratores não serão levados à justiça e que o papel da polícia se resumirá ao registro da ocorrência, algumas palavras de consolo e talvez alguns conselhos de prevenção contra futuros delitos; estão cientes, por fim, de que estão por conta própria e que só uma mudança de hábito (e uma reforma estrutural, para aqueles que puderem pagar por isso) pode reduzir o grau de vulnerabilidade. Nesse sentido, conclui ele, a "necessidade de autoconfiança no controle do crime não é menor no ciberespaço do que na vizinhança física de alguém".[141]

Além disso, uma equidistância virtual sem a correspondente proximidade física também tem sido incentivo aos comportamentos desviantes no ciberespaço. Em entrevista a Wall, um condenado por fraude na internet afirmou que foi a falta de contato direto com a vítima que se tornou um atrativo para suas condutas.[142] As fraudes virtuais, em especial, atraem muitos atuantes em razão da (equivocada) crença de que se trata de uma infração sem vítimas e, por consequência, de que a perda financeira é suportada pelos bancos; essa estratégia de neutralização (ou lenda urbana) esconde a realidade de que as instituições financeiras acabam por repassar o prejuízo aos comerciantes, os quais o compensam transferindo o custo desses riscos operacionais aos consumidores.[143]

Na pesquisa realizada por Moore e McMullan com 44 estudantes de graduação (que cursavam as disciplinas de criminologia ou justiça criminal), os entrevistados

---

[139] GARLAND, David; SPARKS, Richard. "Criminology, Social Theory and the Challenge of our Times", *op. cit.*
[140] GRABOSKY, Peter N. "Virtual Criminality: Old Wine in new Bottles?", *op. cit.*
[141] *Ibid*., p. 245.
[142] WALL, David S. *Cybercrime*, *op. cit.*, p. 64.
[143] *Ibid*., p. 81.

revelaram que a grande maioria deles (96%) jamais cometeria furtos de CDs de músicas ou de DVDs de filmes em estabelecimentos comerciais, enquanto a totalidade deles realizava compartilhamento de arquivos, com uma maioria (86%) fazendo isso diariamente, todos cientes da natureza ilícita dessa atividade.[144]

1.3.1.7 A transnacionalidade (e a irrelevância das jurisdições territoriais)

A aplicação normativa e a persecução criminal, essencialmente vinculadas a jurisdições territoriais, tornaram-se um problema no ciberespaço; nas palavras de Lévy, é como se as leis nacionais sobre informação e comunicação tivessem se tornado "irrelevantes".[145] Colli oferece um exemplo didático:

> O sujeito ativo de um delito pode estar no país *A*, enquanto o provedor por meio do qual ele se conecta a *internet* está no país *B*, os dados aos quais ele acessa ou o computador que ele danifica estão no país *C*, e esses *objetos materiais* são de propriedade de um cidadão do país *D*.[146]

Por isso, a globalização dos *cybercrimes* exige um nível razoável de fundamento legal comum entre os ordenamentos dos países. Capeller defende a adoção de princípios comuns para se permitir um intercâmbio jurídico em escala global.[147] Grabosky argumenta que, sem a dupla criminalização de um injusto cometido e de um acordo diplomático, é pouco provável que haja uma assistência jurisdicional do país no qual o infrator esteja situado, por exemplo.[148] E mesmo que haja uma estrutura jurídica suficiente, exige-se ainda um comprometimento institucional dos governos e de suas agências policiais para o cumprimento da persecução, uma vez que a prática do trabalho policial expõe que as agências têm suas demandas e prioridades locais, que podem preterir a resolução de um caso além de sua jurisdição e o atendimento a uma vítima distante. Para Ripollés[149], cabe ao Direito Internacional Penal o estudo da criminalização das condutas lesivas à comunidade internacional, dentre elas aquelas

---

[144] MOORE, Robert; MCMULLAN, Elizabeth C. "Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students", *International Journal of Cyber Criminology*, v. 3, n. 1, jan-jun 2009, p. 441-451.
[145] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 187.
[146] COLLI, Maciel. *Cibercrimes*, *op. cit.*, p. 80, grifos no original.
[147] CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", *op. cit.*, p. 240.
[148] GRABOSKY, Peter N. "Virtual Criminality: Old Wine in new Bottles?", *op. cit.*
[149] *Apud* COLLI, Maciel. *Cibercrimes*, *op. cit.*, p. 81.

decorrentes dos fenômenos da globalização, da mundialização e as postas em marcha com o advento da sociedade da informação.

1.3.1.8 Uma constante fluida

E o maior desafio de todos é que o dispositivo que se analisa – a transformação tecnológica do cotidiano – é um processo dinâmico, contínuo e que se intensifica a cada novo momento. Essa sensação de movimento acelerado é nítida, por exemplo, nos microfenômenos inéditos de *cybercrimes*: o intervalo de tempo para uma oportunidade de cometimento de um *cybercrime* se tornar uma onda de *cybercrime* passou a ser medido em horas e minutos, em vez de meses e anos, como ocorria com crimes tradicionais.[150]

Capeller cita que, além da *transnacionalidade*, duas outras características da internet têm impacto direto na questão do controle: a *fugacidade* e a *natureza volátil* de seu conteúdo e das estratégias de seus operadores.[151] Um usuário pode ser simultaneamente um servidor, um editor ou um consumidor, gerando uma grande confusão dos diversos papéis na comunidade virtual; e essa confusão de papéis por vezes torna impossível determinar qual norma legal aplicar. Basta pensar na dificuldade de se definir um *spammer*: aquele que compila a lista de destinatários, aquela que vende a lista, aquele que a compra, aquela que distribui as mensagens, aquele que abusa na propaganda de seu produto, todos eles?

Lévy argumenta que, apesar de o movimento fluido e constante dar a impressão de que a tecnologia digital carece de qualquer essência estável, o ritmo de mudança é, em si, e paradoxalmente, uma constante da cibercultura.[152] Essa *constante fluida* parcialmente explica a sensação de impacto, exterioridade e estranheza que nos aflige quando nos aventuramos a apreender o movimento contemporâneo da tecnologia. Tratando da instantaneidade, Kerckhove explica que a perda do espaço de tempo necessário na comunicação moderna coloca todas as culturas num *jet-lag* permanente.[153]

Por mais que todo crime exija instrumentos de detecção mais apurados e qualificação técnica dos profissionais da justiça (pense-se, por exemplo, nos crimes econômicos), esse aspecto do dinamismo da tecnologia da informação é um desafio

[150] WALL, David S. *Cybercrime, op. cit.*, p. 2-3.
[151] CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", *op. cit.*, p. 238.
[152] LÉVY, Pierre. *Cyberculture, op. cit.*, p. 9.
[153] KERCKHOVE, Derrick de. *A pele da cultura, op. cit.*, p. 245.

ainda mais complexo porque dificulta a detecção dos *cybercrimes* pelos tradicionais canais de aplicação da lei e porque seu controle demanda que agentes de segurança (estatais ou privados) desenvolvam qualificação técnica específica, comparada àquela dos atuantes.[154]

1.3.2 Pressuposto filosófico

O *cybercrime* existe como objeto jurídico, como pauta legislativa, como tópico jornalístico, tema literário, ou compartilhado na comunicação cotidiana das pessoas. Mas, o que caracteriza o crime como propriamente *cyber*, exigindo novas e alternativas criminologias para si?

A referência corriqueira a *cybercrimes* e a consequente e expansionista pretensão atributiva do predicado *cyber* aos crimes que envolvem, de algum modo, a arquitetura da tecnologia da informação carecem de esclarecimento sobre o que é propriamente *cyber* neles. Já se afirmou ser comum que, quando assim chamados casos de *cybercrimes* chegam às delegacias especializadas ou aos tribunais, eles se revelem mais por seu aspecto tradicional do que genuinamente *cyber*.[155] Há um amplo e claro problema de divergência epistemológica – pois noções de *cyber* provêm de construções legislativas, acadêmicas, do saber de especialistas, populares[156], e também filosóficas, literárias etc., quando não metafóricas – que se oculta sob um aparente consenso de sentido. Mas, mesmo que se limite o campo de análise, contemplando a criminologia momentaneamente livre de influências de outros saberes, assim idealmente isolada, o que seria propriamente *cyber* para esta nova criminologia? Sugere-se aqui que a resposta deve ser buscada sob a perspectiva da técnica.

Com o propósito de pautar a construção de uma teoria criminológica alternativa, este ensaio propõe a seguinte definição: as criminologias *cyber* estudam o fenômeno criminal originado na técnica (realidade ontológica temporal e dinâmica), estruturado e condicionado pelo dispositivo da tecnologia da informação.

Essa proposição exige, num primeiro momento, que se estabeleça o ponto de vista necessário para a análise fenomenológica. Se a técnica artesanal permitia que o homem tivesse certo conhecimento de si e de seu mundo de acordo com sua medida –

---

[154] SIEGEL, Larry J. *Criminology*, *op. cit.*, p. 468.
[155] WALL, David S. *Cybercrime*, *op. cit.*, p. 8-9.
[156] *Ibid*., p. 12-13.

porque os instrumentos, prestando-se à atividade manual, permaneciam extensão ou parte do corpo humano –, o sistema de instrumentos e, posteriormente, o maquinismo romperam com essa situação. A manualidade cedeu espaço à maquinação; os artesãos foram substituídos pelos operadores; os trabalhadores se converteram em apêndices dos maquinismos.[157]

Numa das aulas do curso que lecionou na Universidade de Freiburg, entre 1942 e 1943, Heidegger apresentou uma distinção alegórica entre a escrita manual (manuscrita) e a escrita mecânica:

> O homem em si age [*handelt*] através da mão [*Hand*]; porque a mão é, junto com a palavra, a distinção essencial do homem. Somente um ser que, como o homem, "tem" a palavra (*μῦθος, λόγος*)[158], pode e deve "ter" "a mão". Através da mão ocorrem ambos oração e assassinato, saudação e agradecimento, juramento e sinal, e também o "trabalho" da mão, o "trabalho manual", e a ferramenta. O aperto de mãos sela o pacto. A mão provoca o "trabalho" de destruição. A mão existe como mão apenas onde há revelação e encobrimento. Nenhum animal tem uma mão, e uma mão nunca originou de uma pata ou uma garra ou presa. Até a mão de alguém em desespero (o mínimo de tudo) jamais é uma presa, com o que uma pessoa agarra selvagemente. A mão brotou a partir da palavra e junto com a palavra. O homem não "tem" mãos, mas a mão detém a essência do homem, porque a palavra como o reino essencial da mão é o fundamento da essência do homem. A palavra, como o que é inscrito e que aparece como tal, é a palavra escrita, ou seja, a escrita. E a palavra como escrita é manuscrito.
>
> Não é por acaso que o homem moderno escreva "com" a máquina de escrever e "dite" [*diktiert*] (a mesma palavra em "poetar" [*Dichten*]) "em" uma máquina. Esta "história" dos tipos de escrita é uma das razões principais da majorante destruição do mundo. Esta não mais vem e parte por causa da mão que escreve, da mão que age propriamente, mas pelas forças mecânicas que ela libera. A máquina de escrever dissocia a escrita do reino essencial da mão, ou seja, do reino da palavra. A própria palavra se torna algo "tipografado". Onde a escrita à máquina, ao contrário, é somente uma transcrição e serve para preservar a escrita, ou torna impresso algo já escrito, ali há um próprio, ainda que limitado, significado. No tempo do primeiro domínio da máquina de escrever, uma carta escrita nesse aparelho representava uma violação das boas maneiras. Hoje, uma carta escrita à mão é uma coisa antiquada e indesejada; ela atrapalha a leitura rápida. A escrita mecânica priva a mão de sua classe no reino da palavra escrita e degrada a palavra a um meio de comunicação. Além disso, a escrita mecânica oferece esta "vantagem", a que ela esconde o manuscrito e, assim, o caráter. A máquina de escrever faz todos parecerem idênticos.[159]

---

[157] RÜDIGER, Francisco. *Martin Heidegger e a questão da técnica*: prospectos acerca do futuro do homem. 2. ed. Porto Alegre: Sulina, 2014. p. 25-26; em sentido contrário: LATOUR, Bruno. *Pandora's hope*: essays on the reality of science studies. Cambridge, London: Harvard University Press, 2000. p. 193-198.

[158] Em português: mitos, logos.

[159] HEIDEGGER, Martin.. *Parmenides*. trad. André Schuwer e Richard Rojcewicz. Bloomington: Indiana University Press, 1998. p. 71-87.

É óbvio que Heidegger não tencionava investigar a máquina de escrever em si – e isso seria absolutamente injustificável num curso sobre o grego Parmenides. Em sua metáfora da máquina de escrever, o aparelho surge, a tecnologia surge de um modo cotidiano – e, por isso, despercebido – e extrai a escrita da origem de sua essência (da mão), transferindo-a para a máquina. Encobre-se a essência da escrita, oculta-se o papel da mão, produz-se uma escrita impessoal, faz-se todos idênticos, desenvolve-se uma acessibilidade uniforme[160], sem que o homem tenha experimentado essa subtração de si.

> Portanto, quando a escrita foi subtraída da origem de sua essência, *i.e.*, da mão, e foi transferida à máquina, uma transformação ocorreu na relação do Ser com o homem. É de pouca importância, para essa transformação, quantas pessoas realmente usam a máquina de escrever e se há alguns que a evitam.[161] Não é por acaso que a invenção da prensa móvel coincide com o início do período moderno. Os sinais das palavras tornam-se tipos e o movimento da escrita desaparece. O tipo é "disposto" e a disposição se torna "prensada". Esse mecanismo de disposição e prensagem e "impressão" é a forma preliminar da máquina de escrever. Na máquina de escrever nós encontramos a irrupção do mecanismo no domínio do mundo. A máquina de escrever leva novamente à máquina de composição tipográfica. A prensa se torna a prensa rotativa. Na rotação, o triunfo da máquina vem à tona. Certamente, a princípio, a impressão de livros e, então, os tipos maquinais oferecem vantagens e conveniências, e esses, então, preferências involuntariamente orientadas e necessidades desse tipo de comunicação escrita. A máquina de escrever oculta a essência da escrita e do escrito. Ela subtrai do homem a categoria essencial da mão, sem que o homem experiencie apropriadamente essa subtração e reconheça que ela transformou a relação do Ser com sua essência.[162]

A transmutação do manuscrito em escrita mecânica é apenas uma maquete utilizada por Heidegger para compreender a relação do homem moderno com a tecnologia. Quando o homem foi desapossado desse saber, abriram-se duas possíveis perspectivas[163] para se analisar a técnica: uma instrumental (calculadora) e outra questionadora (reflexiva). O sujeito da técnica limita-se a pensar superficialmente o

---

[160] A referência à *acessibilidade uniforme* somente aparece na *Carta sobre o Humanismo*: "Assim, a linguagem se entrega ao serviço da comunicação acelerada junto a vias em que a objetificação – a uniforme acessibilidade de tudo a todos – ramifica-se e desconsidera todos os limites. Desse modo, a linguagem submete-se à ditadura da esfera pública a qual decide, antecipadamente, o que é inteligível e o que deve ser rejeitado como ininteligível." (HEIDEGGER, Martin. *Carta sobre el Humanismo*. trad. Helena Cortés e Arturo Leyte. Madrid: Alianza Editorial, 2000. p. 18.)

[161] Se há quem não a opere, tem, ao menos, que renunciar a ela e a evitar, porque a tecnologia "está estabelecida em nossa história" (Heidegger 1942-1943/1998); "Em toda parte nós permanecemos tolhidos e agrilhoados à tecnologia, seja quando passionalmente a afirmamos, seja quando a negamos." (HEIDEGGER, Martin. *The question concerning technology, and other essays*. trad. William Lovitt. New York/London: Garland Publishing/Harper & Row Publishers: 1977. p. 4.).

[162] HEIDEGGER, Martin. *Parmenides*, *op. cit.*

[163] O objeto (técnica) é constante; o que muda é a posição do sujeito.

bom ou mau uso dos meios técnicos (um ativismo a favor ou contra a técnica)[164], ou confronta-se com um problema e se propõe a solucioná-lo mediante a aplicação ou o desenvolvimento de uma fórmula (a criminalização irrefletida de todo comportamento desviante e sua qualificação como *cyber*; o transplante de teorias criminológicas tradicionais para o espaço virtual); sob o jugo da essência da técnica, este *funcionário da técnica* põe em marcha um saber meramente instrumental, funcional.[165] Por sua vez, o sujeito que se propõe a refletir sobre a questão da técnica conserva uma distância com relação a ela "para pensar a origem e o sentido da técnica como saber definido pelo calculismo, a forma e os problemas que advêm do seu crescente e impensado predomínio em nossa existência".[166-167]

Em seguida, em prol da redução de interferências semânticas, faz-se necessária a pronta exclusão de sentidos que não podem mais ser atribuídos à técnica. Primeiro, então: a técnica não pode ser pensada de modo antropológico; o humanismo moderno constitui-se numa obsessão, numa fixação com o humano, na crença no homem, que parte dele e a ele volta.[168] Sobre isso, Giacoia Jr. afirma que o "credo antropocêntrico e humanista é uma ilusão ingênua e perigosa, pois concebe a tecnologia como

---

[164] "Seria insensato atacar cegamente a tecnologia. Seria míope condená-la como a obra do diabo. Nós dependemos de aparelhos técnicos; eles até nos desafiam para sempre maiores avanços." (HEIDEGGER, Martin. *Discourse on thinking*. trad. John M. Anderson e E. Hans Freund. New York: Harper & Row, 1966. p. 53; ver também HEIDEGGER, Martin. *Parmenides*, *op. cit.*).

[165] Lévy parece inicialmente escapar de uma análise instrumental: "Uma tecnologia não é boa nem má (dependendo do contexto, uso e ponto de vista), ou, aliás, mesmo neutra (uma vez que ela condiciona ou compele, expõe ou fecha, a variação de possibilidades)." Mas, na sequência de sua argumentação, o autor revela sua inclinação por um saber funcional: "Não é uma questão de avaliar seu 'impacto', mas de identificar aqueles pontos de irreversibilidade nos quais a tecnologia nos força a nos comprometermos e nos proporciona oportunidades de elaborar os projetos que explorarão as virtualidades que ela guarda em si e de decidir o que nós faremos com eles." (LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 8); "Quando o impacto da tecnologia é negativo, nós devemos questionar a organização do trabalho, ou as relações de dominação, ou a emaranhada complexidade dos fenômenos sociais. Similarmente, quando o impacto é sentido como positivo, obviamente não é a tecnologia que é responsável pelo sucesso, mas as pessoas que conceberam, implementaram e empregaram seus instrumentos. Nesse caso, a qualidade do processo de apropriação (isto é, em última análise, a qualidade das relações humanas) é frequentemente muito mais importante que a particularidade sistêmica de nossa ferramenta, ao ponto de se poder separá-las." (*Ibid*., p. 10)

[166] RÜDIGER, Francisco. *Martin Heidegger e a questão da técnica*, *op. cit.*, p. 24.

[167] Como na reflexão filosófica de um personagem (Noel) de Erico Verissimo: "Se pudéssemos ficar à margem, vendo o rio passar, sem nos deixarmos levar por ele, talvez pudéssemos desvendar um pouco do mistério da vida." (VERISSIMO, Erico. *Um lugar ao sol*. 36. ed. São Paulo: Companhia das Letras, 2006. p. 209.).

[168] Exemplos de como a técnica é pensada de modo antropológico: Lévy se afirma profundamente convencido de que "*permitir que seres humanos conjuguem sua imaginação e sua inteligência para o desenvolvimento e a emancipação do indivíduo* é o melhor uso possível das tecnologias digitais" (LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 190, grifos no original). Para ele, esse projeto de inteligência coletiva amplia (e supera) a filosofia do Iluminismo, pois, além da criação de uma "utopia tecnológica", trata-se do fortalecimento do antigo ideal da emancipação e da exaltação do humano, baseado na tecnologia do presente (*Ibid.*, p. 191).

instrumento à disposição e controle da racionalidade humana"[169], o que nos remete ao próximo sentido.

Segundo: ela tampouco pode ser pensada de modo materialista ou instrumental, como meio de ação originado do desenvolvimento do organismo humano, como instrumento controlado pelo homem; isso porque, ao mesmo tempo em que produz a técnica, o homem se torna dela dependente, ou, em outras palavras, porque o homem somente *vem a ser* pela técnica e pela ciência modernas.[170]

E, terceiro: é preciso esclarecer que a própria técnica não deve ser confundida com a sua condição de *ente* (coisa, algo objetivável que se apresenta no cotidiano: o computador, os cabos conectores), nem com a propriedade que ela confere a certos entes (o técnico).[171]

A técnica é aqui compreendida como uma realidade ontológica temporal e dinâmica.

Nesse ponto, porém, torna-se necessário esmiuçar melhor algumas reinterpretações de termos filosóficos fundamentais. E o que pode parecer uma mera curiosidade etimológica, o resgate da etimologia grega, em verdade, oportuniza uma prova de conhecimento que nos era inacessível – na linha de raciocínio heideggeriana, a linguagem, e neste caso a língua grega, é instrutiva, revelando a experiência fundamental de um povo. O próprio Heidegger argumentara que a apropriação das palavras gregas pelo pensamento romano, isto é, a tradução de nomes gregos para o latim, não foi sem consequência, pois o que estava oculto na tradução aparentemente literal era uma translação da experiência grega para um diferente modo de pensar: "*O pensamento romano assume as palavras gregas sem a correspondente e equiprimordial experiência do que elas dizem, sem o mundo grego*".[172] A falta de raízes do pensamento ocidental, concluía Heidegger, começara com essa tradução.

---

[169] GIACOIA JUNIOR, Oswaldo. *Heidegger urgente*: introdução a um novo pensar. São Paulo: Três Estrelas, 2013. p. 102.

[170] Lyotard parece concordar com a ideia de o homem somente *vem a ser* pela técnica: "Sabem, a técnica não é uma invenção dos homens. Talvez o contrário." (LYOTARD, Jean-François. *O inumano*: considerações sobre o tempo. 2. ed. Lisboa: Editorial Estampa, 1997. p. 20.) Todavia, é preciso esclarecer que, diferente do conceito heideggeriano da técnica como um acontecimento e um modo de saber, Lyotard entende que "É técnico qualquer sistema material que filtre informação útil à sobrevivência, que a memorize e a trate, e que induza, a partir de uma instância reguladora, determinadas condutas, ou seja, a intervir sobre o meio ambiente assegurando pelo menos a sua perpetuidade." (*Ibid*., p. 21.)

[171] RÜDIGER, Francisco. *Martin Heidegger e a questão da técnica*, *op. cit.*, p. 23.

[172] HEIDEGGER, Martin. "The Origin of the Work of Art", *in* YOUNG, Julian; HAYNES, Kenneth (eds.). *Off the beaten track*. trad. Julian Young e Kenneth Haynes. Cambridge: Cambridge University Press: 2002. p. 6, grifos no original.

Os gregos utilizavam a mesma palavra, *tékhnē* (τέχνη), tanto para a arte como para o ofício, a manufatura; no sentido grego original, porém, *tékhnē* não significava nem arte, nem ofício – no amplo sentido medieval de habilidade para produzir alguma coisa –, nem qualquer coisa estritamente técnica – em seu sentido moderno de métodos e atos de produção –, mas um *modo de saber* (tal como o eram, mas de forma distinta, a ciência, *episteme*, a sabedoria, *philosophía*, a crença, *dóksa*).[173] Assim, se *tékhnē* é entendida não meramente como um certo tipo de aptidão prática ou uma maneira de fazer, mas primariamente como uma forma de conhecimento, ela também deve pertencer dentro da órbita da verdade, pois, como um modo de saber, ela é um modo de trazer seres, entes, coisas para fora do ocultamento e ao desocultamento de suas aparências[174] – a *tékhnē* é um acontecimento.

Historialmente, as técnicas tradicional e moderna são fundamentalmente distintas: enquanto aquela era uma forma de revelação poética, a técnica moderna, ou a tecnologia, é uma armação matemática, constituída como sistema e articulada cada vez mais objetivamente, não como o aparato material ou as redes sociotécnicas que vão se formando, mas como "o saber que permite a tudo isso não apenas funcionar, mas se impor como nova e radical forma de mundo".[175] Se no século XVII, o sentido de tecnologia era o estudo das técnicas – isto é, o estudo dos saberes, a exposição das regras de uma arte –, a partir do século XIX, tecnologia passa a se referir à síntese entre a técnica e a ciência, à técnica científica, ou seja, ao saber científico operacionalizável. No entanto, ainda que possa parecer que haja um salto quantitativo do entendimento grego de *tékhnē* para a técnica moderna, o sentido grego ainda nos mostra algo essencial sobre esta. "A tecnologia é um modo de revelação", escreveu Heidegger[176]; ela vem à presença onde a verdade acontece.

Diante da convicção imperante segundo a qual a realidade que vivenciamos é estruturada e movida pela tecnologia, sem, todavia, estar claro qual o sentido ou a definição da tecnologia, as justificativas dessa proposição oferecem um novo critério de análise e delimitação do objeto das criminologias *cyber*: na medida em que é a correspondência entre um processo de posicionamento da realidade e uma forma de chamamento de nossa existência, a tecnologia forma uma época, porque é o vetor de um modo pré-decidido de interpretação do mundo, porque expressa um modo de ser que

[173] HEIDEGGER, Martin. "The Origin of the Work of Art", *op. cit.*, p. 34-35.
[174] *Ibid*., p. 35.
[175] RÜDIGER, Francisco. *Martin Heidegger e a questão da técnica*, *op. cit.*, p. 127.
[176] HEIDEGGER, Martin. *The question concerning technology, and other essays*, *op. cit.*, p. 13.

abre um mundo e, mais importante, porque *condiciona*, em suas próprias possibilidades, todas as atitudes do homem, inclusive as ações que realiza na realidade virtual construída pela tecnologia da informação.

Nesse sentido, discorda-se de Kerckhove, quem afirma que a internet "não é invasora, é-o ainda menos do que o telefone, porque não chama as pessoas, as pessoas é que a chamam".[177] Seguindo o pressuposto desta tese, a internet é forma de comunicação (rede) da tecnologia da informação a partir do qual se estruturam novos comportamentos humanos. E, sendo assim, ela não só chama as pessoas, como se impõe como novo paradigma a partir do qual se revela o mundo para todos.

A noção de condicionamento de possibilidades tecnológicas tem melhor consonância com o que Virilio desenvolve como uma "teoria do acidente": "uma técnica existe não apenas pela monstração – a publicidade, a propaganda, a promoção –, mas também pela demonstração, ou seja, pelo fracasso, pela derrota, pelo acidente".[178] E prossegue ele:

> A internet é um novo objeto informacional que tem a potência de inaugurar o seu acidente. Cada técnica tem o seu acidente. A eletricidade possui a eletrocução ou Chernobyl. Na época da ecologia, do princípio da precaução, do recuo diante da ilusão da técnica e da ciência, os acidentes são elementos muito importantes para analisar, sobretudo quando se trata de uma tecnologia emergente.

Em outras palavras, argumenta Virilio, "o acidente é a demonstração dos limites de uma técnica." No caso da internet, ele cita o *bug do milênio* e os vírus – e poderíamos estender sua reflexão a outras modalidades de *cybercrimes*. A preocupação é um tanto quanto agourenta, porque o acidente pode revelar não somente os "limites" da técnica, mas também vulnerabilidades provisórias ou inclusive oportunidades. Mas, a preocupação é justa, porque, como o próprio Virilio esclarece com sinceridade[179], ele trabalha com a questão da aceleração, mas ele não é um teórico da informática; e, no escopo do aumento da velocidade e da emergência do novo, suas preocupações se justificam:

> O próprio da cibernética é a unidade de tempo e de espaço da interação, de modo que o acidente da internet, logo da cibernética, é geral, passível, potencialmente, de atingir todos e tudo ao mesmo tempo, no mesmo instante.

---

[177] KERCKHOVE, Derrick de. *A pele da cultura*, *op. cit.*, p. 91.
[178] VIRILIO, Paul. "Da política do pior ao melhor das utopias e à globalização do terror", *op. cit.*, p. 10.
[179] *Ibidem*.

> Os meus críticos alegam que isso nunca existiu. Sim, mas antes da invenção da jangada não havia naufrágio. Foi preciso inventá-la para ver que podia afundar. Estamos diante de algo emergente. Porém, não sou o teórico que descreverá por antecipação o acidente integral. Digo apenas que, em potência, ele está aí.[180]

Virilio se contrapõe ao entusiasmo de McLuhan, quem chama de ingênuo, e de Lévy, quem alcunha de guru da internet.[181] Há um evidente prognóstico pessimista em sua análise da técnica cibernética. Num trabalho anterior, ele havia questionado: "depois do fim da guerra fria e do declínio da dissuasão *atômica*, quais serão amanhã os estragos provocados pelo início de uma dissuasão *informática* da realidade sensível que se parece cada vez mais com uma verdadeira 'industrialização da simulação'".[182] Mas não é justo considerá-lo, como o fizeram muitos, como um ludista ou antimodernista.[183]

É importante esclarecer que o argumento desta tese não implica na defesa de um tipo de mistificação, em que as tecnologias são elevadas à condição de elementos geradores privilegiados e sacrossantos de toda uma constelação de eventos históricos, exaltando-lhes o papel em movimentos políticos[184]; tampouco pressupõe o entendimento de qualquer tipo de determinismo. A concepção de dispositivo[185] em Heidegger não sugere isso; o dispositivo, como essência da técnica, é um processo sem sujeito de chamamento tecnológico, que *acontece* entre nós – não nos determina e não pode ser por nós determinada. Por isso, Pattison argumenta que "as repetidas tentativas da humanidade de controlar a tecnologia, de gerir o passo da mudança e da inovação, de conservar um sentido de direção no todo, é inevitavelmente fútil, precisamente porque

---

[180] *Ibid*., p. 11.
[181] *Ibid*., p. 9, 14.
[182] VIRILIO, Paul. *A arte do motor*, *op. cit.*, p. 123, grifos no original.
[183] VIRILIO, Paul. "Da política do pior ao melhor das utopias e à globalização do terror", *op. cit.*, p. 11.
[184] CRARY, Jonathan. *24/7*: capitalismo tardio e os fins do sono. trad. Joaquim Toledo Jr. 2. ed. São Paulo: Cosac Naify, 2015. p. 130.
[185] A palavra original alemã (*Gestell*) tem sido traduzida para o português como *dispositivo*, *armação*, *enquadramento*, *composição* etc. Agamben relaciona o *Gestell* de Heidegger com a *dispositio* dos teólogos e o *dispositif* de Foucault. (AGAMBEN, Giorgio. "O que é um dispositivo?", *outra travessia*, n. 5, 2005.) E prossegue Agamben (*Ibid*., p. 13): "Generalizando posteriormente a já amplíssima classe dos dispositivos foucaultianos, chamarei literalmente de dispositivo qualquer coisa que tenha de algum modo a capacidade de capturar, orientar, determinar, interceptar, modelar, controlar e assegurar os gestos, as condutas, as opiniões e os discursos dos seres viventes. Não somente, portanto, as prisões, os manicômios, o panóptico, as escolas, as confissões, as fábricas, as disciplinas, as medidas jurídicas etc, cuja conexão com o poder é em um certo sentido evidente, mas também a caneta, a escritura, a literatura, a filosofia, a agricultura, o cigarro, a navegação, os computadores, os telefones celulares e – porque não – a linguagem mesma, que é talvez o mais antigo dos dispositivos, em que há milhares e milhares de anos um primata – provavelmente sem dar-se conta das consequências que se seguiriam – teve a inconsciência de se deixar capturar."

controle, administração e direção são eles mesmos valores inscritos no projeto básico do dispositivo".[186]

Lévy é mais esclarecedor na sua explicação de que a tecnologia *condiciona*, e não *determina*, a sociedade:

> Dizer que a tecnologia condiciona é indicar que ela proporciona acesso a certas possibilidades, que certas opções culturais ou sociais não seriam contempladas a sério sem sua presença. Várias possibilidades ainda permanecem abertas e muitas, são deixadas intocadas. A mesma tecnologia pode ser integrada em circunstâncias culturais vastamente diferentes. [...] A imprensa [tipografia] – a qual foi banida na China, mas, como uma atividade industrial, escapou do controle político na Europa – não teve as mesmas consequências no Oriente e no Ocidente. A prensa de Gutemberg não determinou a crise da Reforma, o desenvolvimento da ciência moderna europeia ou a ascensão do idealismo iluminista; ela somente os condicionou.[187]

É bastante evidente a existência de relações entre o desenvolvimento tecnológico e fenômenos (ou tendências) sociais. De uma forma bastante didática, Johnson chama isso de *efeito beija-flor*[188]: uma inovação, ou um conjunto de inovações em dado campo, acaba provocando mudanças que parecem pertencer a um domínio completamente diverso.[189] Explicando o caso que dá nome ao seu argumento, o autor relata como a evolução simbiótica da estratégia reprodutiva das flores com os seus polinizadores criou as condições que permitiram ao beija-flor desenvolver o traço distintivo de pairar: "É fácil imaginar um mundo com flores e sem beija-flores. Muito mais difícil é imaginar um mundo sem flores e com beija-flores".[190] Johnson relata como um fenômeno natural estabeleceu uma corrente de influências evolutivas, e o exemplo serve como fundamento para a alcunha que ele empresta às relações entre invenções e suas consequências (e seu livro está recheado com essas histórias).

Mas, basta que se pense nas consequências do desenvolvimento da técnica da escrita (que, dentre outros efeitos, estruturou e condicionou uma nova forma de saber), ou sobre como o espelho permitiu que o Renascimento acontecesse (sem forçosamente determiná-lo), e ainda como uma específica configuração das antigas máquinas de

---

[186] PATTISON, George. *Routledge philosophy guidebook to the later Heidegger*. London/New York: Routledge, 2000. p. 67.
[187] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 7-8.
[188] Que não se confunde com o *efeito borboleta* da teoria do caos, a qual envolve uma cadeia de causalidade virtualmente incognoscível.
[189] JOHNSON, Steven. *How we got to now*: six innovations that made the modern world. New York: Riverhead Books, 2014.
[190] *Ibid*., p. 36.

escrever influenciou desde o treinamento profissional até um padrão global para a escrita e a fabricação de aparelhos (o modelo QWERTY também evidencia um caso de dependência da trajetória que pode ter resultado num fechamento tecnológico). Ou, mais recente, naquelas referentes ao desenvolvimento dos transportes, mais especificamente, dos automóveis.[191]

O desenvolvimento dos automóveis, no século XX, alterou as estruturas de estradas e cidades, a relação do homem com o seu trabalho, os padrões de moradia; demandou o desenvolvimento de regulamentação própria e de técnicas médicas específicas de emergência e trauma para os acidentes envolvendo os veículos; ao responder à vontade de maior autonomia, promoveu também o comportamento egoísta e a alienação urbana; instalou, assim, uma nova realidade e consumo e, a partir disso isso, declinou-se um novo fenômeno criminal; enfim, a tecnologia automobilística alcançou até mesmo a intimidade das emoções, proporcionando uma inédita liberdade de movimento a centenas de milhões de indivíduos e, consigo, frustrações próprias das fantasias do consumo.

Diante da convicção segundo a qual a realidade que vivenciamos é estruturada e movida pela tecnologia, as justificativas desta proposição oferecem um novo critério de análise e delimitação do objeto das criminologias *cyber*: o fenômeno dos *cybercrimes* próprios é fruto da técnica, ou seja, os comportamentos criminosos, desviantes e ameaçadores, e as correspondentes reações sociais, são estruturados e condicionados pelo dispositivo da tecnologia da informação.

1.3.2.1 Alegoria para explicar a interpretação tecnológica (e não antropológica)

É bastante evidente a existência de relações entre o desenvolvimento tecnológico e fenômenos (ou tendências) sociais. Basta que se pense na história dos transportes ou, mais especificamente, dos automóveis – como analisado acima. Os movimentos sociais ao fim da primeira década do século XXI, contudo, servem de melhor maquete à hipótese acima proposta.

Na Revolução do Panelaço na Islândia (*Búsáhaldabyltingin*, 2009-2011), na Revolução Egípcia (*Thawret 25 Yanayir*, 2011), na Primavera Árabe[192] (2011), nas

[191] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 103.
[192] Inspiradas nas revoltas ocorridas na Tunísia e no Egito, os *Dias de Ira* (*Youm al-Ghadab*) ocorreram em vários países árabes, no ano de 2011: em 7 de janeiro, na Argélia; 12 de janeiro, no Líbano; 14 de

ocupações de espaços públicos (*Occupy*, 2011), nas Jornadas de Junho no Brasil (2013), os movimentos ignoraram instituições políticas tradicionais (partidos políticos), rejeitaram outras organizações formais (sindicatos), desacreditaram a mídia de massa, não reconheceram lideranças e, ainda assim, chacoalharam o mundo.

Tornou-se incontestável que a tecnologia de informação foi uma ferramenta importante para os movimentos. Alguns denominadores comuns aos movimentos espalhados pelo globo comprovam como a tecnologia da informação contribuiu para a explosão desse novo modelo de movimento social:

- *Alta difusão do uso de internet e de redes móveis de comunicação*: Durante os protestos contra a crise financeira na Islândia, 94% dos islandeses estavam conectados à internet e dois terços deles eram usuários do Facebook.[193] No caso do Egito, estima-se que 80% da população possuíam telefones celulares (em 2010), e um quarto das casas tinha acesso à internet (em 2009). Castells relata que após dois anos do lançamento da versão árabe do Facebook, o número de usuários da rede social triplicou, alcançando 5 milhões de usuários em fevereiro de 2011, sendo que 600 mil novos usuários ingressaram na rede social em janeiro e fevereiro do mesmo ano, os meses que marcaram o início da revolução.[194] Nos países onde ocorreu a Primavera Árabe, a população jovem já estava familiarizada com as redes de comunicação digital: em metade dos países árabes, a penetração dos telefones celulares excedia 100% e, nos outros países, ultrapassava a marca de 50%.[195]

- *Surgimento de uma nova forma de espaço – o espaço público híbrido*: A partir das redes sociais virtuais criaram-se comunidades urbanas de ocupação de espaços públicos.[196] Essa característica foi evidenciada pelos movimentos *Occupy*, ocorridos na Praça Tahrir, em Wall Street e tantos outros lugares. Nessas ocupações, os manifestantes interagiram cara a cara,

janeiro, na Jordânia; 17 de janeiro, na Mauritânia, no Sudão e em Omã; 27 de janeiro, no Iêmen; 14 de fevereiro, no Bahrein; 17 de fevereiro, na Líbia; 18 de fevereiro, no Kuwait; 20 de fevereiro, no Marrocos; 26 de fevereiro, no Saara Ocidental; 11 de março, na Arábia Saudita; 18 de março, na Síria.

[193] CASTELLS, Manuel. *Networks of outrage and hope*: social movements in the internet age. Cambridge: Polity, 2014. p. 34.

[194] *Ibid*., p. 57.

[195] *Ibid*., p. 95.

[196] *Ibid*., p. 45.

compartilharam suas experiências, resistiram às dificuldades de acampamento e à violência policial, e colocaram em prática uma variedade de práticas sociais solidárias, autônomas e horizontais, que refletiam o comportamento comum nas redes sociais virtuais.

O espaço físico teve uma função: as ocupações serviram para a publicização dos protestos, para dar uma cara às manifestações, uma representação a partir da qual a mídia *mainstream* pôde compor uma narrativa para transmitir os eventos ao público espectador. "A conexão entre a mídia social da internet, as redes sociais das pessoas e a mídia *mainstream* foi possível por causa da existência de um território ocupado que ancorou o novo espaço público na dinâmica interação entre ciberespaço e espaço urbano".[197]

E o espaço virtual teve sua função: as redes sociais virtuais permitiram que a experiência da ocupação fosse comunicada e amplificada, levando o mundo todo para dentro do movimento; além disso, as redes sociais da internet se estabeleceram como um fórum permanente de planejamento estratégico, debate e solidariedade, alheio ao controle dos governos e de corporações (nos moldes dos monopolizados canais de comunicação de massa).[198]

- *Simbiose comunicativa dos aparelhos*: Os aparelhos de comunicação contêm interfaces com o mundo digital através do qual eles se interconectam. Recentemente, o progresso da digitalização da informação, combinado com a diversificação e a miniaturização de interfaces em elementos móveis, têm convergido à extensão e à multiplicação das entradas ao ciberespaço.[199] Isso pode ser descrito como uma simbiose comunicativa dos aparelhos de comunicação que possibilitou o acesso amplo, constante e imediato à realidade virtual. A confluência de mídias distintas na mesma rede digital integrada é designada "unimídia" (*unimedia*) por Lévy.[200]

  Os protestos foram, geralmente, planejados no Facebook, coordenados via Twitter, divulgados por SMSs e transmitidos ao mundo via Livestream (visualização instantânea), YouTube (visualização posterior) e Tumblr (mídias diversas). Utilizando seus próprios telefones celulares, os quais

[197] *Ibid*., p. 60.
[198] *Ibid*., p. 168-169.
[199] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 20.
[200] *Ibid*., p. 45.

> comportam todos esses aplicativos, cidadãos organizaram e coordenaram protestos, transmitiram imagens e vídeos. Esses aplicativos foram grandemente responsáveis pelo fortalecimento de uma nova estrutura comunicativa, que Castells denomina de *autocomunicação de massa*, baseada em redes horizontais de comunicação multidimensional e interativa na internet, e mais ainda nas redes de comunicação sem fio.[201]
>
> Sem acesso direto aos movimentos (por hostilidade dos manifestantes) e sem uma aproximação tecnicamente adequada aos acontecimentos, algumas das empresas de comunicação alimentaram seus noticiários a partir de informações coletadas nesses aplicativos, enviadas por ativistas presentes nas manifestações e por cidadãos que as captavam por telefones celulares e as transmitiam pela internet (no caso das revoluções árabes, a Al Jazeera se destacou por sua abertura ao jornalismo cidadão).

No entanto, o papel da tecnologia da informação nesses movimentos do início do século XXI foi mais do que isso. Alguns autores sugerem que a tecnologia teve um papel *causal* e *instrumental*.[202] Em contraposição, a análise feita por Castells[203] sobre os protestos esclarece a relação dessa tecnologia com esse fenômeno social. Segundo ele, a tecnologia não é capaz de causar ou determinar movimentos sociais ou, aliás, qualquer comportamento social; os movimentos sociais surgem das contradições e dos conflitos de sociedades específicas, e expressam as revoltas e os projetos individuais.[204] Então,

---

[201] CASTELLS, Manuel. *Networks of outrage and hope*, *op. cit.*, p. 220.

[202] "É verdade que o Facebook e o Twitter não causaram revoluções, mas é insensato ignorar o fato que os usos meticuloso e estratégico da mídia digital para conectar públicos regionais, junto com redes de suporte internacionais, têm empoderado ativistas de novas maneiras que levaram a alguns dos maiores protestos desta década [...]. A mídia digital teve um papel causal na Primavera Árabe no sentido de que ela proporcionou a própria infraestrutura que criou profundas relações de comunicação e capacidade organizacional em grupos de ativistas antes que os maiores protestos acontecessem, e enquanto protestos de rua estavam sendo formados. Certamente, foi por causa dessas redes digitais bem desenvolvidas que líderes civis acionaram, com tamanho êxito, números tão grandes de pessoas para protestar." (Hussain e Howard *apud* CASTELLS, Manuel. *Networks of outrage and hope*, *op. cit.*, p. 105).

[203] "Nas minhas palavras: a Primavera Árabe foram espontâneos processos de mobilização que emergiram de chamados da internet e das redes de comunicação sem fio com base nas redes sociais preexistentes, tanto digitais quanto cara a cara, que existiam na sociedade. Em geral, eles não foram mediados por organizações políticas formais, as quais haviam sido dizimadas pela repressão e não eram confiáveis para a maior parte dos participantes ativos e jovens que encabeçavam os movimentos. Redes digitais e ocupação do espaço urbano, em estreita interação, proporcionaram a plataforma para organização e deliberação autônomas sobre os quais as revoltas se basearam, e criaram a resiliência necessária para os movimentos resistirem a ataques ferozes da violência estatal até o momento em que, em alguns casos, a partir de um instinto de autodefesa, eles se tornaram um contra-estado." (CASTELLS, Manuel. *Networks of outrage and hope*, *op. cit.*, p. 106)

[204] *Ibid*., p. 228-229.

considerando que a tecnologia constitui-se em formas organizacionais, expressões culturais e plataformas para o exercício político[205], a tecnologia da informação contemporânea, caracterizada pela internet e suas plataformas simbióticas (como o telefone celular), criou as condições para uma forma de prática compartilhada[206] que estabeleceu comportamentos peculiares: movimentos sem liderança, coordenações e deliberações horizontais, empoderamento dos participantes como atores autônomos. Uma década e meia antes desses movimentos se espalharem pelo mundo, Kerckhove já havia previsto que o espaço da internet – sem fronteiras, instável, orgânico e em perpétuo movimento – tornaria totalmente obsoletas as nossas ideias políticas.[207]

Discorrendo sobre o movimento *Indignadas* (Espanha), Castells evidencia como a nova proposta política copiou a estrutura das redes virtuais:

> Não houve decisão formal, mas todo mundo concordou na prática, desde o começo do movimento. Não haveria líderes no movimento, tanto local quanto nacionalmente. E mais, nem mesmo porta-vozes eram reconhecidos. Todos representariam a si próprios e a mais ninguém. Isso levou a mídia à loucura, uma vez que as faces de qualquer ação coletiva são ingredientes necessários na técnica narrativa da mídia. A fonte desse princípio antigo, anarquista, frequentemente traído na história, não foi ideológica no caso desse movimento, embora ele tenha se tornado um princípio fundamental, executado pela grande maioria dos atores do movimento. Ele estava presente na experiência das redes de internet, nas quais a horizontalidade é a norma, e há pouca necessidade de liderança porque as funções de coordenação podem ser exercidas pela rede em si, através da interação entre seus nodos. A nova subjetividade apareceu na rede: a rede se tornou o sujeito. A rejeição de líderes foi também consequência das experiências negativas que alguns dos ativistas veteranos haviam sofrido no movimento por justiça global e nas várias organizações radicais da extrema esquerda. Mas isso resultou também da profunda desconfiança de qualquer liderança política organizada após se observar a corrupção e o cinismo que caracterizaram governos e partidos tradicionais.[208]

A experiência da internet proporcionou uma plataforma comunicativa que definiu um modo de mobilização inédito (função *condicionante*) e também se traduziu no comportamento e nas expectativas pessoais ao estabelecer novas demandas de liberdade, autonomia e reconhecimento (função *dispositiva*).

---

[205] *Ibid*., p. 103.
[206] *Ibid*., p. 229.
[207] KERCKHOVE, Derrick de. *A pele da cultura, op. cit.*, p. 242.
[208] CASTELLS, Manuel. *Networks of outrage and hope, op. cit.*, p. 128-129.

2 ESPAÇO

O espaço é um fator de interesse criminológico. Uma vez que esta tese tem como objeto o estudo dos crimes, desvios e ameaças desenvolvidos a partir de, e condicionados por, um novo ambiente, que se convencionou chamar de ciberespaço, é importante que sejam analisadas com maior atenção as teorias criminológicas que tiveram como objeto principal o fator espacial na análise do fenômeno criminal.

Este capítulo, portanto, inicia com o resgate de duas importantes correntes tradicionais: as criminologias ecológicas[209] da Escola de Chicago e as criminologias culturais. E segue com uma análise mais detalhada do ciberespaço, introduzindo duas questões fundamentais: sua neutralidade e sua arquitetura.

2.1 TEORIAS CRIMINOLÓGICAS EXISTENTES

2.1.1 Criminologias ecológicas: Escola de Chicago

Atentas aos novos paradigmas socioeconômicos do início do século XX – urbanização, migrações, segregações de grupos minoritários, conflitos sociais, debilitamento do controle social em certos núcleos (surgimento de gangues em áreas criminógenas, por exemplo) –, as teorias criminológicas nascidas da Escola de Chicago empreenderam valiosas pesquisas sobre a morfologia da criminalidade em meio ao desenvolvimento da urbe.

Com a exclusão dos fundamentos exclusivamente biológicos e psicológicos, a etiologia criminal passou a ser identificada em dois sintomas principais: (i) as carreiras criminosas foram atribuídas às reações sociais da infância e da adolescência dos indivíduos; (ii) e se verificou que a concentração de delinquentes e criminosos ocorria em áreas intersticiais típicas, locais característicos para a reprodução de gangues, delinquência e crime. Essas constatações revelaram aos estudiosos (majoritariamente, sociólogos) que programas de prevenção criminal deveriam voltar-se aos

[209] Ver também a explicação sobre a teoria da atividade rotineira, caracterizada por uma abordagem igualmente ecológica, nas p. 24-29 desta tese.

comportamentos problemáticos dos desviantes e ao mau funcionamento das instituições sociais nas áreas produtoras de crime.[210]

Em razão do recorte temático que interessa ao presente capítulo, as teorizações sobre como a delinquência juvenil decorria da desestrutura familiar e o interesse etnográfico no mundo privado de grupos desviantes, dois aspectos fundamentais da Escola de Chicago, não serão explicados neste capítulo; portanto, por enquanto, me limitarei somente à importância conferida por esses teóricos ao *espaço*.

Os primeiros estudos sobre o espaço foram de autoria de Jane Addams, importante reformadora social e pioneira socióloga feminista. Seus trabalhos formataram a Escola de Chicago e suas produções posteriores, tendo influenciado, por exemplo, Robert Park e Ernest Burgess.[211] No ano de 1895, Addams publicou *Hull-House Maps and Papers...*, uma coletânea de ensaios e de pequenos mapas de ruas que detalhavam regiões pobres de Chicago, mapeando características sociais e demográficas de populações dessa área geográfica.[212]

No entanto, seus trabalhos raramente são destacados no cânone criminológico; na opinião de Hayward[213], além do antifeminismo sintomático da sociologia de Chicago na época, o fascínio pela tecnologia foi predominante: em tempos diversos, a "fascinação com a tecnologia tem frequentemente triunfado sobre outras abordagens mais humanísticas"[214]; nesse caso, o cientificismo associado com os métodos estatísticos de demografia e ecologia humana aplicados à cidade, vista como um laboratório social. Claro, uma das vantagens dessa abordagem é que ela produz resultados facilmente quantificáveis, tipicamente na forma de estatísticas policiais, e essas estatísticas contribuem para o desenvolvimento de uma estrutura mais ampla de atuação governamental, inspirada em estratégias calculistas e atuariais, no controle e gerenciamento dos problemas sociais, tornando o espaço urbano um local privilegiado de monitoramento e campo de testes para novas iniciativas públicas.[215] E, também, essa ênfase no espaços criminogênicos evidencia a superação de um modelo anterior, focado

---

[210] THRASHER, Frederic M. "Juvenile Delinquency and Crime Prevention", *Journal of Educational Sociology*, v. 6, n. 8, 1933, p. 500-509.
[211] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*
[212] ADDAMS, Jane (ed.). *Hull-House maps and papers*: a presentation of nationalities and wages in a congested district of Chicago, together with comments and essays on problems growing out of the social conditions. New York: Thomas Y. Crowell & Co., 1895.
[213] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*, p. 444.
[214] *Ibid*., p. 442.
[215] *Ibid*., p. 445.

no homem delinquente, constituindo um novo objeto de intervenção de práticas governamentais.

Após o precursor trabalho de Addams, as publicações que se preocuparam com o espaço desembocaram no que ficou conhecido como a *teoria ecológica* da criminalidade urbana: a cidade grande passou a ser vista como uma unidade ecológica, no interior da qual se produzia delinquência, desenvolvida de acordo com os "aspectos distributivos" da urbe.[216] A inspiração científica se refletia no empréstimo do léxico ecológico: era comum os autores se referirem a termos como agregação, *habitat*, invasão[217]. Nas palavras de Thrasher, o novo empreendimento científico tratava-se de "uma investigação da anatomia social, histologicamente estudada".[218] A ecologia humana, portanto, compreendia o estudo dos seres humanos, como afetados pelas forças acomodadoras, distributivas e seletivas do ambiente.[219] Essa definição revela que os estudos da Escola de Chicago apresentam também um outro aspecto das ciências naturais: por mais que seja equivocado considerá-los puramente deterministas, é inegável um certo resquício, um quê de determinismo na ideia de uma influência causal do ambiente.[220] Metodologicamente, este viés estava fundamentalmente interessado no efeito da *posição*[221], no tempo e no espaço, sobre instituições e comportamentos humanos.[222]

---

[216] THRASHER, Frederic M. "Ecological Aspects of the Boys' Club Study", *Journal of Educational Sociology*, v. 6, n. 1, 1932, p. 52-58.

[217] *Agregação* é o agrupamento de organismos em resposta a diferentes estímulos ambientais (a oferta de alimento) ou comportamentais (defesa contra predadores). *Habitat* é local ocupado por um organismo, caracterizado por suas propriedades físicas ou bióticas. *Invasão biológica* é o processo que compreende a instalação e grande proliferação de uma espécie não nativa do ambiente, levando a desequilíbrios na comunidade. Sauer criticava a adoção do léxico ecológico: "É melhor não forçar em demasia a nomenclatura biológica na geografia. O nome ecologia não é necessário: ela é ambas morfologia e fisiologia da associação biótica. Uma vez que renunciamos a pretensão das medições de influências ambientais, nós podemos utilizar, em preferência à ecologia, o termo morfologia para se aplicar ao estudo cultural, pois ele descreve perfeitamente o método que é envolvido." (SAUER, Carl Ortwin. "The Morphology of Landscape", *University of California Publications in Geography*, v. 2, n. 2, 1925, p. 45.)

[218] THRASHER, Frederic M. "A Community Study", *Religious Education*, v. 25, 1930, p. 399.

[219] MCKENZIE, Roderick D. "The Ecological Approach to the Study of the Human Community", *American Journal of Sociology*, v. 30, n. 3, 1924, p. 287-301.

[220] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*

[221] Como anotou McKenzie: "A palavra 'posição' é utilizada para descrever a relação local de uma dada comunidade para com outras comunidades, também a localização do indivíduo ou da instituição no interior da própria comunidade". (MCKENZIE, Roderick D. "The Ecological Approach to the Study of the Human Community", *op. cit.*)

[222] *Ibidem*.

Com o desenvolvimento das cidades grandes – com suas peculiaridades urbanas dos arranha-céus, metrôs, lojas de departamentos, jornais diários[223] –, fenômenos espaciais inéditos constituíram novos fatores criminógenos. Contatou-se, primeiro, a crise dos valores tradicionais pela deterioração dos grupos primários[224]. Vínculos de parentesco e de vizinhança, e os sentimentos derivados de uma convivência por gerações sob uma tradição popular comum enfraqueceram-se em agregações cujos membros tinham origens e históricos diversos, e se relacionavam, em grande parte, superficialmente. A maior parte das populações das grandes cidades passou a viver como os hóspedes de um grande hotel: encontram-se, mas não se conheciam.[225-226]

Esse movimento frequente de grandes números de indivíduos em um *habitat* congestionado dava razão a atrito e irritação.[227] Por isso, argumentava Wirth[228], em circunstâncias de convivência e trabalho próximos de indivíduos que não têm laços emocionais e sentimentais, a competição e mecanismos de controle formal forneciam substituintes para os vínculos de solidariedade com os quais se conta para manter unido um grupo social. Mas, a substituição tinha uma sequência: com o fomento do espírito de competição, do enaltecimento e da exploração mútua, tendia-se a recorrer a controles formais para neutralizar a irresponsabilidade e a desordem potencial.[229] Por sua vez, Park sugeria que esse colapso de vínculos locais e o enfraquecimento das restrições e inibições do grupo primário, sob a influência do ambiente urbano, eram, provavelmente e em grande parte, responsáveis pelo aumento do vício e do crime nas grandes cidades; por isso, para se estabelecer essa conexão, sugeria ele que fosse acompanhada a crescente mobilidade da população.[230]

---

[223] BURGESS, Ernest Watson. "The Growth of the City: An Introduction to a Research Project", In PARK, Robert Ezra; BURGESS, Ernest Watson; MCKENZIE, Roderick D. *The city*. Chicago: The University of Chicago Press, (1925) 1967. p. 47.

[224] "Por grupos primários eu quero dizer aqueles caracterizados por associação e cooperação face a face íntimas." (COOLEY, Charles Horton. *Social organization*: a study of the larger mind. New York: Charles Scribner's Sons, 1910. p. 23)

[225] PARK, Robert Ezra. "The City: Suggestions for the Investigation of Human Behavior in the City Environment", *American Journal of Sociology*, v. 20, n. 5, 1915, p. 608.

[226] Talvez faltem maiores reflexões sobre o impacto desse modelo globalizado de hotelaria às relações sociais. Jonathan Crary (CRARY, Jonathan. *24/7*, *op. cit.*, p. 105), analisando a experiência social contemporânea a partir do filme *Psicose* (1960), de Hitchcock, retrata o motel – em sua concepção americana de hotéis de beira de estrada, horizontais e informais – como "emblema central da modernidade, que expressa o não lugar e a mobilidade". E prossegue: "Em seu anonimato degradado, o estabelecimento surge como um terreno de importância lateral, sem profundidade, de fluxo e permutabilidade, de uma vida temporária e provisória, nutrida apenas pela circulação do dinheiro".

[227] WIRTH, Louis. "Urbanism as a Way of Life", *American Journal of Sociology*, v. 44, n. 1, 1938, p. 16.

[228] *Ibid*., p. 11.

[229] *Ibid*., p. 15.

[230] PARK, Robert Ezra. "The City: Suggestions for the Investigation of Human Behavior in the City Environment", *op. cit.*, p. 595.

Segundo, a perda de raízes se intensificava pela alta mobilidade das pessoas. A cidade tornou-se um caldeirão de raças, povos e culturas. Os fenômenos de mobilidade de pessoas e grupos incluíam os fluxos diários da população de uma parte da comunidade a outra, os movimentos sazonais, as dispersões das férias de verão, as migrações, as imigrações e as emigrações, todos eles com o potencial de alterar as características básicas de uma comunidade, tanto no aspecto de valoração espacial e de funcionalidade das instituições, quanto no que toca à solidariedade e ao moral dos bairros.[231] A partir das vívidas e sutis interações do qual ela virou o centro, a cidade transformou-se em um terreno fértil para novos híbridos biológicos e culturais.[232] É assim que Thrasher descrevia a realidade estadunidense:

> Ao contrário dos sistemas sociais mais consistentes, se não mais simples, de alguns povos pré-letrados, os vários elementos na organização social americana são altamente heterogêneos e geralmente em um estado de incerteza e contradição mútua.
> Parcialmente por causa de nossas variadas origens estrangeiras e de nossos diversos desenvolvimentos no país, a América é um conglomerado de grupos e padrões divergentes. Podemos nos tornar mais consistentes com o tempo, mas, no presente, dificilmente pode ser imaginada uma maior variedade de heranças e tendências. Nós somos uma mistura de puritanos e Cavaliers; crueza e refinamento; riqueza e pobreza; brancos, negros, bronzeados e amarelos; norte e sul; cidade e campo; secos e molhados; nativos e imigrantes; leste e oeste; irlandeses e ingleses; virtudes e vícios; Escandinávia e Bálcãs; capital e labor; fundamentalistas e modernistas; russos e franco-canadenses; fazendeiros e fabricantes; católicos e protestantes; judeus e gentios; monásticos e livres-pensadores; boêmios e filisteus; bárbaros e gregos; "Big Bill" e King George[233] – todos inter-remendados na mais intricada das colchas de retalhos.[234]

A causa principal dessa confusão populacional eram as migrações. McKenzie, por exemplo, as comparava às invasões biológicas.[235] Para ele, havia dois tipos invasões: aquelas resultantes da utilização territorial – mudança de uma área residencial para uma comercial, ou de uma área comercial para uma industrial – e aquelas referentes aos ocupantes – mudança da população.

As variações populacionais implicavam segregações espaciais de indivíduos de acordo com cor da pele, herança étnica, status socioeconômico, gostos e preferências.

---

[231] THRASHER, Frederic M. "The Study of the Total Situation", *Journal of Educational Sociology*, v. 1, n. 10, 1928, p. 599-612.
[232] PARK, Robert Ezra. "The City: Suggestions for the Investigation of Human Behavior in the City Environment", *op. cit.*, p. 607; WIRTH, Louis. "Urbanism as a Way of Life", *op. cit.*, p. 10.
[233] Conhecido como *Big Bill*, William Hale Thompson (1869-1944) foi prefeito de Chicago de 1915 a 1923 e de 1927 a 1931. *George V* (George Frederick Ernest Albert, 1865-1936) foi Rei do Reino Unido e dos domínios britânicos, e Imperador da Índia, de 1910 até sua morte em 1936.
[234] THRASHER, Frederic M. "The Study of the Total Situation", *op. cit.*, p. 611.
[235] MCKENZIE, Roderick D. "The Ecological Approach to the Study of the Human Community", *op. cit.*

Nascia, nesse período, a importância conferida ao mapeamento do fenômeno criminal. E foi esse método de análise que permitiu aos estudos ecológicos demonstrar que as áreas delinquentes nas comunidades urbanas americanas eram claramente definidas como intersticiais ou adjacentes a centros comerciais e industriais maiores, e que elas tinham características típicas, como deterioração física, população em declínio, baixo status econômico, alta porcentagem de estrangeiros e negros nas populações locais, desorganização de instituições ou grupos inteiros, falta do moral comunitário, colapso do controle social.[236]

Para Park, essa convivência em grupos segregados fazia com que o sentimento de vizinhança se fundisse com antagonismos raciais e interesses de classe.[237] Além disso, ainda segundo ele, a divisão regional permitia que pobres, depravados e delinquentes, aglomerados em uma intimidade insalubre e contagiosa, se autorreproduzissem; assim, a cidade grande oportunizava fossem propagados e desnudados ao público, de uma forma massiva, todos os traços e características que são normalmente obscurecidos e suprimidos em comunidades menores, particularmente aos tipos anormais e excepcionais do homem. A cidade, argumentava Park, em suma, mostra em excesso o bem e o mal na natureza humana.[238]

Analisando os fenômenos da expansão da cidade (agregação urbana ou conurbação que deram ensejo às áreas metropolitanas da cidade), do metabolismo urbano (ou seja, dos processos pelos quais os indivíduos são incorporados à vida de uma cidade)[239] e da mobilidade (o "pulso da comunidade")[240], Burgess argumentou que eles

---

[236] THRASHER, Frederic M. "Ecological Aspects of the Boys' Club Study", *op. cit.*, p. 52.

[237] PARK, Robert Ezra. "The City: Suggestions for the Investigation of Human Behavior in the City Environment", *op. cit.*, p. 582.

[238] *Ibid*., p. 612.

[239] Burgess distingue dois processos pelos quais um indivíduo se torna parte orgânica da cidade. O processo natural decorre do nascimento na cidade e se caracteriza pelo fácil ajustamento ao ambiente social. E é exatamente o índice de crescimento natural que permite medir os distúrbios de metabolismo causados pelo outro tipo de processo, caracterizado pelo excessivo aumento populacional causado por influxos de migrantes, como, no caso estadunidense citado pelo autor, a migração dos negros sulistas às cidades do norte após a guerra. (BURGESS, Ernest Watson. "The Growth of the City: An Introduction to a Research Project", *op. cit.*, p. 53-54.)

[240] Para Burgess, *movimento* não é necessariamente evidência de mudança ou crescimento; ele pode descrever uma ordem de moção fixa e imutável, como no caso de movimento de rotina: o trabalho, por exemplo. (BURGESS, Ernest Watson. "The Growth of the City: An Introduction to a Research Project", *op. cit.*, p. 58.) A *mobilidade* é a mudança de movimento em resposta a um novo estímulo ou situação: a aventura. Quanto a este aspecto, deve-se ter em mente o contexto de então, quando a cidade grande era admirada por suas "luzes brilhantes", seus "empórios de novidades e barganhas", "palácios de diversões", "submundos de vícios e crimes". A conotação com o pulso do corpo humano decorre da interpretação de Burgess de que a mobilidade "é um processo que reflete, e é indicativo de, todas as mudanças que estão acontecendo na comunidade e que é suscetível de análise por elementos que podem ser apresentados numericamente" (*Ibid*., p. 59).

eram acompanhados pelo aumento excessivo de doenças, crimes, desordem, vício, insanidade e suicídio.[241] E, tratando das questões também analisadas por seus contemporâneos, concluía ele: "Onde é maior a mobilidade, e onde, por consequência, falham completamente os controles primários, como na zona de deterioração na cidade moderna, ali se desenvolvem áreas de desmoralização, de promiscuidade e de vício".[242] As áreas de mobilidade coincidiam, portanto, com as regiões onde se identificavam delinquência juvenil, gangues de jovens, crimes, pobreza, abandono de famílias, divórcios etc.

Nem todos, porém, eram tão alarmistas. Diante do diagnóstico da desorganização social, muitos estudiosos reagiam com otimismo; afinal, ao contrário de uma ordem social estática, o dinamismo das relações e a desorganização social eram interpretadas como um prelúdio necessário para a reorganização a partir de uma base de conhecimento mais adequada, ou, nas palavras do próprio Burgess, apresentando o outro lado da moeda, como "um equilíbrio em movimento da ordem social rumo a um fim vaga ou definitivamente considerado como progressivo".[243] Assim também concluía Thrasher: "a desintegração pressagia ajustes mais satisfatórios de estruturas sociais a funções, e uma abordagem mais esclarecida dos problemas de controle social".[244]

E essa reorganização tomou forma em propostas urbanísticas. O arquiteto americano Oscar Newman foi categórico:

> Nós estamos certos de que a construção física de ambientes residenciais pode induzir atitudes e comportamentos por parte dos residentes que contribuem de forma decisiva em prol de garantir sua segurança; que a forma dos edifícios e seus grupamentos permitem que habitantes executem uma função de policiamento significativa, natural a suas rotinas e atividades diárias. Essas funções atuam como importantes restrições contra o comportamento antissocial.[245]

Direta ou indiretamente, Newman foi influenciado pelas inquietações dos sociólogos da geração anterior à sua. E, a partir delas, ele ofereceu uma explicação teórica para a articulação entre um projeto físico e o evento criminoso: tomando como pressuposto que o *design* físico de ambientes residenciais tem forte influência na

---

[241] *Ibid*., p. 57.
[242] *Ibid*., p. 59.
[243] *Ibid*., p. 54.
[244] THRASHER, Frederic M. "The Boy's Club Study", *Journal of Educational Sociology*, v. 6, n. 1, 1932, p. 5.
[245] NEWMAN, Oscar. *Architectural design for crime prevention*. Washington: U.S. Government Printing Office, U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, 1973. p. xii.

ocorrência de crimes e no medo dos residentes quanto ao crime, Newman revelou que certas características de *design* poderiam encorajar as pessoas a estenderem sua esfera de influência além dos confins imediatos de suas unidades de habitação individual, para áreas adjacentes; essa extensão inibiria, assim, a atividade criminal e proporcionaria uma sensação de segurança – de outra forma: a pouca utilização do espaço externo caracterizaria menor controle espacial, o que oportunizaria o aumento do índice de crimes e a majoração do medo.[246] Por exemplo, quanto maior o prédio (o que implica menor controle exercido pelos residentes), maior a incidência de crimes e do medo de crimes.[247]

Para Newman, o efetivo controle do crime seria aquele que acontece preventivamente, e não após o fato.[248] No entanto, diferente de programas de prevenção punitiva (ameaça e possibilidade de punição), o seu programa caracterizava-se como uma prevenção mecânica (colocação de obstáculos na execução criminal) e também uma prevenção corretiva (porque eliminaria as causas do comportamento criminoso).[249]

A partir da seleção do espaço como objeto e da defesa como meio, Newman desenvolveu a teoria do espaço defensível (*defensible space*), o qual tinha por objetivo permitir aos residentes a retomada do controle de seus bairros, a redução dos crimes e o estímulo ao reinvestimento privado de seus espaços.[250] Operacionalmente, o espaço defensível era uma tecnologia arquitetônica fundamentada na autoajuda (envolvimento dos residentes) em vez de na intervenção governamental.[251] De fato, o projeto exigia uma maior participação das potenciais vítimas. Newman argumentava que essa era uma forma de catalisar os naturais impulsos produtivos dos residentes, evitando, pois, que estes abandonassem as responsabilidades sociais compartilhadas e se rendessem a uma autoridade formal, fosse ela a polícia, o administrador, o segurança ou o porteiro.[252] Porém, é importante situá-lo em seu contexto: a perceptível desconfiança que Newman demonstra, nos textos de seus projetos, no que toca à participação governamental na reorganização urbana é própria das décadas marcadas pelo fim das políticas de *welfare*,

---

[246] NEWMAN, Oscar; FRANCK, Karen A. "The Effects of Building Size on Personal Crime and Fear of Crime", *Population and Environment*, v. 5, i. 4, 1982, p. 203-204.
[247] *Ibid*., p. 213.
[248] NEWMAN, Oscar. *Architectural design for crime prevention*, *op. cit.*, p. 17.
[249] *Ibid*., p. 3-4
[250] NEWMAN, Oscar. "Defensible Space: A New Physical Planning Tool for Urban Revitalization", *Journal of the American Planning Association*, v. 61, i. 2, 1995, p. 149-155; *Idem*. *Creating Defensible Space*. Washington: U.S. Department of Housing and Urban Development, Office of Policy Development and Research, 1996.
[251] *Idem*. *Creating Defensible Space*, *op. cit.*
[252] *Idem*. *Architectural design for crime prevention*, *op. cit.*, p. 1.

quando qualquer projeto público encontrava-se vulnerável ao desinteresse do governo ou à retirada da administração pública em meio à execução.

Pelas características socioeconômicas próprias de cada área urbana, os planejamentos exigiam análise e propostas particulares. Ainda assim, pode-se afirmar que, genericamente, a ideia do espaço defensível apresentava duas premissas principais: permitir que residentes pudessem distinguir entre vizinhos e intrusos[253], e evitar crimes premeditados e causados por agentes externos.[254] Em consonância com o viés da Escola de Chicago, a figura do delinquente confundia-se no *outro*.

É possível extrair orientações comuns a projetos diversos, aqui apresentados a título de curiosidade:

- reestruturação das ruas para a criação de minibairros; transformação das vias menores em ruas sem saída, com unificação de acesso (motoristas entram e saem pelo mesmo acesso) e redução do tráfego de veículos, o que reduz rotas de fuga e aumenta a interação entre vizinhos;[255]

- redução do compartilhamento das entradas comuns, pois quanto mais residentes utilizam áreas comuns, mais difícil é a sua reivindicação e a distinção entre residentes e intrusos;[256]

- criação de limites definidores de uma hierarquia de zonas cada vez mais privativas na transição do espaço público para o privado;[257]

- implementação de mecanismos de justaposição de áreas de atividade no interior dos apartamentos com áreas não privadas externas para facilitar a vigilância visual a partir de dentro;[258]

- envidraçamento, iluminação e posicionamento de áreas não privadas e vias de acesso (corredores, escadas, elevadores etc.) para facilitar sua vigilância pelos residentes e autoridades formais;[259]

[253] *Ibid*., p. 9.
[254] *Ibid*., p. 10.
[255] *Idem*. *Creating Defensible Space*, *op. cit.*, p. 41.
[256] *Ibid*., p. 28-29.
[257] *Idem*. *Architectural design for crime prevention*, *op. cit.*, p. 45-48.
[258] *Ibid*., p. 60-64.

- disposição de entradas, vias de acesso, corredores e edifícios de um modo que facilitasse o reconhecimento de origens e destinos ao longo das rotas de circulação;[260]

- justaposição de áreas residenciais com outras instalações funcionais e seguras (comerciais, institucionais, de entretenimento).[261]

2.1.2 Criminologias culturais: geografia cultural

Hayward critica as concepções criminológicas que interpretam o espaço como algo objetivo, ou seja, que se desenvolveram com uma implícita noção de espacialidade que aborda o ambiente meramente como um local geográfico, e não como um produto de relações de poder, de dinâmicas sociais e culturais, ou de significados e valores cotidianos.[262] Sua proposta prioriza o lugar fenomenológico sobre o espaço abstrato, como tentativa de compreender as relações estruturais e culturais que contribuem para o crime e a desordem, e, em consequência, para a segurança da comunidade e sua estabilidade. Por isso, Hayward busca na geografia cultural o fundamento teórico para suas investigações.

Para a geografia cultural, o espaço é entendido quase como se fosse uma coisa viva, um congresso de dinâmicas espaciais, políticas e culturais. Divergindo das ideias um tanto quanto deterministas dos sociólogos urbanos de Chicago, o geógrafo Carl Sauer partiu da premissa, explicitamente antropocêntrica[263], de que era o homem que moldava o ambiente, e não o contrário – podendo, é claro, o ambiente limitar fisicamente a força modeladora da cultura, condicionando possibilidades[264].

Num artigo publicado em 1925 (mesmo ano que Burgess publicou seu *The Growth of the City*), Sauer argumentou que as atividades e qualidades humanas são menos produtos do ambiente do que o uso do espaço pelo próprio indivíduo. Para Sauer,

---

[259] *Ibid*., p. 64-69.
[260] *Ibid*., p. 69-70.
[261] *Ibid*., p. 78-81.
[262] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*
[263] SAUER, Carl Ortwin. "The Morphology of Landscape", *op. cit.*, p. 29.
[264] Isso fica explícito na seguinte passagem de seu texto: "Com a introdução de uma cultura diferente, isto é, alienígena, um rejuvenescimento da paisagem cultural se inicia, ou uma nova paisagem é sobreposta aos remanescentes de uma mais antiga. A paisagem natural é certamente de fundamental importância, pois ela fornece os materiais a partir dos quais é formada a paisagem cultural." (*Ibid*., p. 46).

a paisagem podia ser definida como uma área composta pela associação de formas, tanto físicas quanto culturais[265], reciprocamente influenciadas; por isso, ele se dizia preocupado com a importância do lugar para o homem, e também com sua transformação do lugar.[266] Reconhecendo os homens como agentes distintos de modificação[267], Sauer estabelecia uma distinção entre paisagem natural e paisagem cultural. "A paisagem natural", escreveu ele, "está sendo sujeita a transformação nas mãos do homem, o último e, para nós, o mais importante fator morfológico. Por meio de suas culturas, ele faz uso das formas naturais, em muitos casos as altera, em alguns, as destrói".[268] Por sua vez, a definição de paisagem cultural não se relaciona com energia, costumes ou crenças do homem, mas com o seu registro sobre a paisagem.[269] Deriva dessa compreensão a sua famosa declaração: "A paisagem cultural é modelada a partir de uma paisagem natural por um grupo cultural. A cultura é o agente, a área natural é o meio, a paisagem cultural, o resultado".[270]

Com esse viés e com foco de análise nos particularismos culturais, na atividade geográfica humana, na leitura dos espaços em termos de sua história e sua antropologia cultural, Sauer estabeleceu os conceitos axiomáticos da geografia cultural. Dessa proposição declinou-se uma *nova* geografia cultural, com suas variantes politicamente carregadas e diversificadas (Denis Cosgrove, James Duncan e Peter Jackson), a qual pode ter considerável utilidade para as criminologias contemporâneas. Hayward[271] explicita algumas possibilidades:

> - É inegável que uma das vantagens do mapeamento é a fácil produção de resultados quantificáveis, geralmente na forma de estatísticas policiais. "Essas estatísticas, por sua vez", argumenta Hayward, "contribuem para um enquadramento mais amplo de redes governamentais baseadas em torno de abordagens atuariais e calculistas para o controle e o gerenciamento ('de risco') de problemas sociais".[272] Nesse contexto, porém, o espaço urbano torna-se um foco somente de análise estatística, um lugar de auditoria e campo de testes para novas iniciativas políticas. Assim, se a criminologia

[265] *Ibid*., p. 25-26.
[266] *Ibid*., p. 53.
[267] *Ibid*., p. 37.
[268] *Ibid*., p. 45.
[269] *Ibid*., p. 46.
[270] *Ibid*., p. 46.
[271] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*, p. 448-449.
[272] *Ibid*., p. 445.

ecológica, com suas práticas de mapeamento e policiamento de áreas com altos índices de criminalidade (*hot spot policing*), é falha em considerar a intricada natureza do espaço e a complexidade das ações humanas dentro do espaço, a nova geografia cultural pode oferecer corretivos úteis.

- Segundo: a nova geografia cultural pode também melhorar investigações criminológicas quanto ao significado, ao poder e à economia política em razão da ênfase que deposita na natureza espacial das influências políticas e econômicas e no modo como paisagens funcionam como sistemas de reprodução social.

- Por fim, ela pode auxiliar as criminologias hodiernas a abandonarem seu estado intelectual isolado e a lidarem com as várias transformações socioeconômicas e culturais descritas como *modernidade tardia*, a partir da utilização de teorias sociais contemporâneas e de interdisciplinaridade.

As criminologias ecológicas e culturais demonstram como o espaço pauta as relações humanas e evidenciam o seu relevante papel na etiologia e no controle dos comportamentos desviantes. Todavia, podemos também considerar este novo espaço virtual, o ciberespaço, como um dispositivo que estrutura e condiciona os comportamentos dos atuantes – em especial: os crimes, desvios e ameaças?

2.2 O CIBERESPAÇO

> Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no não espaço da mente, aglomerados e constelações de dados. Como luzes da cidade, se afastando...[273]

O termo ciberespaço foi cunhado por William Gibson. Primeiro apareceu no conto *Burning Chrome*[274], mas a expressão realmente se difundiu a partir da publicação de seu romance de ficção científica *Neuromancer*[275]. Neste livro, o ciberespaço se revela como um espaço virtual, protegido por baluartes de softwares, modelo que serviu de inspiração para o filme *Matrix* (1999).

O vocábulo foi logo apropriado pela tecnologia de informação para denotar o espaço virtual e contrastar com o mundo real (ou *materespaço*[276]). No entanto, não se pode pensar o ciberespaço por meio de uma simples analogia, uma substituição ou uma assimilação do espaço territorial. Isso seria o equivalente a tentar materializar o imaterial.[277]

> O *mundo ciberespacial* é composto e constitui-se não pelo *espaço* ou *tempo* que ocupa, mas pelo intercâmbio das *informações* – permuta de dados e comunicabilidade inter-significativa –, propulsionado pela *energia colateral* teleológica de sistemas vivos (seres humanos e sociedade).[278]

Essencialmente, o ciberespaço é *virtual*. Mas, esse predicado oculta conotações distintas, que podem até se fundir para um caso concreto.[279]

O primeiro e mais tradicional sentido de *virtual* é filosófico: aquilo que existe em potência, e não presentemente. Trata-se de uma importante dimensão da realidade.

---

[273] GIBSON, William. *Neuromancer*. trad. Fábio Fernandes. 4. ed. São Paulo: Aleph, [1984] 2008. p. 77.
[274] GIBSON, William. "Burning Chrome", *Omni*, jul 1982, p. 72.
[275] *Idem*. *Neuromancer*, *op. cit.*, *passim*.
[276] Colli emprega *materespaço* para se referir ao ambiente material, em oposição ao *ciberespaço*. (COLLI, Maciel. *Cibercrimes*, *op. cit.*, p. 24.) O autor é prudente em declarar que o neologismo não pretende separar categoricamente dois espaços, tornando um a negação do outro; sua utilização tem o propósito didático de reforçar as distinções dos dois ambientes que, como se verá no decorrer desta tese, se relacionam mútua e continuamente.
[277] *Ibid*., p. 24.
[278] *Ibid.*, p. 25, grifos no original.
[279] LÉVY, Pierre. *Cyberculture*, *op. cit.*

Há aqui uma questão temporal: o virtual precede sua concretização efetiva ou formal: a árvore está virtualmente presente na semente.[280]

No segundo sentido, mais comum, *virtual* caracteriza a *irrealidade* – considerando que por realidade se compreende a materialização, a presença tangível. Diferente do sentido filosófico – no qual, o virtual se opõe ao presente, não ao real –, esse sentido mais ordinário pressupõe que algo é real ou virtual, não podendo possuir ambas as qualidades ao mesmo tempo. Essa distinção é clara em uma passagem de *Neuromancer*: "O ciberespaço, conforme o deck apresentava, não tinha nenhuma relação especial com a localização física do deck".[281] Virtual é algo falso, ilusório, imaginário, possível.[282] Sob esse aspecto, a expressão *realidade virtual* revela-se um oximoro: ao combinar palavras de sentidos opostos, que parecem excluir-se mutuamente, tem-se um efeito contrário que, no contexto, reforça a expressão – nesse caso, de incorporeidade e intangibilidade. Nesse sentido, a informação digital (a notação binária) pode ser qualificada como virtual à medida que é inacessível à leitura humana imediata; somente pelo seu processamento é que ela se apresenta à interação humana: códigos binários ilegíveis concretizam-se em textos legíveis, em imagens visíveis e em sons audíveis.[283]

O terceiro sentido, conforme compreendido pelos sistemas de informação ou pelo viés tecnológico específico, estabelece que, no sentido "mais forte" do termo, a realidade virtual se refere a um tipo particular de simulação interativa na qual o explorador tem a sensação física de estar imerso em uma situação definida por um banco de dados.[284] Na concepção da tecnologia da informação, em sentido "fraco", um mundo virtual é um universo de possibilidades que podem ser calculadas a partir de um modelo digital – quando as interações com a realidade virtual são capazes de enriquecer ou modificar o modelo, o mundo virtual se torna um vetor de inteligência e criação coletivas.[285]

A partir de qualquer uma dessas acepções da virtualidade do ciberespaço, fica evidente que o ciberespaço não é uma infraestrutura técnica para telecomunicação (aparelhos, *softwares*, cabos de fibra ótica, a internet), mas o acontecimento da transmissão de informação e o tipo peculiar de relacionamento entre pessoas. Nas

[280] *Ibid.*, p. 29.
[281] GIBSON, William. *Neuromancer*, *op. cit.*, p. 134.
[282] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 56.
[283] *Ibid*., p. 30.
[284] *Ibid*., p. 52.
[285] *Ibid*., p. 56-57.

palavras de Lévy, trata-se de "um certo modo de usar infraestruturas existentes e explorar recursos e é baseado em uma incessante inventividade distribuída que é indissoluvelmente técnica e social".[286]

Essa imaterialidade estrutural fica ainda mais evidente com o desenvolvimento das "nuvens" para o armazenamento de dados: em vez de se utilizar o armazenamento físico de conteúdo (discos rígidos), as informações do ciberespaço estão hoje disseminadas em diversos servidores no mundo, em plataformas corporativas (Dropbox, Google Drive, iCloud, OneDrive) e nas redes sociais (Facebook, Instagram, Twitter), reforçando a concepção de um acontecimento nodal.[287]

Se não é a infraestrutura, o ciberespaço tampouco é o conteúdo (isto é, o consumo de informação e de serviços interativos). Para Lévy, o ciberespaço se constitui com a participação em um processo social de inteligência coletiva. Em suas palavras:

> A maneira como o ciberespaço se desenvolveu sugere que ele não é um território convencional ou uma infraestrutura industrial, mas um processo tecnossocial auto-organizado, finalizado, a curto prazo, por um imperativo categórico de conectividade (a interconexão sendo um fim em si) que se esforça por um ideal de inteligência coletiva, que, em grande medida, já foi implementada. A relação entre o ciberespaço e a cidade, entre a inteligência coletiva e o território, é essencialmente uma questão de imaginação política.[288]

Para a melhor compreensão, pense-se em uma tecnologia mais antiga: foi a técnica postal desenvolvida a partir do século XVII que constituiu uma inovação comunicativa que transformou as relações entre indivíduos, e não a mera mensagem escrita ou o serviço do mensageiro.[289]

Ciberespaço é, portanto, o "espaço de comunicação, acessível através da interconexão global de computadores e memórias de computadores".[290] Nessa definição, Lévy inclui todos os sistemas eletrônicos de comunicação, na medida em que eles transmitem informação a partir de fontes digitais ou de fontes destinadas à digitalização.[291] Ou seja, não é um espaço de interconexão somente de computadores, mas de um número crescente de aparelhos interativos.

---

[286] *Ibid*., p. 174-175.
[287] PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*: developing a theoretical model for understanding criminal behaviour on the internet. 2015. 333 f. Tese (Doutorado em Filosofia) – The University of Huddersfield, Huddersfield, 2015. p. 27.
[288] LÉVY, Pierre. *Cyberculture, op. cit.*, p. 175.
[289] *Ibid*., p. 104.
[290] *Ibid*., p. 74.
[291] *Ibidem*.

O processo de convergência é uma chave importante para a compreensão da ampliação e da infiltração do ciberespaço no cotidiano social, da modelagem das experiências e dos comportamentos individuais, e, no que interessa a essa tese, da transformação das oportunidades e das condutas desviantes na era da informação. Ele pode ser definido como "a capacidade de diferentes plataformas tecnológicas (em rede), tais como aparelhos de consumo (telefone, televisão e computadores pessoais), de proporcionar tipos similares de serviços".[292] Sob a perspectiva do produto, esse processo agrega um valor (a rede de informação) que não havia sido previsto quando cada uma dessas tecnologias foi criada. Sob a perspectiva do consumidor, a interfuncionalidade dos produtos aumentou e aperfeiçoou nossa capacidade de construir novas redes sociais.[293]

O desenvolvimento de uma arquitetura de comunicação em rede fez com que os computadores deixassem de ser centros de recebimento, armazenamento, processamento e envio de dados, e tornou cada um deles em nodos, terminais, componentes atomizados de uma rede tecnocósmica. Eventualmente, argumentou Lévy, haverá somente um computador, mas nos será impossível localizar suas fronteiras ou determinar seus contornos.[294] Sem circunferência, com centro em todos os lugares: este é o próprio ciberespaço.

Neste ponto, é necessário fazer um esclarecimento: em si, nem a *internet*, nem a *world wide web* (WWW) constituem *redes de computadores*, tecnicamente falando. A internet é um agrupamento de redes de computadores, ou a rede das redes – por isso, muitos se referem a ela como *the Net*.[295] A *world wide web* é um sistema distribuído (*distributed system*), ou um caso de computação distribuída, um agrupamento de computadores independentes e passíveis de identificação individualizada que compartilham uma "linguagem comum" por meio da qual é transmitida informação e que aparecem aos atuantes como se fosse um único sistema coerente.[296] Nesta tese, entretanto, a referência à comunicação em rede terá um sentido mais genérico, compreendendo a internet, a WWW e toda comunicação convergente originada da tecnologia da informação.

---

[292] WALL, David S. *Cybercrime*, *op. cit.*, p. 35.
[293] *Ibidem*.
[294] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 26.
[295] YAR, Majid. "Online Crime", *op. cit.*
[296] COLLI, Maciel. *Cibercrimes*, *op. cit.*, p. 43; YAR, Majid. "Online Crime", *op. cit.*

No que toca à suas características, para Lévy, o ciberespaço é *universal sem totalidade*.[297] Ou melhor, à medida que se expande, o ciberespaço se torna mais *universal* e o mundo da informação menos *totalizante*. Se a sentença causa incômodo, é porque os conceitos não estão claramente definidos ou porque há uma confusão entre eles. A filosofia pós-moderna, afirma Lévy, "cometeu o erro de jogar fora o bebê do universal com a água de banho da totalidade".[298] O ciberespaço é universal, não porque esteja *de fato* em todos os lugares, mas porque sua ideia ou sua forma envolve todos os seres humanos *por direito*, sem um centro determinado e sem diretrizes. Enfim, *universal* é a virtual presença da humanidade para si própria. E, por *totalizante*, Lévy caracteriza o encerramento semântico, a unidade da razão, a redução a um denominador comum, a coleção estabelecida de sentidos de uma pluralidade (de discursos, situações, eventos, sistemas etc.), como, por exemplo, a comunicação produzida pela mídia de massa.

Isso não significa que a universalidade do ciberespaço seja neutra ou inconsequente – e, como se verá a seguir, a sua constituição e as suas repercussões políticas, sociais e econômicas provam que não se pode atribuir neutralidade a esse ou qualquer espaço.

2.2.1 A neutralidade do ciberespaço

...the street finds its own uses for things[299].

O espaço físico não é neutro. Harvey sugere que o mapeamento do mundo já dera provas de que o espaço era pouco neutro ideologicamente, em particular porque abriu caminho para que se considerasse o espaço algo disponível à apropriação para usos privados, fosse pela percepção dos poderes individuais e locais num quadro de lealdades nacionais, fosse pela tomada de posse conceitual e visual efetiva do reino físico e sua relação com o resto do globo.[300] Mas, não é necessário ir tão longe assim. Toda a história da organização territorial demonstra como forças (políticas, ideológicas, econômicas) formataram o mundo: colonização e imperialismo, contradições urbano-

[297] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 91-102.
[298] *Ibid*., p. 102.
[299] GIBSON, William. "Burning Chrome", *op. cit.*, p. 106.
[300] HARVEY, David. *Condição pós-moderna*, *op. cit.*, p. 209.

rurais, conflitos geopolíticos.[301] As teorias criminológicas ecológicas e culturais (itens 2.1.1 e 2.1.2) também evidenciaram o arranjo de poderes e dinâmicas dos espaços urbanos, indicando que planejamentos, arquiteturas, gestões e usos da cidade estão imbuídos de interesses múltiplos.

O ciberespaço, por sua vez, é neutro? Se por um viés, as redes virtuais são o equivalente contemporâneo de sociedades sem Estado, por outro e óbvio, não pode se referir à ausência de organização social: o ciberespaço tem uma estrutura, distribuição de poder e normas.[302]

Tampouco se pode entender a suposta neutralidade por uma ausência de valores, porque toda tecnologia, conforme afirma Snyder, incorpora certas presunções sobre as relações sociais.[303] Dant argumenta que objetos sem vida não têm qualquer intencionalidade própria; no entanto, uma das características dos objetos artificiais é que eles são feitos por pessoas que têm intenções, e essas intenções são projetadas e convertidas no objeto: "Nesse sentido, todos não-humanos se tornam imbuídos com intencionalidade humana; armas são destinadas para matar, carros para condução".[304] Além disso, toda novidade tecnológica porta um aspecto revolucionário: quase não há nova invenção que apareça e seja proclamada a salvação para uma sociedade livre.[305]

Apesar desses argumentos, Winner é cauteloso quanto a isso.[306] É inquestionável que o desenvolvimento tecnológico – expresso nos mais diversos sistemas: indústria, guerra, comunicações – alterou fundamentalmente o exercício de poder e a experiência da cidadania. No entanto, critica ele, ir além dessa constatação e argumentar que certas tecnologias têm *em si* propriedades políticas parece completamente equivocado. Para Winner, descobrir virtudes e vícios em agregados de ferro, plástico, químicos, transistores e circuitos integrados é uma maneira de mistificar artifícios humanos e evitar as reais origens dos problemas; o que importa, diz ele, a partir de uma teoria que poderia ser chamada de *determinação social da tecnologia*, não é a tecnologia em si, mas o sistema social ou econômico no qual ela está inserida.

---

[301] *Ibid*., p. 217.
[302] SNYDER, Francis. "Sites of Criminality and Sites of Governance", *Social & Legal Studies*, v. 10, i. 2, 2001, p. 251-256.
[303] *Ibid*., p. 251.
[304] DANT, Tim. "The Driver-car", *Theory, Culture & Society*, v. 21, n. 4/5, 2004, p. 71.
[305] WINNER, Langdon. "Do Artifacts Have Politics", *Daedalus*, v. 109, n. 1, Modern Technology: Problem or Opportunity?, 1980, p. 122; *Idem*. *The whale and the reactor*: a search for limits in an age of high technology. Chicago: The University of Chicago Press, 1986. p. 20.
[306] WINNER, Langdon. "Do Artifacts Have Politics", *op. cit.*; Idem. *The whale and the reactor*, *op. cit.*, p. 19-39.

Contudo, evitando uma generalização teórica, Winner reconhece uma corrente de pensamento – que ele chama de *teoria da política tecnológica* –, cuja abordagem identifica certas tecnologias como fenômenos políticos, a qual não substitui a sua proposição, mas a complementa. Nesse sentido, ele destaca e ilustra duas formas nas quais artefatos podem conter propriedades políticas.

Primeiro, são os casos em que a invenção, o *design* ou o arranjo de uma técnica específica (o saber ou o aparelho) se torna um modo de resolver uma questão de uma comunidade particular, como dão prova as histórias da arquitetura, do planejamento urbano e das obras públicas. Nesse caso, o aparelho é projetado ou construído de um tal modo (maior flexibilidade) que produz um conjunto de consequências lógica e temporalmente antes de qualquer de seus usos declarados.

Segundo, são os casos de sistemas fabricados que parecem exigir ou ser fortemente compatíveis com tipos particulares de relações políticas – e que, por isso, poderiam ser chamados de *tecnologias inerentemente políticas* –, nos quais não há genuínas possibilidades de intervenção que possa mudar a intratabilidade do ente ou alterar significativamente qualidade de seus efeitos políticos, como é o caso (extremo) da bomba atômica ou daquelas tecnologias nas quais certas razões de necessidade prática, amplamente aceitas, tendem a eclipsar outros tipos de raciocínio político ou moral.

Essas interpretações se assemelham àquela de Sauer quanto ao poder de modificação da paisagem natural pelas pessoas e pela cultura (ver p. 76-77 desta tese).

A partir de um ponto de partida distinto, Lawrence Lessig, fundador da Creative Commons, aproxima-se das proposições da teoria da política tecnológica, ao identificar propriedades políticas na experiência tecnológica do ciberespaço.[307] Lessig parte do pressuposto de que os comportamentos no mundo real são regulados por quatro tipos de restrições:[308]

[307] LESSIG, Lawrence. *The laws of cyberspace*, *op. cit.*
[308] *Ibid*., p. 2-3.

- a *lei*[309] regula comportamentos por meio de sanções impostas *ex post*;

- as *normas sociais* os regulam através de expectativas e reações dos participantes da comunidade, de um modo descentralizado, porém mais amplo;

- o *mercado* regula os comportamentos pelo preço, estabelecendo oportunidades e restrições;

- por fim, há uma regulação imposta pela *arquitetura*, isto é, a limitação imposta pelo espaço da forma como o encontramos.

Esses quatro tipos também regulam os comportamentos no ciberespaço: há leis que protegem direitos, proíbem ou determinam condutas específicas; há uma norma de comportamento comum e não escrito, que avalia práticas e oportuniza sanções; há operações de mercado que determinam acessos e limitações; e há uma arquitetura própria do ciberespaço, que Lessig chama de *código*.

Por código, ele compreende o conjunto de protocolos e de regras codificadas e implementadas que determinam como as pessoas interagem (ou, existem) nesse espaço. Tal como uma estrutura arquitetônica sujeita o comportamento humano, o código estabelece restrições e permissões compulsórias – salvo para *hackers*.[310]

A arquitetura é política. No ciberespaço, em específico, a seleção de uma arquitetura é tão importante quanto a escolha de uma constituição. Pois, em um sentido fundamental, o código do ciberespaço é sua constituição; um conjunto de protocolos – onipresente, onipotente, suave, eficiente, crescente[311] – que regulamenta e controla os comportamentos[312]. (Retome-se aqui o que foi dito sobre a prevenção mecânica de Newman, na p. 74 desta tese.) Para Lessig, notório ativista da liberdade de informação, o ciberespaço experimenta o conflito de escolha entre arquiteturas de controle e arquiteturas de liberdade. Em sua opinião, se valores constitucionais implicam a arquitetura do ciberespaço, eles devem orientar os projetos desse espaço e limitar os

[309] Em ambos os espaços, a *lei* impõe uma regulação direta (ameaça ou aplicação de sanção) tal como uma regulação indireta por meio das outras modalidades regulatórias: a lei pode regular normas, mercados e arquiteturas. (*Ibid*., p. 11.)
[310] *Ibid*., p. 4.
[311] *Ibid*., p. 16.
[312] *Ibid*., p. 9.

tipos de regulação que essa arquitetura permite.[313] Se a arquitetura do ciberespaço, sua codificação constitucional, possibilita valores políticos, ela é essencialmente política, o que impede uma atribuição de neutralidade.

Nesse sentido, escreveu Sérgio Amadeu da Silveira:

> É a lembrança de que o poder não se faz por meio da tecnologia somente, mas está embutido na própria tecnologia. Redes digitais e seus dispositivos não são neutros. Seus arranjos e limites embarcados em protocolos e códigos são programados para cumprir determinações, muitas vezes de ordem geoestratégica, política e econômica. Um algoritmo do Google ou do Facebook funciona de um determinado modo não porque não haveria outra forma de funcionar, mas porque foi concebido daquele modo.[314]

Mas, de que forma se arquiteta o ciberspaço?

2.2.2 A arquitetura do ciberespaço

Lessig é um constitucionalista por formação. E é importante esclarecer que quando ele utiliza o termo "constituição", ele não se refere ao texto legal. Ele próprio esclarece que seu conceito de constituição se assemelha mais ao modelo britânico – do que ao americano (e ao nosso) –, sendo constituição uma arquitetura que estrutura e limita o poder social e legal, com o fim de proteger valores fundamentais.[315] Por isso, afirma Lessig: "Deixado por conta própria, o ciberespaço se tornará um perfeito instrumento de controle".[316]

E ele cita quatro aspectos da arquitetura do ciberespaço: regulabilidade, regulação pelo código, soberanias concorrentes e ambiguidade latente.

2.2.2.1 Regulabilidade

Aquilo que no mundo real caracteriza a capacidade de um governo de regular o comportamento dentro de sua jurisdição, no ciberespaço a regulabilidade identifica a habilidade do governo em regular seus cidadãos enquanto estão atuando na internet.[317]

---

[313] *Ibid*., p. 10.
[314] In ASSANGE, Julian. *Quando o Google encontrou o Wikileaks*. trad. Cristina Yamagami. São Paulo: Boitempo, 2015. p. 11.
[315] LESSIG, Lawrence. *Code*: version 2.0, *op. cit.*, p. 4.
[316] *Ibidem.*
[317] *Ibid*., p. 23.

Enquanto a primeira geração de operadores, ativistas e críticos do ciberespaço defendia que esse ambiente virtual era um espaço sem controle possível, perspectivas mais recentes têm sugerido o contrário. Lessig indica que pode resultar em falácia a confusão entre o que algo *deveria ser* e o que algo *é*.[318] O ciberespaço é construído.[319] E, por isso, suas características dependem de sua constituição, que é dinâmica. "A arquitetura original da internet tornava a regulação extremamente difícil. Mas aquela arquitetura original pode mudar. E todas as evidências do mundo indicam que está mudando".[320]

2.2.2.2 Regulação pelo código

Considerando que há uma regulação de comportamentos na internet e no ciberespaço, essa regulação é imposta primeiramente por meio de um código. De acordo com Lessig, a tecnologia não apenas influencia a estrutura regulatória, mas ela é em si – a partir de seus códigos constituintes – uma estrutura regulatória. A regulabilidade do ciberespaço depende de certas arquiteturas de autenticação, que é o reconhecimento de que uma informação é verdadeira, o que, por sua vez, depende do código.[321]

2.2.2.3 Soberanias concorrentes

Contudo, que soberania irá regular/governar o ciberespaço e a internet? Se, na década de 1990, os pioneiros da internet tinham razões ideológicas para resistir aos mandos dos governos, a realidade das transações contemporâneas evidencia um novo contexto, que Geist denomina de *Código 2.0*.[322] Na medida em que a programação dos códigos se torna comercial e produto em menor número de grandes empresas, aumenta a capacidade governamental de regulação.[323] Lessig explica que o mercado promove a regulabilidade, no sentido de que as tecnologias que tornam o comércio mais eficiente são também as tecnologias que tornam mais fácil a regulação da internet ao induzir o

---

[318] *Ibid*., p. 32.
[319] *Ibid*., p. 31.
[320] *Ibid*., p. 32.
[321] *Ibid*., p. 24, 40, 42.
[322] GEIST, Michael. "Cyberlaw 2.0", *op. cit.*
[323] LESSIG, Lawrence. *Code*: version 2.0, *op. cit.*, p. 71.

desenvolvimento de uma arquitetura que torna o comportamento *mais* regulável – não *perfeitamente* regulado.[324]

Enquanto há uma função própria e comum do código (usar comandos para controlar), há, todavia, dois tipos de códigos. O primeiro tipo de código denota a técnica, tão antiga quanto o próprio governo, pela qual um congresso legisla: temos códigos civis, penais, tributários, de trânsito etc. O segundo tipo de código é aquele elaborado por programadores, concretamente representado por instruções embutidas em discos rígidos e programas que fazem o ciberespaço funcionar. O que Lessig afirma é que o primeiro tipo de código pode afetar o segundo: "Quando o comércio escreve um código, então o código pode ser controlado, porque entidades comerciais podem ser controladas. Assim, aumenta o poder legislativo sobre o programador conforme o código legislativo se torna cada vez mais comercial."[325-326]

E por esse argumento não se deve concluir que a governança tem uma oportunidade unicamente comercial. Considerando que o código codifica valores – ainda que muitos insistam, ingenuamente, a lhe atribuir uma neutralidade legislativa ou resumi-lo a um problema de engenharia –, é de interesse do governo aproveitar uma oportunidade alternativa de afetar a arquitetura do ciberespaço com importantes valores públicos: "Se o mercado vai definir as arquiteturas emergentes do ciberespaço, não é função do governo assegurar que aqueles valores públicos que não são de interesse comercial também estejam incorporados na arquitetura?".[327]

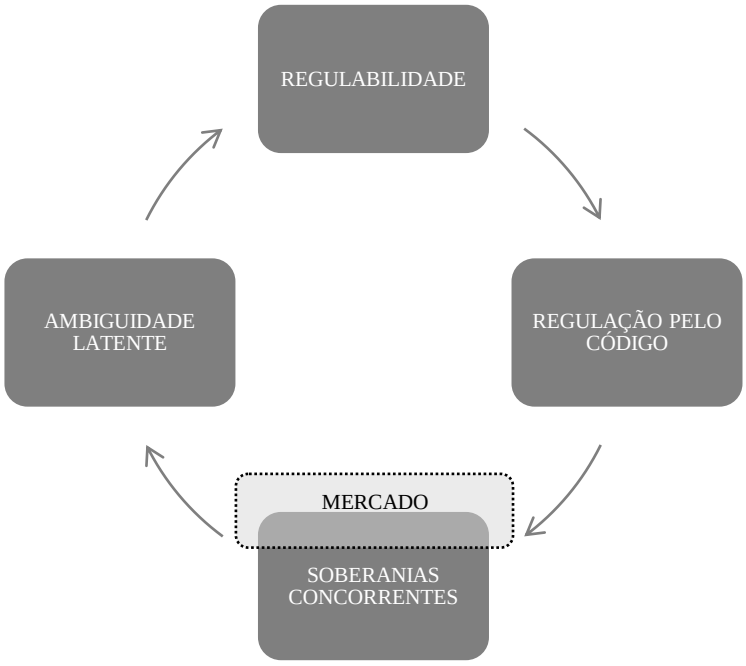
2.2.2.4 Ambiguidade latente

O ciberespaço apresenta constantes ambiguidades. Ele impõe questões de como melhor prosseguir, afirma Lessig: "Nós temos ferramentas do espaço real que nos ajudarão a resolver questões interpretativas ao nos indicar uma ou outra direção, ao menos algumas vezes. Mas, no fim, as ferramentas nos guiarão ainda menos do que o fazem nos espaço e tempo reais".[328]

---

[324] *Ibid*., p. 57, 61-62.
[325] *Ibid*., p. 72.
[326] Lessig (*Ibid*.) chama de *East Coast Code* (código da costa leste) o código legislativo elaborado em Washington, D.C., e de *West Coast Code* (código da costa oeste) o código desenvolvido no Vale do Silício (*Silicon Valley*), Califórnia. Na transcrição original, lê-se: "(...) *Thus, the power of East over West increases as West Coast Code becomes increasingly commercial*."
[327] *Ibid*., p. 77-78.
[328] *Ibid*., p. 25.

A dinâmica dos aspectos da arquitetura do ciberespaço pode, então, ser assim esquematizada:



3 ATUANTES

3.1 PERTURBADORES DO *STATUS QUO*

Diferente do mito do *hacker* com habilidades sobre-humanas que desafia Estados e grandes corporações, perpetuado pelas obras literárias e cinematográficas, a realidade mostra que os atuantes do ciberespaço combinam suas motivações e emoções próprias, com habilidades e conhecimento avançado sobre sistemas de comunicação e com estratégias de acesso à informação que transita ou está armazenada no ciberespaço.

Neste espaço virtual, estabeleceram-se regras consuetudinárias de comportamento – chamadas, em seu conjunto, de *netiquette* por Lévy[329] – que foram desenvolvidas entre os usuários da internet: a defesa da liberdade de expressão e a correspondente condenação à censura, a promoção da autonomia, a abertura à alteridade, o compartilhamento de informações, a evitação de propagandas em espaços não comerciais, a inibição de ofensas, o respeito à delimitação temática de um determinado fórum de discussões.[330] Essa moralidade implícita que governa as relações cibernéticas pauta-se, genericamente, na reciprocidade.

Com fundamento nesse compromisso ético, desenvolveu-se uma distinção entre os dois tipos de atuantes no ciberespaço: *hackers* alegam ser motivados por esses princípios éticos, ao passo que *crackers* não. No entanto, mesmo essa distinção não pode ser tomada como absoluta. A motivação dos *hackers*, por exemplo, gerou uma outra divisão, desde sua origem bastante confusa, entre *white hat hackers* e *black hat hackers*: aqueles mantêm as tradições éticas do *hacking* de liberdade de acesso à informação pública, enquanto estes são motivados por questões financeiras ou vingança. Noutra possível taxonomia, é possível argumentar que esses mesmos atuantes podem ser utópicos (aqueles que acreditam que estão contribuindo com a sociedade ao demonstrar suas vulnerabilidades – uma autojustificação em vez de uma convicção) ou *cyberpunks* (que são agressivos contra o *status quo* e voluntariamente causam danos aos alvos que rejeitam).

Todavia, categorizá-los num maniqueísmo de bons e maus atuantes não parece ser, portanto, apropriado e de qualquer modo proveitoso. O que parece ser óbvio é que esses atuantes, responsáveis por crimes, desvios ou novas ameaças, independentemente

---

[329] LÉVY, Pierre. *Cyberculture*, *op. cit.*, p. 108.
[330] *Ibid*., p. 108-109, 112.

das titulações que lhes sejam atribuídas, são perturbadores do *status quo*, da ordem programada, esperada, vigente e imposta no ciberespaço. Assim, ainda que devamos conferir ao termo *hacker* todas as conotações subversivas, marginais, anti-*establishment*, como afirma Žižek[331], porque, ao fim e ao cabo, esses atuantes visam perturbar o funcionamento suave e tranquilo das grandes empresas burocráticas, isso não pode resultar numa condenação sumária e absoluta de suas atividades, uma vez que, como já registraram muitas vezes a sociologia e a criminologia, esses mesmos comportamentos criminosos, desviantes e ameaçadores podem trazer consigo uma revolução positiva de paradigmas. Basta que se recorde como *hackers* revolucionaram o mercado de computadores pessoais, a relação das pessoas com produtos artísticos e de entretenimento, e até mesmo contribuíram para movimentos sociais.

3.2 TEORIAS CRIMINOLÓGICAS ADAPTÁVEIS

No tópico 2.1.1, acima, foi destacada a importância que a Escola de Chicago teve no desenvolvimento das teorias ecológicas do crime, nas quais a arquitetura espacial teve um papel fundamental no fenômeno criminal. Um outro aspecto da Escola de Chicago foi o foco etnográfico no mundo privado do desviante (jovens, gângsteres, *hobos*), o que exigiu métodos de pesquisa revolucionários, como a *observação participante* e a *história de vida*.[332] Aqui são destacadas algumas das teorias que daí decorreram e que podem servir de modelo, desde que adaptadas, para futuros desenvolvimentos criminológicos dos atuantes *cyber*.

Para que fique registrado um novo campo de pesquisa, merecem referência as explicações biológicas. Siegel, por exemplo, sugere que os *cybercrimes* demandam um grau de autocontrole e dedicação, algo que uma pessoa muito impulsiva ou mentalmente instável teria dificuldade de conseguir.[333] Nesse sentido, a análise psicológica de muitos dos notórios *hackers* revela que eles são portadores da síndrome de Asperger, uma condição neurológica do espectro autista caracterizada por dificuldades significativas na interação social e comunicação não-verbal, com padrões de comportamento repetitivos e interesses restritos. Essas explicações, entretanto, estão excluídas deste capítulo porque as pesquisas são ainda muito incipientes.

---

[331] ŽIŽEK, Slavoj. *Violência*: seis reflexões laterais. trad. Miguel Serras Pereira. São Paulo: Boitempo, 2014. p. 28.
[332] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*, p. 445.
[333] SIEGEL, Larry J. *Criminology*, *op. cit.*, p. 469.

3.2.1 Delinquência juvenil: conflito cultural

Em resposta à ideia de um conflito cultural, Sykes e Matza argumentaram que os valores por trás da delinquência juvenil são muito menos desviantes do que eles são comumente retratados e que esse retrato imperfeito decorre de uma supersimplificação grosseira do sistema de valores da classe média.[334] Os autores relataram que há três temas principais que aparecem regularmente nos textos sobre a delinquência juvenil:

- Jovens delinquentes estão profundamente imersos em uma incansável busca por excitação, emoção ou estímulo, que não são facilmente satisfeitos através de meios legítimos de recreação organizada. Inclusive, a possibilidade de uma atividade envolver a infração legal é precisamente o que geralmente infunde um ar de excitação.[335]

- Jovens delinquentes frequentemente demonstram certo desdém em "se sair bem" no domínio do trabalho, convencendo-se que só os otários trabalham e que, por isso, o regime de trabalho de fábricas, lojas e escritórios deve ser evitado.[336]

- Jovens delinquentes apresentam uma hostilidade fundamental, um impulso em lesionar e destruir, que se manifestam em ataques verbais e físicos. A utilização de violência pode ainda expressar, de uma forma extrema, que a agressão é uma demonstração de força e, portanto, masculinidade.[337]

Todavia, os elementos da busca excitação, do desdém ao trabalho e da violência também estão presentes na cultura social dominante e adulta.[338]

O desejo por aventura, por exemplo, manifesto nos atos de atrevimento ou na busca por excitação, são aceitáveis e desejáveis, como uma diversão oposta à rotina, mas desde que confinadas a determinadas circunstâncias como esportes, recreação e feriados. (No caso das festas de feriados, os cânones convencionais são interpretados

[334] SYKES, Gresham M.; MATZA, David. "Juvenile Delinquency and Subterranean Values", *American Sociological Review*, v. 26, n. 5, 1961, p. 713.
[335] *Ibid*., p. 713.
[336] *Ibid*., p. 714.
[337] *Ibid*., p. 714-715.
[338] *Ibid*., p. 716-717.

bastante frouxamente, e a maioria das sociedades parece dar espaço, de uma ou outra forma, a periódicas anomias, como reflexos saturnais.)

O mesmo pode ser dito sobre a relativização do valor do trabalho, sendo perceptível que, em todas as classes, houve uma flexibilização da ética protestante do trabalho.

E, quanto às atitudes sociais com relação à violência, é bastante evidente o gosto por ela, característico nos livros, filmes e programas que a retratam, cada vez mais explicitamente. (Além do fato de que a ideia crucial de força e masculinidade ser amplamente aceita em muitos pontos no sistema social.)

Para os dois autores, portanto, o "delinquente simplesmente traduz em comportamento aqueles valores que a maioria geralmente é muito tímida para expressar".[339] Parafraseando a alquimia moral citada por Merton[340], Sykes e Matza[341] sugerem que o conflito cultural aparente – próprio do conflito entre *virtudes do intragrupo* e *vícios do extragrupo* – pode ser assim descrito:

Eu sou atrevido
Você é imprudente
Ele é delinquente

O que Sykes e Matza demonstraram, em suma, é que o delinquente pode não parecer um estranho no corpo social, mas, ao contrário, pode sim representar um incômodo reflexo ou uma caricatura da sociedade.[342] E que, portanto, a qualidade dos valores "deliquentes" é obscurecida por seu contexto. Sykes e Matza citam o exemplo de que, quando o atrevimento vem a ser decorrente de atos de adolescentes dirigidos contra figuras adultas de autoridade aceita, é mais facilmente reconhecível a autoridade ostentada do que a coragem que pode estar envolvida.[343] Fossem os valores da delinquência juvenil bem avaliadas pela sociedade dominante, é possível que a interpretação da natureza da delinquência e do delinquente pudesse ser muito diferente –

[339] *Ibid*., p. 717.
[340] No original: *I am daring / You are reckless / He is delinquent*. A versão original (traduzida) de Merton era: Eu sou firme / Tu és obstinado / Ele é emperrado (MERTON, Robert K. "A profecia que se cumpre por si mesma". In *Idem*. *Sociologia*: teoria e estrutura. trad. Miguel Maillet. São Paulo: Mestre Jou, 1968. p. 523).
[341] SYKES, Gresham M.; MATZA, David. "Juvenile Delinquency and Subterranean Values", *op. cit.*, p. 715.
[342] *Ibid*., p. 717.
[343] *Ibid*., p. 715.

como é o caso do desvio comportamental dos prisioneiros de guerra ou daqueles que se rebelam contra as regras de seus opressores.[344]

Essa explicação do comportamento delinquente, centrado nas atividades desviantes de jovens, é suscetível de empréstimo para a compreensão dos comportamentos criminosos, desviantes e ameaçadores dos atuantes no ciberespaço. De fato, muito do que é considerado *cybercrime* (em especial, aqueles tradicionais e híbridos) simplesmente traduz valores sociais que, por motivos vários, a maioria geralmente não expressa, em razão de dificuldades técnicas para acesso e uso da tecnologia da informação, ou indica valores e conflitos sociais emergentes.

Tome-se, como exemplo da hipótese de um mero reflexo (incômodo ou radicalizado) de valores majoritários, a facilidade com que ocorre a apropriação e pirataria de propriedade intelectual no ciberespaço. A utilização e o compartilhamento de mídia (textos, imagens, áudios e vídeos) tornaram-se tão socialmente disseminados e adequados (aqui não se entra no mérito dogmático da "adequação social") que é difícil que alguém apresente objeção moral a isso ou a perceba sua conduta como criminosa, apesar de o ser. Alguns *hackers* podem provocar maior incômodo ou reação institucional pelo volume de material apropriado, mas, basicamente, trata-se de um comportamento compartilhado e aceito por praticamente todos os atuantes.

E, como exemplo da hipótese de que os *cybercrimes* podem indicar valores e conflitos sociais emergentes, tome-se a crescente prática de veiculação de conteúdo violento e perigoso. Discursos de ódio proferidos em redes sociais têm origem em conflitos sociais contemporâneos reais e encontram nessas plataformas um local privilegiado de propagação e reforço. A disseminação de imagens de violência reflete uma também crescente atração geral pela representação imagética da violência e pela explicitação do corpo, além de uma crescente cultura odiosa que deseja a aniquilação do outro. Ainda dentro dessa hipótese, pense-se no *sexting*, a troca de mídia sexualmente explícita, que passa a gerar conflitos na violação da consensualidade e da confidencialidade, mas indica novos valores e práticas da sexualidade.

[344] *Ibid*., p. 715.

3.2.2 Associação diferencial

Entre as décadas de 1930 e 1960, desenvolveram-se várias teorias para as quais o crime derivava de processos sociais e das interações psicossociais do próprio indivíduo. Deste guarda-chuva teórico, decorreram três orientações principais: as teorias da aprendizagem social (*social learning*), as teorias do controle social (*social control*) e a teoria do etiquetamento (*labelling approach*). A hipótese da associação diferencial pertence à primeira orientação.

A hipótese trabalhada por Sutherland e outros autores sugeriu que os fundamentos da conduta humana são o resultado do aprendizado proporcionado pela experiência cotidiana; ou seja, o comportamento é constantemente promovido e remodelado a partir das reações heteronômicas que a conduta do agente provoca. A conduta criminal, pois, é um hábito adquirido: num complexo processo de comunicação social, o indivíduo aprende um comportamento criminoso, os valores criminais, as técnicas específicas e os mecanismos subjetivos de racionalização de seu agir desviado.[345]

É daí que se extrai a sua teoria da associação diferencial, cuja primeira proposição encontra-se em *Principles of Criminology*, publicado em 1934. Considerando que, numa comunidade, estruturam-se diversas associações com interesses e metas comuns, as quais mantêm a conjunção dos seus associados e constituem seu substrato psicológico, Sutherland assumiu como pressuposto que o comportamento criminoso não poderia ser biologicamente determinado (hereditariedade degenerativa), não procedia da desorganização social ou da anomia, nem poderia ser atribuído a um único grupo social (subcultural ou *lower class*): o comportamento delitivo era aprendido mediante associações em uma sociedade pluralista e conflitiva.[346] A associação constituía um afastamento daqueles que viam a violação como disfuncional e uma aproximação àqueles que a viam como positiva; ou seja, os indivíduos tenderiam a se identificar valorizando positivamente o não cumprimento da norma.[347]

---

[345] GARCÍA-PABLOS DE MOLINA, Antonio. *Criminologia*: introdução a seus fundamentos teóricos; introdução às bases criminológicas da Lei 9.099/95, Lei dos Juizados Especiais Criminais. trad. Luiz Flávio Gomes e Davi Tangerino. 5. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2006. p. 274.
[346] *Ibid*., p. 276.
[347] SUTHERLAND, Edwin Hardin. *White collar crime*: the uncut version: with an introduction by Gilbert Geis and Colin Goff. New Haven/London: Yale University Press, (1949) 2012. p. 240.

Para explicar melhor esse processo, Sutherland estabeleceu as seguintes proposições:

1. Tal como ocorre com o comportamento virtuoso, a crime se aprende. (Essa assertiva contrariava o argumento de que o comportamento criminal é hereditário e nato.)

2. A conduta criminal se aprende por um processo de comunicação com outras pessoas.

3. O grau de intimidade do contato interpessoal é decisivo, sendo a aprendizagem maior nas relações do indivíduo com familiares ou com pessoas do seu meio. Meios de comunicação não teriam um papel tão relevante. (É importante lembrar que, nas décadas de 1930-1940, a tecnologia da televisão era ainda incipiente e não se tinha uma rede de computadores na dimensão da internet.)

4. O aprendizado do comportamento desviado compreende também as técnicas de cometimento do delito e a orientação dos correspondentes motivações, impulsos e atitudes, além da própria racionalização da conduta delitiva.

5. A partir das definições de preceitos legais, favoráveis ou desfavoráveis ao agente, aprende-se a direcionar os motivos e impulsos.

6. A pessoa se converte em delinquente quando, em suas associações diferenciais, ela aprendeu mais modelos criminais do que modelos lícitos, ou seja, quando as definições favoráveis à violação da lei superaram as desfavoráveis.

7. As associações diferenciais podem ser distintas, variáveis conforme idade do agente, frequência, intensidade, duração, valoração atribuída.

> 8. O processo de aprendizagem implica o aprendizado de todos os seus mecanismos inerentes.
>
> 9. Embora a conduta delitiva seja uma expressão de necessidades e de valores gerais, não pode ser explicada como concretização deles, já que também a conduta adequada ao Direito corresponde a idênticas necessidades e valores. (Por exemplo: ganhar dinheiro é uma aspiração tanto de quem trabalha para consegui-lo como de quem o rouba.)

No que toca à concepção da associação diferencial, muito se criticou a generalização, a simplificação e a mecanização do processo de aprendizagem. Policiais e agentes penitenciários, por exemplo, têm contato frequente com criminosos, mas não necessariamente se convertem em delinquentes. Do mesmo modo, a padronização teórica desconsiderava a incidência de fatores individuais de personalidade e ignorava a existência de crimes estranhos a padrões racionais e utilitários: "existem crimes absurdos, ocasionais, espontâneos, impulsivos, alheios por completo a qualquer mecanismo de aprendizagem".[348]

No entanto, no que alcança a etiologia do comportamento delinquente, por mais que tenha traçado e generalizado um processo nem sempre comprovável (primeiro, a associação; e, com a subsequente aprendizagem, a conduta criminosa), Sutherland conseguiu invalidar as teses de que o comportamento criminoso era biologicamente determinado (hereditariedade degenerativa), conforme ditava a antropologia criminal, ou de que era resultado de uma inteligência deficiente ou de uma instabilidade emocional, de acordo com o que defendeu, posteriormente, a psicologia criminal.

Da mesma forma, foi possível demonstrar que o crime não procedia diretamente da desorganização social ou da anomia, nem poderia ser atribuído a um único grupo social. Enquanto se difundia a ideia de que a invasão de estrangeiros ameaçava a paz social, Sutherland demonstrou que eram exatamente os profissionais de destaque da população residente quem explorava os imigrantes e denegria suas condições de vida com salários irrisórios, condições de trabalho perigosas, táticas de destruição de uniões e sindicatos, enfim, cometendo crimes de consequências mais severas que os delitos ordinários de rua que preocupavam a população. A criminalidade tampouco decorria

---

[348] GARCÍA-PABLOS DE MOLINA, Antonio. *Criminologia*, *op. cit.*, p. 277.

exclusivamente da pobreza. (Desde então já se afirmava que o fim da pobreza e a redução do índice de desemprego teriam um impacto direto no índice de criminalidade. No Brasil, até hoje, é comum o argumento de que a educação é a *solução* para a violência cotidiana.) A pesquisa de Sutherland demonstrou que indivíduos com boas condições financeiras, com empregos e educação satisfatória, também cometem crimes (e as recentes grandes operações da Polícia Federal brasileira confirmam isso). O debate sobre a etiologia criminosa, desde então, alcançou níveis maiores de sofisticação.

A sua teoria da associação diferencial pode não ter se sustentado como uma teoria geral do comportamento delinquente; todavia, no decorrer do seu desenvolvimento, possibilitou importantes contribuições ao estudo criminológico: Sutherland foi pioneiro no anúncio de cifras ocultas nos índices de criminalidade; antecipou também a percepção de profunda desigualdade na investigação, na persecução, no julgamento e na condenação de certas condutas e determinados agentes; esboçou uma ideia referente aos interesses difusos (interesses legítimos que quando afetados prejudicam a comunidade indiscriminadamente, pela importância dos bens afetados, pela quantidade de vítimas e o seu anonimato, a magnitude econômica e a possível irreparabilidade da ofensa); com o delineamento científico de crimes ocorridos no mundo dos negócios, estabeleceu uma distinção entre as jurisdições civil e penal para melhor compreensão dos casos; ao colocar o foco na criminalidade dos poderosos, o autor iniciou uma revolução paradigmática e incentivou inúmeros estudos sobre a criminalidade econômica e também fomentou a discussão sobre a responsabilidade penal da pessoa jurídica, tornando-a uma realidade possível no mundo contemporâneo.

Os *cybercrimes* podem encontrar explicação na ideia da associação diferencial e ressonância com a concepção dos crimes de colarinho-branco porque eles são comumente considerados como crimes leves e ocultos. *Cybercrimes* híbridos (como ciberfraudes e apropriação de propriedade intelectual) e especialmente *cybercrimes* próprios (hacktivismo, ataques de DDoS, distribuição de *malwares*) exigem o aprendizado e o aprimoramento de técnicas que não estão amplamente acessíveis à sociedade. Os fóruns virtuais são espaços privilegiados onde os *newbies* aprendem essas técnicas com *hackers* mais experientes, enquanto absorvem a ética própria do ciberespaço.

Uma afinação teórica, porém, é necessária. A transposição da hipótese de Sutherland exige uma adaptação dos sujeitos criminologicamente analisados. Enquanto a associação diferencial permite a compreensão de como os *crimes de colarinho-branco*

são crimes de *poderosos*, seu empréstimo aos atuantes no ciberespaço deve adequar os *cybercrimes* a uma classe *especialista*.[349]

3.2.3 Técnicas de neutralização

Num artigo que se tornou clássico na literatura criminológica (*Techniques of Neutralization*), Sykes e Matza contextualizaram que "[n]a tentativa de descobrir as raízes da delinquência juvenil, o cientista social há muito tempo parou de procurar demônios na mente ou estigmas no corpo".[350] E, prosseguindo, reconheceram a importância da teoria de Sutherland: "Hoje é amplamente aceito que o comportamento delinquente, como a maior parte do comportamento social, é aprendido e que é aprendido no processo de interação social." Mas, nesse artigo de 1957, eles ofereceram uma nova teoria sobre a delinquência.

Em uma forma de contraposição à teoria da associação diferencial, Sykes e Matza desenvolveram a teoria das técnicas de neutralização. Enquanto aquela partia do pressuposto do aprendizado de "atitudes, valores ou imperativos morais que se colocam em contradição direta com aquelas da sociedade dominante"[351], a tese de Sykes e Matza pressupõe que os infratores desenvolvem racionalizações (assim comumente descritas pelos autores) que justificam o comportamento desviante:

> É nosso argumento que muito da delinquência é baseado naquilo que é essencialmente uma extensão irreconhecível das defesas dos crimes, na forma de justificações para o desvio que são vistas como válidas pelo delinquente, mas não o são pelo sistema legal ou pela sociedade em geral.[352]

Sykes e Matza focavam, em particular, a delinquência juvenil; mas, a hipótese desenvolvida compreende o desvio aos sistemas normativos, em geral.[353] São cinco os tipos de técnicas de neutralização identificados pelos autores: negação de responsabilidade (*slogan*: "*I didn't mean it*"), negação de lesão ("*I didn't really hurt anybody*"), negação da vítima ("*They had it coming to them*"), condenação dos

[349] Nesse sentido: WALL, David S. *Cybercrime, op. cit.*, p. 210.
[350] SYKES, Gresham M.; MATZA, David. (1957) "Techniques of Neutralization: A Theory of Delinquency", *American Sociological Review*, v. 22, n. 6, p. 664.
[351] *Ibid*., p. 667.
[352] *Ibid*., p. 666.
[353] *Ibid*., p. 670.

condenadores ("*Everybody is picking on me*"), e apelo a lealdades maiores ("*I didn't do it for myself*").

- *Negação de responsabilidade*: Essa técnica vai além da alegação de que os atos desviantes são um "acidente" ou de qualquer similar negação de responsabilidade pessoal; por ela, pode-se afirmar que os atos delinquentes decorrem de forças externas ao indivíduo e além de seu controle, tais como: ausência de afeto parental, más companhias ou bairros pobres.

> Com efeito, o delinquente assume uma concepção de si como uma "bola de bilhar", na qual ele se vê como impotentemente propelido a novas situações. (...) Ao aprender a se ver mais como coagido do que agindo, o delinquente abre caminho ao desvio do sistema normativo dominante sem a necessidade de uma agressão frontal às próprias normas.[354]

Sykes e Matza sugerem uma clara similaridade entre esse modo de justificar o comportamento ilegal assumido pelo delinquente e as implicações de um viés "sociológico" de referência ou de uma jurisprudência "humanizada".

- *Negação de lesão*: Para o delinquente, a ilicitude pode levantar a questão de se alguém se lesionou ou não em razão do seu comportamento desviante, e isso está aberto a uma variedade de interpretações: o vandalismo pode ser definido pelo delinquente como uma "travessura" (afinal, o proprietário lesado pode bancar o prejuízo); o furto de automóveis pode ser visto como "empréstimo"; uma luta de gangues pode ser vista como uma "briga privada", um "acerto" entre duas partes, que não interessa à comunidade em geral.[355]

- *Negação da vítima*: Por parte do delinquente, há um reconhecimento de alvos apropriados e inapropriados para seus atos ilícitos. E quanto mais a vítima for fisicamente ausente, desconhecida ou uma vaga abstração, mais é enfraquecida a percepção da sua existência.[356]

---

[354] *Ibid*., p. 667.
[355] *Ibid*., p. 667.
[356] *Ibid*., p. 668.

> Mesmo que o delinquente aceite a responsabilidade por suas ações desviantes e esteja disposto a admitir que suas ações desviantes envolvem uma lesão ou dano, a indignação moral de si e outros pode ser neutralizada por uma insistência de que a lesão não é errada à luz das circunstâncias. A lesão, pode ser argumentado, não é realmente uma lesão; ao invés, é uma forma de retaliação ou punição merecida. Por uma alquimia sutil, o delinquente se move à posição de um vingador e a vítima é transformada em um malfeitor.[357]

- *Condenação dos condenadores*: O delinquente desloca o foco de atenção, dos seus próprios atos desviantes para o comportamento e motivos daqueles que desaprovam suas violações. Os condenadores são tratados como "hipócritas", "condenadores disfarçados", impelidos por rancor pessoal. Como exemplo prático: a polícia é vista como corrupta, estúpida e truculenta; professores exibem favoritismo; pais sempre descontam em seus filhos.[358]

- *Apelo a lealdades maiores*: Argumento no qual se expressa um sacrifício das demandas da sociedade em geral em prol das demandas de grupos sociais menores ao qual pertence o delinquente (irmandade, gangue, turma de amigos). O delinquente não necessariamente repudia os imperativos do sistema normativo dominante, mas se vê apanhado num dilema que pode ser resolvido, infelizmente, ao custo da violação da lei, quando se confere precedência a lealdades maiores.

O grande mérito dos trabalhos de Sykes e Matza foi a normalização da ideia da delinquência.[359] Anteriormente tratado como uma anomalia biológica ou social pelos discursos criminológicos tradicionais, o delinquente deixa de ser um estranho social quando se evidencia que ele detém os mesmos recursos morais dos não-delinquentes, conforme os argumentos sobre o conflito cultural e as técnicas de neutralização. O jovem delinquente, em particular, e os infratores, em geral, seriam reflexos, explícitos e intensos, dos valores sociais dominantes e seriam capazes de racionalizar suas condutas desviantes.

---

[357] *Ibid*., p. 668.
[358] *Ibid*., p. 668.
[359] SYKES, Gresham M.; MATZA, David. "Techniques of Neutralization: A Theory of Delinquency", *op. cit.*; *Idem*. "Juvenile Delinquency and Subterranean Values", *op. cit.*

Essas hipóteses, porém, seriam suscetíveis de transposição ao contexto dos *cybercrimes*? Alguns autores sugerem que os atuantes comumente identificados como infratores no ciberespaço também são fruto dos valores de seu tempo e lançam mão dessas mesmas e outras técnicas de neutralização. As técnicas de neutralização abaixo, colacionadas a partir da complementação de vários pesquisadores[360] às ideias de Sykes e Matza, revelam-se de grande utilidade para que indivíduos sintam-se livres de amarras morais, éticas e legais, possibilitando que racionalizem sua participação em alguma forma de violação:

- *Negação de lesão*: Indivíduos que cometem *cyberbullying* (*cybercrime* híbrido) podem justificar seus atos como uma mera travessura; aqueles que fazem downloads ilegais, como forma de apropriação de propriedade intelectual (*cybercrime* híbrido), podem argumentar que "isso não é o mesmo que roubar", ou que o compartilhamento de arquivos não causa prejuízo aos artistas, mas que a atividade os ajuda, divulgando seus trabalhos e levando um público maior aos seus shows.[361]

- *Negação da vítima*: Essa racionalização é comum nas ciberfraudes (*cybercrime* híbrido), quando as vítimas de golpes são vistas como gananciosas – ou simplesmente difusas ou inexistentes –, e nos ataques promovidos pelo hacktivismo (*cybercrime* próprio), nos quais os atuantes assumem um papel de vigilantes e os destinatários de seus ataques são retratados como infratores.

Por mais que esses autores adaptacionistas não se dediquem a explorar mais a fundo as outras racionalizações, é possível aqui estender seus argumentos. Verifica-se, por exemplo, a *negação de responsabilidade* no indivíduo que, sendo vítima de um sequestro de dados por *ransomware*, repassa o *malware* a outros destinatários, contaminando novos computadores, como forma de resgate para receber a chave para descriptografar seus arquivos.

---

[360] MOORE, Robert; MCMULLAN, Elizabeth C. "Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students", *op. cit.*; PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*, *op. cit.*, p. 62.

[361] MOORE, Robert; MCMULLAN, Elizabeth C. "Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students", *op. cit.*

A *condenação dos condenadores* é muito evidente no hacktivismo e nos casos de *leaking*: as operações de invasão, desconfiguração e vandalismo de *websites*, sobrecarregamento de servidores por meio de DDoS, utilização de *malwares* etc., tal como o vazamento indevido de informações sensíveis, são justificados como resposta a medidas que, para a ética hacker, indicam corrupção, injustiça e hipocrisia, como restrições de conteúdo, restrições de direitos autorais ou ocultação de crimes de guerra.

E, no mesmo sentido, a forte adesão a essa *netiquette* (regras consuetudinárias de comportamento no ciberespaço) sugere um sacrifício das demandas da sociedade em geral em prol das demandas de grupos sociais menores ao qual pertence o atuante, ou seja, um *apelo a lealdades maiores*. Como explicaram Sykes e Matza, isso não significa que os atuantes repudiem necessariamente os imperativos do sistema normativo dominante, mas, apanhados num dilema, resolvem-no com atendimento a essa moralidade implícita que governa as relações cibernéticas.

É digno de nota que as racionalizações disponíveis não se resumem àquelas apresentadas por Sykes e Matza. Esses mesmos autores adaptacionistas reconhecem a existência de outras técnicas de neutralização, utilizadas pelos atuantes no ciberespaço:

- *Metáfora do registro*: Um indivíduo considera um caso particular de violação como único em uma série de outros bons comportamentos. Esse recurso justificativo se adéqua melhor aos *cybercrimes* híbridos de violação de conteúdo. Um atuante eventualmente responsabilizado por compartilhar material pornográfico infantil, por publicar conteúdo odioso ou por praticar *revenge porn* pode entender que sua conduta foi um "deslize", uma falha moral singular, um desvio de conduta momentâneo, uma pequena mácula numa biografia de acertos.

- *Negação da necessidade da lei*: Segundo ela, a lei é resultado de tentativas de se regularem comportamentos que não têm nada a ver com algo bom às pessoas, o que a torna inadequada e indigna de ser obedecida. A apropriação de propriedade intelectual e o *leaking* são modelos de *cybercrimes* em que as normas violadas (que visam a proteger direitos autorais e sigilo da informação) são vistas como restritivas do livre fluxo de informação e consideradas, portanto, como inadequadas (anacrônicas, ineficazes) e indignas (injustas) de cumprimento.

- *Reivindicação do direito*: Os desvios e as violações podem ainda ser justificados por meio da reivindicação de um direito, que favoreça o desviante/infrator, diante de um conflito jurídico. No caso dos *cybercrimes*, a apropriação de propriedade intelectual pode ser justificada pelo direito de acesso à cultura e à educação (em contraposição aos direitos autorais), o discurso de ódio pode ser justificado como direito de livre manifestação do pensamento e de liberdade de expressão (em contraposição aos direitos de dignidade e igualdade), o hacktivismo pode ser justificado como direito de livre manifestação e de reunião (em contraposição aos direitos de privacidade e propriedade), o *leaking* pode ser justificado pelo direito de acesso à informação (em contraposição ao direito de sigilo).

- *Todo mundo faz isso*: Uma dupla racionalização pode ser expressa nesse argumento: (i) o indivíduo pretende legitimar sua conduta pressupondo que um tamanho consenso geral em ignorar determinada norma indica que ela é considerada sem importância ou até socialmente revogada, tornando aceitável sua conduta; ou, (ii) ao reclamar a universalidade da conduta, o indivíduo pode indicar que "quando todos fazem" reduz-se a chance de ser pego. Essa neutralização é recurso comum nos casos de apropriação de propriedade intelectual.

- *Defesa da necessidade*: Argumenta-se que, ao passo que o comportamento realizado seja desviante, ele também é necessário para prevenir que ocorra uma violação ainda maior. O hacktivismo e o *leaking* encontram nesse argumento uma justificativa privilegiada para suas atividades.

As técnicas de neutralização exigem que os infratores percebam seu comportamento como ato criminoso e que sintam culpa (controle interno) e/ou vergonha (controle externo). Como adverte Copes, pessoas que não se sentem subordinados às normas sociais ou que entendem que seu comportamento não está errado não precisam recorrer a racionalizações para preservar sua própria identidade e sua identidade

social.[362] Algumas entrevistas têm reforçado a ideia de que algumas condutas, como o download e o compartilhamento de arquivos, não são vistos como violações e seus atuantes não indicam uma redução ou interrupção do comportamento.[363]

3.2.4 Teoria da ação situacional

A teoria da ação situacional integra as perspectivas criminológicas sobre os atuantes (sua constituição moral, suas tendências, seus hábitos) com aquelas que analisam as influências do ambiente sobre o comportamento humano (fatores sociais, regras e contexto moral). Ela se propõe a fazer algumas previsões sobre como a interação entre uma propensão individual e a exposição ambiental causa atos desviantes, sugerindo, então, o processo causal pelo qual isso acontece. A teoria apresenta os seguintes pressupostos:

- A motivação é um conceito situacional que deriva da relação entre o indivíduo (exercício de autocontrole) e o ambiente (dissuasão externa).

- As pessoas podem desejar cometer violações; todavia, o mero desejo não resulta em uma conduta desviante.

- As ações desviantes são ações morais, porque o que faz o indivíduo perceber sua motivação desviante como uma alternativa de ação é o *filtro moral*.

- As pessoas empreendem condutas porque elas compreendem essas ações como ações alternativas e porque escolhem realizá-las.

- A probabilidade de uma pessoa entender uma ação desviante como uma alternativa de ação depende de sua propensão e sua inter-relação com sua exposição a ambientes criminogênicos.

---

[362] COPES, Heith. "Societal attachments, offending frequency, and techniques of neutralization", *Deviant Behavior: An Interdisciplinary Journal*, v. 24, n. 2, 2003, p. 104.
[363] MOORE, Robert; MCMULLAN, Elizabeth C. "Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students", *op. cit.*

- A propensão reflete os fatores pessoais que afetam a possibilidade de se perceber uma ação desviante como uma alternativa de ação e de executá-la em reação a uma particular ambientação.

O ecletismo teórico possibilita a conclusão de que a ação individual é sempre um resultado das características ambientais, do qual um indivíduo participa, e do processamento e avaliação da absorção ambiental. Inspirado nesses argumentos, Pérez Suárez desenvolveu uma teoria da ação situacional revisada para a internet, a qual pretende medir a propensão do cometimento de um *cybercrime* em certos indivíduos quando eles têm contato com a rede e têm um catálogo apropriado de neutralizações à sua disposição.[364]

A relação entre a propensão individual (P), a exposição à internet (E) e as técnicas de neutralização (N), após um processo de deliberação moral (mediada pelo autocontrole), pode resultar no cometimento de um determinado *cybercrime* (CC). Ou:

$$P \times E \times N \sim CC$$

A internet é entendida por Pérez Suárez como um contexto moral autônomo (não relacionado com o contexto moral off-line) e um ambiente criminogênico *per se*.[365] A ênfase no processo deliberativo que conduz ao crime evidencia que se trata de uma variação da teoria da escolha racional (teoria econômica de Gary Becker).

3.2.5 Criminologias culturais

Nascidas de influências teóricas americanas (teoria do etiquetamento, teorias subculturais, abordagens naturalísticas do crime, pesquisas etnográficas) e britânicas (criminologia crítica, nova criminologia), as criminologias culturais estabeleceram um novo paradigma para a compreensão do fenômeno criminal contemporâneo. Ferrell e Hayward explicam como elas representam a adaptação da criminologia ao contexto da modernidade tardia:

[364] PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs, op. cit.*
[365] *Ibid*., p. 58-59.

> O fluxo do mundo tardo-moderno sugere que os crimes dessa era precisarão ser amiúde entendidos em termos de imediatismo, efemeridade e incerteza; assim como as identidades associadas com localização ocupacional ou espacial foram desestabilizadas, assim também o foram aquelas geradas na interação de crime e transgressão. Nesse sentido, modelos mais antigos de criminalidade e de causas criminais, geralmente fundadas em hipóteses de sequenciamento linear, previsibilidade positivista e identidade criminal estável, bem podem necessitar uma reimaginação.[366]

As criminologias culturais se estabeleceram, primeiramente, pela contraposição de seus pressupostos, objeto e métodos àqueles utilizados pelas criminologias mais tradicionais. Há nelas uma evidente resistência, por exemplo, às teorias fundadas em antecedentes (pobreza, falta de instrução, vizinhanças pobres, desigualdade social) ou causalidades (desemprego, associação diferencial, tensão), tal como à teoria da escolha racional (que se volta ao cotidiano e cria a abstração do *calculador racional*) e ao positivismo (que se concentra no mensurável e cria a abstração do *agente mecanicístico*).[367] E há também uma contestação às criminologias administrativas, que não se preocupam em debater a natureza do fenômeno do crime ou em questionar suas definições.[368]

As criminologias culturais estão interessadas na convergência de processos culturais, criminais e de controle do crime; elas situam a criminalidade e seu controle no contexto de dinâmicas culturais e da produção de significados.[369] Situando o crime em seu próprio contexto cultural, elas possibilitam ver tanto o crime quanto os dispositivos de controle como produtos culturais, os quais devem ser lidos a partir dos significados que carregam. Seu foco é sempre sobre a contínua geração de significado em torno da interação: regras criadas, regras quebradas, constante interação do empreendedorismo moral, inovação moral e transgressão.[370] Ou seja, trata-se de ver tanto o crime quanto as agências de controle como produtos culturais, como construções criativas – e, como tais, devem ser lidos em termos dos significados que carregam.[371]

---

[366] FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada" In CARLEN, Pat; FRANÇA, Leandro Ayres. *Criminologias alternativas*. Porto Alegre: Canal Ciências Criminais, 2017. p. 40.
[367] HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *Theoretical Criminology*, v. 8, n. 3, 2004. p. 263-264.
[368] *Ibid*., p. 262.
[369] FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada", *op. cit.*
[370] HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *op. cit.*, p. 259.
[371] *Ibidem*.

Como características comuns, podemos identificar nas criminologias culturais:

- Adoção de perspectivas interdisciplinares e métodos alternativos, extraindo de estudos de mídia, antropologia, estudos sobre jovens, estudos culturais, geografia cultural, sociologia, filosofia e outras disciplinas, e utilizando novas formas de etnografia, análise textual e produção visual.[372]

- Ênfase no individualismo e na geração do estilo de vida contemporâneo, combinado com a mídia de massa que se expandiu e proliferou a ponto de transformar a subjetividade humana.[373] Isso exige um enfoque na análise crítica da produção cultural e um compromisso com a criatividade e o lúdico.

- Engajamento com os sujeitos estudados.[374] Por isso, o foco no primeiro plano da experiência do crime e na psicodinâmica existencial do agente[375], possibilitando melhor absorção do momento "experiencial" do crime, com o "sentido localizado da atividade criminosa", com as estruturas interpretativas, imagens e significados por meio dos quais e nos quais o crime é aprendido e realizado.

  Sobre a metodologia do primeiro plano do crime, Ferrell e Hayward[376], inspirados em Jack Katz (1988), argumentam que a criminologia tradicional tem se constituído de trás para frente – ou seja, construída sobre hipóteses antecedentes ou estruturais que conduzem à criminalidade –, ignorando as situações do crime. A análise do imediatismo do crime permite a compreensão das emoções da dinâmica pessoal e social do momento, imprevisíveis para as teorias criminológicas *mainstream*. Daí, o interesse pelos *performers*, que, para Caldeira são

[372] FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada", *op. cit.*
[373] HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *op. cit.*, p. 259.
[374] HAMM, Mark S. "Apocalyptic violence: The seduction of terrorist subcultures", *Theoretical Criminology*, v. 8, n. 3, 2004. p. 337.
[375] HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *op. cit.*, p. 266.
[376] FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada", *op. cit.*

> decifradores dos espaços urbanos [que] os exploram desde ângulos inusitados, como, por exemplo, o topo dos edifícios mais altos (escalados pelo exterior), os corrimãos que servem de guia aos skatistas, os muros que devem ser transpostos pelos traceurs, as ruas e avenidas percorridas em alta velocidade pelos motociclistas entre as filas de carros, ou ainda diversos locais que ninguém mais se arrisca a visitar, como as galerias de esgoto aproveitadas como suporte para grafites.[377]

- Análise dual do espaço urbano, não necessariamente de divisão e segregação espacial, mas no sentido da *underlife* da cidade.[378] Hamm refere-se à ênfase nas "desenterradas histórias enterradas da vida subterrânea".[379]

- Compromisso em entender os papéis da emoção[380], da sedução e do desejo. Sobre isso, Hayward e Young explicam que:

> A real experiência do cometimento do crime, o real resultado do ato criminoso, carrega pouca relação com esses essencialismos limitados [da teoria da escolha racional e positivismo]. Ao contrário, o *rush* de adrenalina do crime, que (como apresenta Jeff Ferrell) acontece entre "prazer e pânico", os vários sentimentos de raiva, humilhação, exuberância, excitação e medo, não cabem nessas abstrações.[381]

Daí o interesse nas *ações-limite*: atos de voluntária assunção de risco e geralmente ilícitos; "atos transgressivos que vão desde aqueles no limiar da ilegalidade até os patentemente criminosos"[382]; ou "necessidade dinâmica de forçar os limites do comportamento convencional no intuito de alcançar transcendência moral sobre ele"[383]. Exemplos: produção de inscrições (grafites e pixações[384])[385], deslocamentos espaciais

---

[377] CALDEIRA, Teresa Pires do Rio. "Novas visibilidades e configurações do espaço público em São Paulo", *Novos Estudos – CEBRAP*, n. 94, 2012. p. 59.
[378] HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *op. cit.*, p. 265.
[379] HAMM, Mark S. "Apocalyptic violence: The seduction of terrorist subcultures", *op. cit.*, p. 337.
[380] Nesse aspecto, Robert Merton parece ter antecipado a mudança de paradigma provocado pelo que viria a ser chamado de criminologia cultural: "parece que a 'versatilidade' e o 'gostinho' com que alguns rapazes praticam seus desvios apoiados pelo seu grupo, não são diretamente explicados pela teoria da estrutura social e da anomia." (MERTON, Robert K. "Continuidades na Teoria da Estrutura Social e da Anomia" In *Idem*. *Sociologia*: teoria e estrutura. São Paulo: Mestre Jou, 1970. p. 254.)
[381] HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *op. cit.*, p. 264.
[382] CALDEIRA, Teresa Pires do Rio. "Novas visibilidades e configurações do espaço público em São Paulo", *op. cit.*, p. 32.
[383] HAMM, Mark S. "Apocalyptic violence: The seduction of terrorist subcultures", *op. cit.*, p. 335.
[384] A correta grafia da palavra é *pichação*, mas praticantes e pessoas associadas à arte de rua em geral empregam o *x* em vez de *ch* (CALDEIRA, Teresa Pires do Rio. "Novas visibilidades e configurações do espaço público em São Paulo", *op. cit.*, p. 32).
[385] *Ibidem*.

(*skate*, *parkour*, motociclismo[386] e "rolezinhos"[387]), paraquedismo, roubos nas ruas, provocações de incêndios, lutas amadoras, prostituição de rua, fisiculturismo, terrorismo[388] etc.

Os relatos sobre as motivações e sensações de atuantes no ciberespaço parecem refletir a noção de *ações-limite*; na descrição de um dos membros do coletivo Anonymous, Olson relata o seguinte:

> Arruinar a vida das pessoas animou William e lhe deu uma sensação de poder diferente de qualquer coisa que ele tinha sentido no mundo exterior. O único outro momento em que ele sentiu qualquer coisa similar era quando ele escapava silenciosamente de casa, na calada da noite, encontrava com alguns velhos amigos e fazia grafites coloridos nos trens ou muros locais. O grafite era sua amante nas noites de verão. No inverno, era o 4chan e agora, às vezes, as atividades maiores dos Anonymous.[389]

O engajamento voluntário em atividades de alto risco reverte a lógica do gerenciamento de riscos contemporâneo, adotando o risco por seus prazeres sensuais e possibilidades transgressivas. Por meio dos riscos das ações-limite, por exemplo, os participantes recuperam algum senso de identidade.[390] Caldeira, tratando da pixação e do grafite, sugere que "[e]ssa produção da representação de si mesmo é, sem a menor dúvida, uma das consequências mais inovadoras da democratização brasileira".[391]

As criminologias culturais não estiveram (ou estão) isentas de críticas. O'Brien, por exemplo, questiona se a criminologia cultural realmente representa um novo empreendimento intelectual em vez de uma elaboração lógica de trabalhos anteriores sobre subculturas desviantes.[392] De certa forma, o que se chama hoje criminologia cultural já é algo realizado por pesquisadores sociais há algumas décadas, sem esse rótulo.[393]

O'Brien prossegue argumentando que a utilização de metáforas aquosas (ondas, fluidez, liquidez, inundado), claramente inspiradas em Zygmunt Bauman, e marítimas (à

---

[386] *Ibidem*;
[387] *Idem*. "Qual a novidade dos rolezinhos?: Espaço público, desigualdade e mudança em São Paulo", *Novos Estudos – CEBRAP*, n. 98, 2014. p. 13-20.
[388] HAMM, Mark S. "Apocalyptic violence: The seduction of terrorist subcultures", *op. cit.*
[389] OLSON, Parmy. *We are Anonymous*: inside the hacker world of LulzSec, Anonymous, and the Global Cyber Insurgency. New York: Little, Brown and Company, 2012. p. 30.
[390] FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada", *op. cit.*
[391] CALDEIRA, Teresa Pires do Rio. "Novas visibilidades e configurações do espaço público em São Paulo", *op. cit.*, p. 39.
[392] O'BRIEN, Martin. "What is *cultural* about cultural criminology?", *The British Journal of Criminology*, v. 45, n. 5, 2005. p. 600.
[393] No contexto brasileiro, por exemplo, ver CALDEIRA, Teresa Pires do Rio. "Novas visibilidades e configurações do espaço público em São Paulo", *op. cit.*; *Idem*. "Qual a novidade dos rolezinhos?, *op. cit.*

deriva, flutuação, líquida, mar de comunicação) é em si instrutiva para descrever os contextos sociais e políticos bastante desprovidos de agentes institucionais concretos e efetivos (como o Estado) e relações sociais padronizadas (como classes, gêneros), mas, segundo ele, esse recurso gera muita confusão sobre o que representa a cultura na explicação do crime e seus controles.[394]

Uma quase-exclusiva atenção às subculturas também foi bastante criticada. Entender as atividades ilícitas de determinada subcultura é impossível sem uma densa descrição das ações dos participantes e das condições e situações em que elas acontecem. No entanto, a mesma perspectiva de, e o mesmo comprometimento a, essa determinada cultura não são aplicados aos outros atores-chave, que contestam ou enfrentam tal subcultura. Estes são caracterizados como cifras unidimensionais de uma cultura unidimensional. A cultura *mainstream*, cidadãos "convencionais", o estado local, políticos, agências policiais, a mídia, organizações comerciais são representados como tolos culturais ou como empresários morais egoístas, que manipulam imagem e ideologia por meio da criação de um pânico moral com o intuito de reforçar seu poder social, econômico e político.[395]

Numa crítica mais pesada, e emprestando a alcunha que Alvin W. Gouldner (1975) atribuiu aos primeiros etnógrafos da transgressão, O'Brien chama os criminologistas culturais de *tratadores de zoológico do desvio*: porque, ao fim e ao cabo, eles contam narrativas compreensivas dos comportamentos de grafiteiros, motociclistas, paraquedistas, usuários de drogas e outros, de uma forma voyeurística e sensual[396]. Essas narrativas podem revelar tanto sobre os sujeitos narrados na pesquisa quanto dos próprios narradores. O'Brien afirma que isso não necessariamente é algo ruim, mas questiona se isso é ou não criminologia.[397] Por isso, ele aconselha a criminologia cultural a reduzir o estudo de espécies desviantes e focar mais no aspecto geralmente político da criminalização, explicando, por exemplo, porque algumas pessoas que cometem crimes estão livres, enquanto muitos presos nas prisões do mundo não foram condenados ou sequer processados.[398] Em suma, sua crítica sugere que a criminologia cultural ignora uma mais ampla economia política do crime e falha em explicar formas mais graves de criminalidade.

---

[394] O'BRIEN, Martin. "What is *cultural* about cultural criminology?", *op. cit.*, p. 609-610.
[395] *Ibid*., p. 602-603.
[396] *Ibid*., p. 610.
[397] *Ibidem*.
[398] *Ibid*., p. 610-611.

Valendo-se dos *insights* da teoria do etiquetamento, os criminologistas culturais respondem que a importância ou a seriedade de qualquer forma de criminalidade é amplamente determinada pela resposta legal (isto é, a atribuição de um sentido por parte de quem detém o poder). Assim, a criminalidade cotidiana merece a mesma atenção crítica da criminalidade excepcional.[399] Os criminologistas culturais também contestam essa crítica argumentando que são precisamente esses habitantes da vida cotidiana que, ao contrário dos cidadãos "convencionais", percebem e resistem a uma estratégia de controle social que, na modernidade tardia, assumiu uma forma discreta, constante, capilar, oportunizando um exercício de poder embutido nos arranjos espaciais, infiltrado em ideologias de gerenciamento de risco e empregado por meio da mitologia do conforto e conveniência.[400]

Não se registram ainda estudos criminológicos culturais voltados aos atuantes cibernéticos e seus crimes, desvios e ameaças. Mas, há uma oportunidade ímpar do uso dos recursos criminológicos culturais para a compreensão do estilo de vida contemporâneo desses *performers*, da experiência (em primeiro plano) dos *cybercrimes*, da dualidade dos espaços físico e virtual, das emoções, seduções e dos desejos que os atuantes experimentam.

Criminologias alternativas que procurem entender os *cybercrimes* devem prestar atenção às condições materiais (etnia, classe social, gênero etc.) e às recompensas morais e emocionais (humilhação, arrogância, desejo de vingança, indignação etc.) que essas ações fornecem para aqueles que os cometem, porque, com frequência, esses crimes não são suficientemente explicáveis a partir de eventuais recompensas materiais.

[399] FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada", *op. cit.*
[400] *Ibidem*.

3.3 ATUANTES

Ainda que seja possível transportarmos algumas das teorias criminológicas tradicionais para explicar – biológica, psicológica, sociológica ou culturalmente – as condutas desviantes no ciberespaço, resta ainda verificar se podemos igualmente entender os atores dessas condutas num processo de continuidade. Podemos também partir do pressuposto de que aquele responsável por um *cybercrime* é aquele mesmo ser humano, dotado de consciência e vontade em realizar um ato injusto, ou há algo de novo naquele que atua no reino da técnica cibernética?

Virilio era muito receoso com a possível perda da íntima percepção da massa ponderável do corpo em razão do advento das novas tecnologias:

> Se antes, *estar presente era estar próximo*, fisicamente próximo do outro, em um face-a-face, um frente-a-frente em que o diálogo se torna possível através do alcance da voz e do olhar, o advento de uma *proximidade midiática* fundada nas propriedades do domínio das ondas eletromagnéticas parasita o valor da aproximação imediata dos interlocutores, esta súbita perda de distância ressurgindo sobre o "estar-lá", aqui e agora. Se a partir de então pode-se não somente agir, mas ainda "tele-agir" – ver, ouvir, falar, tocar ou ainda sentir à distância – surge a possibilidade inaudita de um brusco desdobramento da personalidade do sujeito que não saberá deixar intacta por muito tempo "a imagem do corpo", ou seja, a PROPRIOCEPÇÃO do indivíduo... Cedo ou tarde, esta íntima percepção da massa ponderável perderá qualquer evidência concreta, liquidando em um mesmo ato a clássica distinção entre o "de dentro" e o "de fora". O hipercentro do *tempo real* (ou, se preferirmos, do presente-vivo) do corpo próprio – EGOCENTRAMENTO – doravante levando a melhor sobre o centro do *espaço real* do mundo próprio – EXOCENTRAMENTO – perdendo todo e qualquer sentido a noção essencial de ser e de agir, aqui e agora.[401]
>
> Subjugado além do imaginável, o "novo homem-máquina" concretiza, é preciso que se diga, as rupturas inauguradas pelo futurismo, o cubismo e o surrealismo, mas a partir de então trata-se menos de dissociar as aparências objetivas da realidade, de interpretação subjetivado artista, que de romper *a unidade de percepção do homem* e de realizar, desta vez de forma AUTOMÁTICA, a permanência de um abalo de propriocepção que afetará duravelmente sua relação com o real.[402]

Em entrevista posterior, tratando especificamente da internet, Virilio explicitou sua ideia sobre a incorporeidade no ciberespaço:

> Efetivamente, a internet, o cibermundo, é atópico, sem lugar, sem território. Não se trata apenas de uma atopia territorial, mas também corporal, o que a torna mais grave. É um não-lugar e um não-corpo. (...) Ora, a atopia da

[401] VIRILIO, Paul. *A arte do motor*, *op. cit.*, p. 96.
[402] *Ibid*., p. 127, grifos no original.

> internet é uma atopia em relação ao corpo territorial, ou seja, a geografia e a geopolítica, ao corpo social – a comunidade virtual não tem realidade física – e, enfim, talvez o mais grave, em relação ao corpo humano, ao corpo animal, no sentido de anima, a alma, não apenas no sentido biológico do termo.[403]

Por mais compreensível que seja sua preocupação, não compartilho da mesma interpretação de atopia corporal. Há, em sua interpretação, uma absoluta distinção do corpóreo e o incorpóreo, assim como o faz Lyotard quando reflete sobre a possibilidade de um pensamento sem corpo – no específico sentido do complexo organismo vivo terrestre conhecido como corpo humano.[404]

Teóricos mais recentes têm trabalhado com uma ideia de fusão. Para início da reflexão, tomemos uma explicação de Dant sobre a relação do ser humano com o automóvel.[405] As ciências sociais apresentam duas perspectivas-chave para a análise do automóvel: primeiro, como uma mercadoria que ilustra o desenvolvimento da produção no capitalismo industrial; segundo, como uma mercadoria que ilustra o objeto de desejo que motiva consumidores no capitalismo tardio. Dant, por sua vez, explora "o conjunto do motorista-carro como uma forma de ser social que produz uma variedade de ações sociais que são associadas com o carro"[406], como a condução, o transporte, o estacionamento, o consumo, a poluição, a morte, a comunicação e assim por diante. Dant rejeita a terminologia "ciborgue" para a fusão do motorista com o carro (porque a ideia de ciborgue tende a fixar e reificar o conjunto) e tampouco aceita o termo "híbrido" (porque ele se refere a entes que resultam da combinação permanente de tipos similares de objetos, ou por sua referência ao fruto de duas espécies que geralmente é incapaz de se reproduzir). O motorista-carro, explica Dant, "não é uma espécie resultante do cruzamento ao acaso, mas um produto de projeto, manufatura e escolha humanos [que] permite uma forma de ação social que se tornou rotineira e habitual, afetando muitos aspectos da sociedade tardo-moderna".[407]

---

[403] VIRILIO, Paul. "Da política do pior ao melhor das utopias e à globalização do terror", *op. cit.*, p. 7.
[404] LYOTARD, Jean-François. *O inumano*, *op. cit.*, p. 22. Concluindo, na sequência, que "o que torna inseparáveis o pensamento e o corpo, é muito simplesmente o facto deste último ser o indispensável *hardware* do primeiro, a sua condição material de existência é que cada um deles é análogo ao outro no seu relacionamento com o respectivo ambiente (sensível, simbólico), sendo o próprio relacionamento em si do tipo analógico nos dois casos." (p. 24) Importante ressaltar que, com esses argumentos, Lyotard busca contestar a ideia de inteligência artificial.
[405] DANT, Tim. "The Driver-car", *op. cit.*
[406] *Ibid*., p. 61.
[407] *Ibid*., p. 62.

> Nem o motorista humano, nem o carro atuando apartados poderiam causar os tipos de ação que o conjunto pode; são as particulares formas nas quais suas capacidades são reunidas que causam o impacto do automóvel nas sociedades modernas.[408]

O motorista aprende e se habitua no carro como um conjunto que pode alcançar a automobilidade: uma orientação incorporada a um mundo de objetos que se movem rapidamente, a partir de uma posição sentada, que também se move rapidamente.[409] Reunidas as habilidades aprendidas pelo motorista com a funcionalidade do carro, oportuniza-se o acontecimento de um fenômeno cultural característico das sociedades contemporâneas: tornar-se um objeto que se move rápido num espaço restrito com outros objetos que se movem rápido.[410]

Para reforçar seu argumento de como o conjunto constituído do motorista-carro produz uma forma de ser social e um conjunto de ações sociais que são diferentes de outras formas de ser e ação, Dant resgata uma reflexão de Bruno Latour. Um dos exemplos de Latour da fusão de humanos e não-humanos deriva do debate sobre se as armas matam pessoas ou se são as pessoas com armas que matam: "Qual deles, a arma ou o cidadão, é o *ator* nessa situação? *Um outro alguém* (um cidadão-arma, uma arma-cidadão)".[411] O famoso slogan de que "armas matam pessoas" é materialista: a arma age em virtude de componentes materiais irredutíveis às qualidades sociais do atirador. O outro notório slogan de que "armas não matam pessoas; pessoas matam pessoas" é sociológico: a arma não faz nada em si ou em virtude de seus componentes materiais; ela é um instrumento, um meio, um veículo neutro da vontade humana. "O que a arma acrescenta ao disparo?", questiona Latour, radicalizando propositalmente as duas perspectivas diametrais. No relato materialista, tudo; na versão sociológica, nada.[412] O duplo e idêntico equívoco dos argumentos materialistas e sociológicos é começar a partir das essências, sejam aquelas do sujeito ou aquelas do objeto.[413] Porque o agente humano é transformado pela posse da arma, e a arma também é transformada por estar na mão de alguém disposto a usá-la.[414] O programa de ação de ambos sujeito e objeto é

---

[408] *Ibid*., p. 62.
[409] *Ibid*., p. 73.
[410] *Ibid*., p. 74.
[411] LATOUR, Bruno. *Pandora's hope*: essays on the reality of science studies. Cambridge: Harvard University Press, 2000. p. 179, grifos no original.
[412] *Ibid*., p. 176-177.
[413] *Ibid*., p. 180.
[414] *Ibid*., p. 179.

transformado quando eles se reúnem – combinados, eles podem atuar com um objetivo um tanto diferente do que poderiam ter alcançado independentemente.

Agamben, em raciocínio semelhante, explicou que os sujeitos são o resultado da relação entre duas grandes classes, os seres viventes (ou as substâncias) e os dispositivos. Um mesmo indivíduo, então, relacionando-se com dispositivos diversos, poderia ser o lugar de múltiplos processos de subjetivação: "o usuário de telefones celulares, o navegador na internet, o escritor de contos, o apaixonado por tango, o não-global etc etc".[415] O dispositivo, para Agamben, é uma máquina que produz subjetivações e, assim, é uma máquina de governo.[416]

Pensá-los separadamente – sujeito e objeto, motorista e carro, agente e arma, ser humano e tecnologia – já não explica a mediação técnica contemporânea. Humanos não estão por si sós. (Talvez jamais tenham estado. Kerckhove sugere que desde sempre desenvolvemos relações quase biônicas com as nossas invenções e que nunca houve um "homem natural", nem mesmo o de Jean-Jacques Rousseau.[417]) E artefatos e tecnologias não imprimem cadeias de causa e efeito sobre humanos maleáveis. A ação não é simplesmente uma propriedade de humanos, mas uma associação de atuantes. (Latour é um dos autores que sugerem que, em razão do desconforto que o termo "agente" traz para a contribuição de entes não humanos para uma ação, a alcunha "atuante" proporciona uma identificação mais adequada.) Para Latour o adjetivo "técnico", dentre vários sentidos possíveis, pode designar um tipo específico de movimento que atravessa os entes com um tempo diferente, espaços diferentes, propriedades diferentes, ontologias diferentes, fazendo-os compartilharem o mesmo destino, então criando um novo atuante.[418]

A partir dessas reflexões, torna-se possível que sejam desenvolvidas novas formas de compreender outros conjuntos de humanos/objetos. E que se questione se a vida social é simplesmente o resultado de relações entre seres humanos ou se colaborações entre seres humanos e objetos materiais contribuem para a formação de sociedades, dando-lhes características próprias.

---

[415] AGAMBEN, Giorgio. "O que é um dispositivo?", *op. cit.*, p. 13.
[416] *Ibid*., p. 15.
[417] KERCKHOVE, Derrick de. *A pele da cultura*, *op. cit.*, p. 235.
[418] LATOUR, Bruno. *Pandora's hope*, *op. cit.*, p. 192.

Brown foi responsável por analisar a questão do atuante no ciberespaço.[419] Segundo ela, para o direito, o corpo tradicionalmente compreende o corpo criminalizado, o corpo (probatório) culpável, o corpo punível, o corpo vitimizado. O indivíduo, incorporado, tornou-se um ponto de referência estável para fundamentar, interpretar e avaliar o estado de ordem social. No entanto, uma vez que o corpo não pode ser concebido como inteiramente "humano" em redes tecno-sociais, temos experimentado uma percepção da falsidade do conceito de personalidade puramente incorporada, o que faz com que passemos a pensar o corpo como um *corpo-atuante*.[420] Afinal, questiona Brown[421], o humano é necessariamente incorporado?

Rejeitando a presunção de que a tecnologia é um objeto, um instrumento, para utilização pelo homem, e se fundamentando no complexo realinhamento de atores e artefatos, Brown prefere reconfigurar o objeto como participante ativo, rematerializar o mundo virtual, descrevendo *atuantes* em vez de *atores*: "Atuantes são entidades simultaneamente informacionais e orgânicas, no sentido mais profundo, tecnologia coextensiva com o sensório humano, sua individualidade/personalidade".[422]

3.4 UMA QUESTÃO DE GÊNERO

Ainda que não seja uma questão principal nesta tese, é válida a referência a uma preocupação presente nos recentes trabalhos sobre os atuantes de *cybercrimes*: o gênero.

É interessante notar que na primeira descrição literária do ciberespaço (*Neuromancer*, 1984), William Gibson chama o ambiente virtual de dados de *matrix*:

> Case tinha vinte e quatro anos. Aos vinte e dois era um cowboy [hacker], cowboy fora da lei, um dos melhores no Sprawl. Ele havia sido treinado pelos melhores, McCoy Pauley e Bobby Quine, lendas do negócio. Na época, operava num barato quase permanente de adrenalina, subproduto da juventude e da proficiência, conectado num deck de ciberespaço customizado que projetava sua consciência desincorporada na alienação consensual que era a matrix.[423]

A raiz indo-europeia *matr-* faz referência à maternidade. Sua expressão latina (*matrix*) conota os sentidos de mãe, fêmea que cria seus filhos, ventre, útero.

---

[419] BROWN, Sheila. "The criminology of hybrids: Rethinking crime and law in technosocial networks", *op. cit.*
[420] *Ibid*., p. 231.
[421] *Ibid*., p. 234.
[422] *Ibid*., p. 230, 235-236.
[423] GIBSON, William. *Neuromancer, op. cit.*, p. 89.

Foi uma mulher quem escreveu o primeiro algoritmo para ser processado por uma máquina analítica (projeto de computador mecânico): Ada Lovelace, nascida Byron (1815-1852). Se estendermos um pouco mais essa reflexão, percebe-se que, ainda antes, foi uma mulher quem primeiro se deu conta da possibilidade da tecnologia dar forma a uma vida artificial: Mary Shelley, nascida Godwin (1797-1851) – curiosamente, amiga de Lord Byron, pai de Ada Lovelace. E o próprio "pai da computação", Alan Turing (1912-1954), quem, após ter sido descoberto homossexual, foi obrigado a escolher entre uma pena de prisão ou uma suspensão condicional da pena com a obrigação de passar por tratamento hormonal (aplicação do hormônio feminino estrogênio) para reduzir sua libido.

A partir dessas reflexões, Plant sugere que é aparente – e enganosa – a impressão de que a cultura em rede é dominada por homens e pelas intenções e pelos projetos masculinos: "há mais do que pode ver o olhar masculino".[424] A autora nos lembra que as primeiras telefonistas, operadoras e calculadoras eram mulheres. E também as primeiras programadoras: Ada Lovelace escreveu o primeiro algoritmo sem que o protótipo de computador fosse criado; em 1944, quando a máquina foi finalmente construída, ela foi programada por Grace Murray Hopper. Segundo a autora, os feitos das mulheres nas escolas e universidades excedem a de seus colegas homens; a comunicação global e a migração do capital ocidental estão minando o mundo masculino branco e as estruturas patriarcais do sul e do oriente, trazendo um poder econômico sem precedentes às mulheres trabalhadoras e multiplicando as possibilidades de comunicação, aprendizado e acesso a informação; as "*replicunts*" escrevem programas, abrem novos furos no mundo, se infiltram nas artes e nas indústrias, pervertem códigos, hackeam controles de segurança, corrompem as transmissões, descobrindo sua própria pós-humanidade.[425] "Elas estão no limite do novo limite, despudoradamente oportunistas, inteiramente irresponsáveis e comprometidas somente com a infiltração e a corrupção de um mundo que já lamenta o dia em que elas saíram de casa".[426]

No entanto, pesquisa realizada Hutchings e Chua, com análise de dados quantitativos e qualitativos coletados na Austrália e no Reino Unido, confirma que

[424] PLANT, Sadie. "On the matrix: cyberfeminist simulations" In BELL, David; KENNEDY, Barbara M. *The cybercultures reader*. London, New York: Routledge, 2000. p. 325.
[425] *Ibid*., p. 325, 334, 336.
[426] *Ibid*., p. 336.

poucos *cybercrimes* são cometidos por mulheres.[427] A desproporcional participação feminina nos *cybercrimes* é comparável à sua reduzida presença nos registros dos crimes tradicionais. Mas os motivos para o pouco envolvimento feminino nos *cybercrimes* são distintos:

- *Acessibilidade ao conhecimento formal*: O campo das ciências da computação revela pouca participação de estudantes mulheres e, no caso daquelas que ingressam nos estudos, verifica-se que a falta de apoio de professores e colegas pode diminuir o grau de confiança das estudantes. Assim, as mulheres acabam tendo oportunidades mais restritas de serem treinadas no conhecimento necessário para se envolverem com a tecnicidade dos *cybercrimes*.

- *Acessibilidade ao conhecimento informal*: Fóruns virtuais são espaços onde hackers comunicam, aprimoram e compartilham seus valores, normas e técnicas. Existe uma possível suposição de que a ausência de uma imediata identificação biológica pode tornar o espaço virtual num ambiente de livre construção de gênero, onde os usuários podem escolher suas performances de acordo ou não com seu sexo biológico. Recentes estudos confirmam-na parcialmente ao sugerir que gêneros, no contexto virtual, são mais fluidos e mais facilmente adaptáveis às respectivas necessidades individuais. Porém, apesar dessa maior flexibilidade, também se evidencia que se mantêm desafios e adversidades que as mulheres enfrentam em espaços e comunidades online. Hackers femininas são percebidas com absoluto desdém ou em alta consideração pela comunidade hacker geral.

Hutchings e Chua identificaram que 78,6% dos casos registrados no Cambridge Computer Crime Database – banco de dados sobre *cybercrimes* no Reino Unido – correspondiam a atuantes masculinos, enquanto a participação feminina se limitava a 12,1%. (Para 9,2% dos casos, o gênero era desconhecido.) Para esse levantamento, as pesquisadoras consideraram os registros de hacking, ciberfraudes, DDoS e utilização de *malware*, categorizados como "técnicos" (aqueles que exigem um conhecimento mais

[427] HUTCHINGS, Alice; CHUA, Yi Ting. "Gendering cybercrime", In HOLT, Thomas J. (ed.). *Cybercrime through an interdisciplinary lens*. London: Routledge, 2017, p. 167-188.

profundo ou um conjunto de habilidades específicas) e "gerais" (aqueles menos complicados, que podem ser realizados por meio de abuso de confiança ou a partir de engenharia social). De acordo com a pesquisa, era menos provável que mulheres cometessem, ou fossem suspeitas de cometer, violações técnicas, se comparadas aos homens. E, comparado com os homens, era mais provável que as mulheres tivessem um papel "periférico" na violação – fosse por meio de auxílio à infração principal ou por uma conduta acessória (como a lavagem de dinheiro) –, o que corresponde a funções menos técnicas e menos graves.

Os gêneros, de acordo com Plant, podem ser flexionados e matizados e, tal como as coordenadas de tempo-espaço, tendem a ser perdidos.[428]

> Mas, o ciberespaço está fora do controle do homem: a realidade virtual destrói a identidade, a digitalização está mapeando sua alma e, no auge de seu triunfo, a culminação de suas ereções mecânicas, o homem confronta o sistema que ele construiu para sua própria proteção e descobre que ela é feminina e perigosa.[429]

A questão de gênero dos atuantes é um dos possíveis desdobramentos das criminologias *cyber*, o que confirma o potencial de derivações teóricas que podem ser produzidas pelos estudos criminológicos alternativos sobre os *cybercrimes*.

[428] PLANT, Sadie. "On the matrix: cyberfeminist simulations", *op. cit.*, p. 328.
[429] *Ibid*., p. 335.

4 *CYBERCRIMES*

A terminologia notória "*cybercrime*" não é a mais acertada para uma prudente análise das possíveis violações sociais e legais cometidas no ciberespaço. Na análise de um fenômeno global, a referência a "crime" não pode pressupor somente a descrição legal do ato como socialmente danoso e a previsão legal de pena – critérios criticados por Sutherland para explicar por que os *crimes de colarinho-branco* eram, de fato, crimes apesar de não tipificados como tais.[430] Em recente discussão com Pat Carlen, pareceu-nos mais acertado diferenciar três categorias dinâmicas dessas violações:

- *Cybercrime* é a violação de uma norma legal; o comportamento foi explicitamente proibido pela lei, ou seja, criminalizado em determinada jurisdição local. Capeller denomina os atuantes de *cybercrimes* de *netcriminals*.[431]

- *Cyber violation*, ou *cyber deviance*, é a violação de um regramento social; há um significado social à violação, considerada indesejável ou censurável, mas não de uma norma legal[432]. Capeller refere-se, então, a *netdeviants*.[433]

- E *neo cyber threat* é a prática de ato injusto, desenvolvida a partir da própria natureza da tecnologia, mas contra a qual não há (ainda) qualquer regra local ou universal sob a qual ela possa ser categorizada (dado um sentido). Em outras palavras: enquanto não constitui uma conduta criminosa em algumas jurisdições, uma *neo cyber threat* é geralmente tratada como um problema técnico ou uma novidade, e seu sentido não tende a gerar imediata reprovação social e a traduzir a gravidade nem a dramaticidade do termo "crime", o que pode ser alterado em decorrência de possíveis danos

---

[430] SUTHERLAND, Edwin Hardin. "Is 'White Collar Crime' Crime?", *American Sociological Review*, v. 10, n. 2, 1945, p. 132-139.
[431] CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", *op. cit.*, p. 234.
[432] Um exemplo, citado por Yar é paradigmático: os dois programadores filipinos que criaram o *worm* ILOVEYOU, que atacou dezenas de milhares de computadores, em meados do ano 2000, causando prejuízos estimados entre US$ 7 e 10 bilhões, foram absolvidos de todas as acusações imputadas a eles em razão da falta de leis sobre crimes cibernéticos nas Filipinas à época. (YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 2.)
[433] CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", *op. cit.*, p. 234.

> causados pela ameaça, por sua maior difusão e/ou pela melhor compreensão dela.

Mas, porque o espaço deste ensaio não permite maiores elucubrações sobre essas distinções, opto por manter o termo *cybercrime* pela facilidade de tratamento. Portanto, a conotação que *cybercrime* implica aqui é ainda mais ampla: crimes aqui são quaisquer condutas interpretadas como tais por normas, reações sociais, estudos ou por declarações políticas ou jornalísticas. Nesse mesmo sentido, Yar argumentou que um problema primário para a análise de *cybercrime* é a ausência de uma definição atual consistente.[434] Consequentemente, prossegue Yar, em vez de tentar definir os estágios de emergência e reconhecimento de diferentes graus do que poderia ser chamado de cibercriminalização, "o termo [*cybercrime*] pode ser melhor compreendido para significar uma *variedade* de atividades ilícitas cujo denominador comum é o papel central desempenhado por redes de tecnologia da informação e comunicação em sua comissão."

Partindo da premissa de que eventual criminalização das violações no ciberespaço deve ter por fim a proteção da capacidade funcional do sistema, Moreira de Oliveira define os *cybercrimes* (que ele denomina "delitos informáticos") como condutas realizadas com o intuito de alterar, destruir, copiar, inserir ou obter dados, afetando o funcionamento de um sistema, causando-lhe paralisação, temporária ou permanente, indisponibilidade de acesso ou de dados, ou diminuindo, de qualquer forma, o seu desempenho frente ao fim que se destina.[435] Por mais que sua pesquisa tenha uma preocupação muito mais dogmática sobre a tipificação de condutas executadas pela internet, o conceito apresentado pelo autor merece referência porque reacomoda adequadamente a tecnologia da informação como fonte, centro e alvo dos *cybercrimes* próprios.

Pérez Suárez sugere que talvez não haja necessidade de uma tal definição e que pode ser mais prudente a referência a um conceito "guarda-chuva" ou a uma metaestrutura tão infinitamente líquida que é capaz de conter uma miríade de fenômenos cambiantes que se alteram e se adaptam conforme a tecnologia acontece.[436]

---

[434] YAR, Majid. "The Novelty of 'Cybercrime': As Assessment in Light of Routine Activity Theory", *op. cit.*, p. 409; *Idem*. *Cybercrime and society*, *op. cit.*, p. 9.
[435] MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*, *op. cit.*, p. 96.
[436] PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*, *op. cit.*, p. 34.

Também, e mais substancialmente, o dinamismo característico da tecnologia da informação também influencia na compreensão conceitual dos *cybercrimes*. Para Wall, *cybercrimes* são "atividades criminais ou prejudiciais que são informacionais, globais e em rede"[437], e "que envolvem a aquisição ou manipulação de informação em prol de vantagem"[438]. A partir desse conceito, Wall limita os *cybercrimes* àquelas atividades que são produto da tecnologia em rede e que transformaram a divisão do trabalho criminoso, oferecendo oportunidades inteiramente novas, ou seja, novas formas de crimes. Mas, para o autor, eles não devem ser compreendidos como uma ideia imutável. Wall identifica, no seu desenvolvimento fenomenológico, variações de sentido que podem ser categorizados cronologicamente como gerações distintas de crimes. Ele justifica sua opção por dispor os *cybercrimes* num enquadramento de tempo, ao invés de organizá-los conforme argumento de espaço, porque assim se evidencia como sucessivas gerações foram definidas por diferentes estágios de desenvolvimento tecnológico.[439]

Para distinguir as diversas manifestações ofensivas da tecnologia da informação, Wall propõe uma "tese de transformação", que consiste em questionar o que resta, no todo que chamamos de *cybercrimes*, se aquelas mesmas tecnologias em rede forem retiradas da equação. O teste, diz ele, não pretende ser científico; em vez disso, trata-se de um instrumento heurístico, uma regra geral.[440] A noção de transformação lhe permite (i) oferecer um aspecto geral e reconciliatório de tipos de *cybercrimes* aparentemente distintos ao categorizá-los em diferentes fases de um processo de mudança, e (ii) compreender que as mesmas tecnologias que criam os *cybercrimes* também fornecem a oportunidade para sua regulação e seu controle.

A distinção temporal dos *cybercrimes* não é um método exclusivo de Wall. Hollinger também apresenta uma divisão particular desse fenômeno criminal, em quatro períodos distintos.[441]

O primeiro, considerado um período de descoberta e descrição do abuso da tecnologia da informação, cobriu um intervalo de três décadas (1946 a 1976). Como nesses anos a referência aos computadores remetia, em grande parte, aos sistemas de

---

[437] WALL, David S. *Cybercrime*, *op. cit.*, p. 4.
[438] *Ibid*., p. 10.
[439] *Ibid*., p. 48.
[440] *Ibid*., p. 34.
[441] HOLLINGER, Richard Clifton. "Computer Crime" In LUCKENBILL, David; PECK, Denis (eds.). *Encyclopedia of crime and juvenile delinquency (vol. II)*. Philadelphia: Taylor and Francis, 2001. p. 76-81.

mainframes, as violações mais comuns referiam-se a prejuízos patrimoniais: computadores eram vandalizados, destruídos, subtraídos.

A partir do desenvolvimento dos computadores pessoais – ainda raros, porém já mais acessíveis –, surgiram as possibilidades de instrumentalização dos computadores para a perpetração de crimes patrimoniais tradicionais: furto de valores passaram a ser realizados com transferências não autorizadas; fraudes diversas revestiram-se em faturas de cobrança enviadas pela internet. Ainda que poucos crimes realmente lesivos fossem perpetrados, o prognóstico de jovens *hackers* promovendo o caos institucional ou quiçá iniciando acidentalmente a Terceira Guerra Mundial deu ensejo à principal atividade do segundo período (1977 a 1987): a "correção" de inúmeras deficiências e inadequações no direito penal e a criminalização do uso ilícito da tecnologia da informação. Mas, mesmo com a promulgação de estatutos legais sobre o tema, em diversos países, o público em geral ainda não percebia os *cybercrimes* como um problema social tão relevante e poucos infratores eram processados.

No intervalo de cinco anos entre 1988 e 1992, porém, constituiu-se um terceiro período caracterizado por um vigoroso esforço de aplicação legal para identificação, apreensão e responsabilização dos indivíduos considerados infratores virtuais; foi o momento da demonização de *hackers* e *crackers*.

Por fim, a última fase, que se iniciou em 1993 e se estendeu por quase uma década (a análise de Hollinger limita-se ao ano da publicação de seu texto), foi rotulada como o período de censura, quando o foco de atenção voltou-se à limitação de acesso dos usuários de computadores a materiais "perigosos" diversos disponíveis na internet.

Apesar de historicamente esclarecedora, a metodologia de Hollinger se estrutura na reação social ao fenômeno dos *cybercrimes*; ou melhor, cada fase indica por que e para o que se voltou o processo de criminalização.

Ambos Wall e Hollinger apresentam análises sociológicas. Mas, enquanto o foco de Hollinger está sobre reação social ao novo mundo da tecnologia *cyber*, Wall se concentra mais na relação entre técnica e saber. A categorização dos *cybercrimes* a seguir acompanha a distinção geracional elaborada por Wall, com algumas adaptações.

4.1 PRIMEIRA GERAÇÃO: CYBERCRIMES TRADICIONAIS (OU ORDINÁRIOS)

Os *cybercrimes* de primeira geração aconteciam (e acontecem) em sistemas de computação distintos e se caracterizaram pela exploração criminosa de computadores *mainframes* e de seus sistemas operacionais. Trata-se de crimes *tradicionais* (Wall) ou *ordinários* (McQuade) nos quais os computadores são utilizados no estágio preparatório do crime, como uma ferramenta de comunicação, para obter informações preparatórias, enfim, para assistir violações tradicionais. Como exemplo, podemos imaginar a utilização da internet para o recrutamento de potenciais atuantes, para o estudo de mapas na preparação para um crime, ou para a instrução de como fabricar produtos proibidos a partir de tutoriais disponíveis na rede. Por esse motivo, Brenner chama-os de *cybercrimes* incidentais.[442]

Como já mencionado (p. 21-22), (*cyber*)crimes categorizados como tradicionais são aqueles cometidos no assim chamado mundo real: as condutas para o cometimento do crime, as circunstâncias envolvidas no ato e os resultados dele ocorrem em espaços concretos. Essa concepção é pautada pelo próprio modelo de direito penal moderno, o qual, como premissa fundamental, limita a responsabilização às condutas, ativas ou omissivas, que ocorram no mundo físico, excluindo de sua alçada as ações não externalizadas, como os pensamentos.[443] Nos crimes dessa primeira geração, a extração da tecnologia da equação criminosa não evita a execução criminosa, que pode ocorrer por outros meios.[444]

4.2 SEGUNDA GERAÇÃO: CYBERCRIMES HÍBRIDOS (OU ADAPTATIVOS)

Os *cybercrimes* de segunda geração, por sua vez, são aqueles cometidos através de redes. São crimes *híbridos* (Wall) ou *adaptativos* (McQuade), também passíveis de serem descritos como crimes tradicionais para os quais surgiram novas oportunidades globalizadas. Extraída a internet da equação, o comportamento infrator permanece; todavia, as novas oportunidades de infrações desaparecem e o comportamento se realiza por outros meios, em menores número e escala.[445] A hipótese, compartilhada por Brenner, é que crimes tradicionais também podem ocorrer nos dois espaços – na

[442] *Apud* PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*, *op. cit.*, p. 36.
[443] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 10.
[444] WALL, David S. *Cybercrime*, *op. cit.*, p. 44-45.
[445] *Ibid*., p. 45-47.

realidade *física* compartilhada e na realidade *conceitual* compartilhada –, sem que sejam distintos em seus elementos constitutivos, o que se aproxima da noção de *continuidade* de Capeller.[446]

No mesmo sentido, porém criticando o apelo dos "vulgarizadores da norma penal" em criminalizar condutas danosas que envolvam a utilização de computadores, Moreira de Oliveira argumenta que "a grande maioria das ações tidas como crimes informáticos encontram-se já previstas no atual ordenamento jurídico, porém, sem a desejada roupagem de 'Crimes de Computador'".[447] Crimes contra o patrimônio (subtração de valores, extorsão, dano, estelionato), por exemplo, podem correr no espaço físico e no espaço virtual, preservados os mesmos elementos de conduta, circunstâncias pertinentes e resultado de dano. Nesses casos, o ciberespaço é somente o meio pelo qual o crime é realizado.[448] O mesmo pode ser dito quanto aos crimes contra a honra (calúnia, difamação e injúria), contra a liberdade individual (constrangimento ilegal, ameaça), contra a intimidade (violação de correspondência, divulgação de segredos, interceptação de dados), contra a propriedade imaterial (apropriação, pirataria), contra pessoas especialmente protegidas (pedofilia), crimes econômicos (lavagem de dinheiro).

Os exemplos a seguir são categorizados em três criminologias qualitativamente distintas, conforme originalmente proposto por Wall.[449] Essa classificação, porém, não é fixa e exclusiva (e tampouco se limita aos *cybercrimes* híbridos), havendo tipos de *cybercrimes* que flexionam esses limites e integram a combinação de dois ou três grupos.[450]

4.2.1 Violações contra a integridade dos sistemas de informação

Assim, algumas dessas violações são contra a integridade dos sistemas de informação, ou seja, elas visam a própria rede de comunicações eletrônicas, alvejando tanto o hardware quanto o software do computador.[451] Em entendimento um pouco

---

[446] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*; CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", *op. cit.*
[447] MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*, *op. cit.*, p. 67.
[448] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 41-43.
[449] WALL, David S. *Cybercrime*, *op. cit.*
[450] *Ibid.*, p. 49.
[451] YAR, Majid. "Online Crime", *op. cit.*

distinto, Brenner intitula-as como *cybercrimes* de alvo, nos quais o computador é invadido (*hacking*) ou bombardeado (DDoS).[452]

4.2.1.1 *Hacking*

Trata-se do acesso não autorizado a espaços sobre os quais os direitos de propriedade ou acesso já foram estabelecidos, por meio de aproveitamento de falhas de segurança, com ampla variedade de motivações e atividades.[453] O acesso não autorizado pode ter, mas nem sempre, como consequências: o uso dos recursos dos computadores invadidos (armazenamento de arquivos, uso da banda, criação de *botnets*); subtração de dados; alteração, sabotagem e destruição de sistemas[454]; desconfiguração e falsificação de *websites*.[455]

Por mais que o termo *hacking* tenha uma referência limitada ao acesso não autorizado, é importante esclarecer que a palavra é ampla e genericamente utilizada para uma variedade de violações que afetam computadores e aparelhos em rede, seja por assumir controle deles, por alterar ou danificar seu normal funcionamento ou pela apropriação de conteúdo.[456] Quando executado por agentes estatais – visando outros governos, cidadãos estrangeiros ou sua própria população –, para obtenção de informações de inteligência sobre as capacidades e estratégias econômicas, políticas e militares, assim como para minar suas capacidades por meio de sabotagem, o *hacking* é mais recorrentemente caracterizado como *cyberwarfare*.[457]

A desconfiguração (*defacement*) de *websites* constitui um tipo de vandalismo virtual no qual um ou mais hackers insere ou altera códigos, expondo os visitantes do site a informações enganosas ou provocativas. Essa desconfiguração varia de modificações leves (como a inserção de anotações humorísticas) a outras mais graves (como a sabotagem e corrupção do conteúdo do site). Ao evidenciar a inadequação das medidas de segurança de empresas ou de agências governamentais, a desconfiguração

---

[452] *Apud* PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*, *op. cit.*, p. 36.
[453] WALL, David S. *Cybercrime*, *op. cit.*, p. 53.
[454] Yamaguchi defende que a destruição de elementos de *hardware* do computador, obstruindo a função de processamento de dados, caracteriza um crime de dano (ou *computer sabotage*); por outro lado, a destruição de *software*, por outra forma que a física, como o apagamento de programa, constitui manipulação de dados. (ver MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*, *op. cit.*, p. 78.)
[455] YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 28-30.
[456] YAR, Majid. "Online Crime", *op. cit.*
[457] *Ibidem*.

causa prejuízos à credibilidade e à reputação das organizações, afastando clientes e usuários.[458]

Quando os atos têm como consequência a quebra (*crack*) de um sistema de segurança ou a produção de dano, a atividade é denominada *cracking*. Brenner interpreta extensivamente o *hacking* como uma invasão de propriedade e o *cracking* como uma invasão de propriedade com intenção de cometer crime subsequente.[459]

Com uma interpretação catalogadora distinta, Yar categoriza o *hacking* como um tipo de *cybercrime* de terceira geração; para ele, o *hacking* somente é possível pela existência e pela arquitetura da própria rede de computador, sem as quais não poderia existir.[460] Todavia, e de forma provocativa, o hacker Jake Leslie Davis (aka Topiary), ex-membro do coletivo Anonymous, em palestra feita para um evento da revista Wired, em 2013, demonstrou como realizou um *hacking* (invasão de propriedade) no mundo físico contra um dos organizadores do evento.[461]

4.2.1.2 Ciberespionagem

Também envolve acesso não autorizado para a obtenção ilícita de informações consideradas privadas ou confidenciais. A ciberespionagem pode ser executada por motivos particulares (como conflitos conjugais), comerciais (quando empresas buscam informações sigilosas de concorrentes: novas ofertas, lista de fornecedores ou consumidores, projetos de produtos, mensagens internas) ou governamentais (quando agências de governo monitoram outros governos ou seus próprios cidadãos).

Contudo, ao contrário de *hackers* e *crackers*, os *cyber-spies* não buscam reconhecimento público de suas atividades e trabalham com discrição nas invasões para obtenção de informações restritas.

4.2.1.3 Ciberextorsão

É uma extorsão realizada por meio de um *ransomware*. Com ele, os dados de um sistema são ilicitamente criptografados e é exigido o pagamento de um "resgate" (ou a concordância em distribuir o software malicioso) em troca da chave de criptografia.

---

[458] SIEGEL, Larry J. *Criminology*, *op. cit.*, p. 477.
[459] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 77-86.
[460] YAR, Majid. "Online Crime", *op. cit.*
[461] https://www.youtube.com/watch?v=DurOYPdXyF4

4.2.1.4 Ciberterrorismo

> O ladrão moderno pode roubar mais com um computador do que com uma arma. Conclui-se, então, que o terrorista de amanhã pode ser capaz de causar mais danos com um teclado do que com uma bomba?[462]

O ciberterrorismo utiliza a tecnologia da informação para atacar *infraestrutura crítica* com a *finalidade de provocar terror* social ou generalizado, expondo a perigo pessoa e/ou patrimônio, e, assim, manipular a agenda política. Exemplos: ataques ao suprimento de água e alimentos, ao fornecimento de energia, a sistemas de telecomunicação, ao controle do tráfego de trens e aviões, a sistemas hospitalares, de transações financeiras, de segurança e emergência, ou a ativos materiais de importante conteúdo simbólico.

Nesse sentido, uma das melhores definições de ciberterrorismo foi apresentada por Dorothy Denning perante o House Armed Services Committee, em maio de 2000:

> O ciberterrorismo é a convergência do ciberespaço e do terrorismo. Ele se refere a ataques ilícitos e a ameaças de ataques contra computadores, redes e a informação ali armazenada, quando realizados para intimidar ou coagir um governo ou sua população em prol de objetivos políticos ou sociais. Mais, para se qualificar como ciberterrorismo, um ataque deve resultar em violência contra pessoas ou propriedade, ou, ao menos, causar dano suficiente para gerar medo. Ataques que levam à morte ou à lesão corporal, explosões, ou graves perdas econômicas seriam exemplos. Graves ataques a infraestruturas críticas podem ser atos de ciberterrorismo, dependendo do seu impacto. Ataques que interrompem serviços não essenciais, ou que são sobretudo um incômodo caro, não são.[463]

Berner recorre a uma definição um pouco distinta. Para ele, o ciberterrorismo caracteriza o "ataque premeditado e politicamente motivado contra sistemas e programas de computador, dados e informações, que resulte em violência contra alvos não combatentes, por grupos subnacionais ou agentes clandestinos."[464]

Três características principais merecem atenção. Primeiro, Berner considera fundamental a motivação política; assim, eventual ataque promovido por um hacker, motivado pelo desafio técnico da invasão, ao sistema de defesa de um país, ainda que

---

[462] BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *South African Journal of Information Management*, v. 5, n. 1, 2003.
[463] *Apud* WEIMANN, Gabriel. *Cyberterrorism*: how real is the threat? Washington: United States Institute of Peace, 2004. p. 4.
[464] BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *op. cit.*

resulte em prejuízos ou em potencial risco de dano, não configura um ato ciberterrorista. A agenda política do atuante é um fator necessário. Segundo, Berner torna evidente que o ataque ciberterrorista atinge a arquitetura ou o conteúdo da tecnologia da informação, causando com isso violência para pessoas ou infraestruturas críticas. Terceiro, ele limita a autoria do ciberterrorismo a grupos não institucionais ("subnacionais") ou politicamente ilegítimos ("clandestinos"), excluindo a possibilidade de Estados e seus agentes serem autores de atos ciberterroristas.

Brenner interpreta o ciberterrorismo como uma declinação do crime de terrorismo tradicional.[465] De fato, se analisarmos a lista de potenciais atos terroristas feita por Collin[466], quem cunhou o termo *cyber-terrorism* na década de 1980[467], confirmaremos que, neste caso, a tecnologia da informação não fez surgir tipos inéditos de ações, mas permitiu uma maior amplitude para atos terroristas tradicionais:

> - Um ciberterrorista acessará remotamente os sistemas de controle de processamento de um fabricante de cereais, alterará os níveis de suplemento de ferro, e fará adoecer e matará as crianças de uma nação que desfrutam de sua comida. O ciberterrorista, então, executará similares alterações remotas em um processador de fórmula infantil. A chave: o ciberterrorista não precisa estar na fábrica para executar esses atos.
>
> - Um ciberterrorista colocará diversas bombas computadorizadas ao redor de uma cidade, todas transmitindo simultaneamente padrões numéricos únicos, cada bomba recebendo o padrão de cada outra. Se a bomba um para de transmitir, todas as bombas detonam simultaneamente. As chaves: 1) o ciberterrorista não precisa estar amarrado a qualquer dessas bombas; 2) não é necessário qualquer caminhão grande; 3) o número de bombas e a dispersão urbana são vastos; 4) os padrões criptografados não podem ser previstos e combinados por meio de transmissão alternativa; e 5) o número de bombas impede o desarmamento de todas elas simultaneamente. As bombas detonarão.
>
> - Um ciberterrorista interromperá as transações bancárias e financeiras internacionais, as bolsas de valores. A chave: a população de um país perderá toda confiança no sistema econômico. Um ciberterrorista tentaria entrar no prédio do Federal Reserve ou equivalente? Pouco provável, uma vez que a prisão seria imediata. Além disso, uma longa fila de caminhões ao lado do prédio seria notada. No entanto, no caso do ciberterrorista, o perpetrador está sentado num outro continente, enquanto os sistemas econômicos de uma nação param de funcionar. A desestabilização será alcançada.
>
> - Um ciberterrorista atacará a próxima geração de sistemas de controle do tráfego aéreo e colidirá duas grandes aeronaves civis. Esse é um cenário realista, pois o ciberterrorista também destruirá os sensores da cabine das aeronaves. O mesmo pode ser feito com as linhas férreas.

[465] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 95-98.
[466] COLLIN, Barry C. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", *Proceedings of 11th Annual International Symposium on Criminal Justice Issues*. The University of Illinois at Chicago, 1996.
[467] BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *op. cit.*

> - Um ciberterrorista alterará remotamente as fórmulas de medicamentos nas indústrias farmacêuticas. A potencial perda de vida é incomensurável.
>
> - Um ciberterrorista pode, então, decidir mudar remotamente a pressão nas tubulações de gás, causando uma falha na válvula e a explosão e o incêndio de uma quadra de um pacato subúrbio. Igualmente, a rede elétrica está continuamente se tornando mais vulnerável.

Os exemplos refletem condutas tradicionalmente criminalizadas nos ordenamentos jurídicos, respectivamente: alteração de produto alimentício destinado a consumo, tornando-o nocivo à saúde; atentado (terrorista) contra a vida ou a integridade física de pessoas; sabotagem (terrorista) da rede bancária e dos meios de transporte; alteração de produtos medicinais; sabotagem (terrorista) de instalações de gás ou da transmissão de energia. Em resumo, trata-se do terrorismo tradicional para o qual a tecnologia da informação proporcionou novas oportunidades de execução e extensão dos danos.

Estudiosos[468] apontam condições desenvolvidas no ciberespaço – já descritas nesta tese – que potencializam o risco da utilização da tecnologia da informação para atos terroristas: o reduzido investimento (se comparado com o preço de armamento de fogo e explosivo), a possibilidade de executar atos à distância, a ausência de fronteiras físicas para atravessar ou de funcionários da imigração, o anonimato e a dissimulação técnica, o empoderamento de atuantes individuais ou de grupos pequenos, o menor risco de vida para os atuantes e o maior potencial do resultado pretendido.

Uma vez que se trata de uma questão mais contemporânea, é importante que, desde já, sejam tomadas duas cautelas com relação ao ciberterrorismo: evitar reproduzir pré-conceitos tradicionais e evitar superestimar hollywoodianamente as possibilidades do ciberterror. Siegel, por exemplo, afirma que "organizações terroristas estão começando a entender o poder destrutivo que a guerra *cyber* pode infligir em seus inimigos, ainda que, ironicamente, elas possam vir de uma região onde os bancos de dados de computadores e a internet não são amplamente utilizados".[469] Essa observação pode refletir a equívoca impressão de terroristas como sendo tipicamente um grupo de indivíduos rudimentares, de comportamento tribal e de motivações religiosas fanáticas. Trata-se do senso comum que retrata basicamente muçulmanos (africanos ou orientais)

---

[468] WEIMANN, Gabriel. *Cyberterrorism*, *op. cit.*, p. 6; YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 53-54.
[469] SIEGEL, Larry J. *Criminology*, *op. cit.*, p. 480.

como terroristas. De qualquer modo, aqui parafraseando Dalla Vigna[470], é fato que quem é demasiado pobre para a bomba atômica tem, todavia, à disposição o ciberterrorismo, agora ao alcance de todos. Analisando as possibilidades do *cyberwarfare*, Yar também esclarece como as atividades no ciberespaço podem estabelecer um equilíbrio de forças em conflitos que, de outro modo, seriam assimétricos, tanto em poder quanto em recursos:

> Estados pequenos podem não ser capazes de se igualar a seus poderosos correspondentes em termos militares ou econômicos, mas poderiam utilizar as ferramentas de *cyberwarfare* para lançar ataques eficazes. De fato, a grande dependência de nações tecnologicamente avançadas em sistemas de computador, por todas as classes sociais, torna sua "infraestrutura informacional crítica" ainda mais vulnerável a ataques *cyber*, que poderiam causar prejuízos às atividades financeiras e econômicas, e causar grande perturbação a serviços essenciais como transporte, eletricidade e telecomunicações.[471]

Siegel também causa alarme ao alegar que as "organizações terroristas estão adaptando a tecnologia da informação a seu arsenal de terror", e, por isso, "as agências do sistema de justiça têm de estar preparadas para um ataque contínuo sobre a infraestrutura eletrônica da nação".[472] Na década anterior Collin havia anunciado: "Não se enganem, *as ameaças são reais, hoje*".[473] Nesse ponto, é importante ressaltar que o ciberterrorismo constitui mais uma ameaça (também um ornamento retórico e uma confusão com o ciberativismo) do que evidência concreta de que grupos terroristas estejam se adaptando para ataques a infraestruturas críticas por meio da tecnologia da informação.[474] Thomas argumenta que o *cyberfear* é gerado pela associação, nem sempre real, entre o que *poderia acontecer* e o que *acontecerá*.[475] Berner afirma que houve poucos, se é que houve, ataques a redes de computadores que satisfazem os critérios do conceito de ciberterrorismo.[476] Weimann, por sua vez, alega que "a ameaça potencial é, de fato, muito alarmante; todavia, apesar de todas as sombrias previsões,

---

[470] DALLA VIGNA, Pierre. "Guerra local e guerra total" In PERNIOLA, Mario; FORMENTI, Carlo; DALLA VIGNA, Pierre; VILLANI, Tiziana; GUATTARI, Felix; BAUDRILLARD, Jean. *Guerra virtual e guerra real*: reflexão sobre o conflito do Golfo. Lisboa: Vega/Passagens, 1991. p. 73. O texto original diz: "Quem é demasiado pobre para a bomba atómica tem todavia à disposição as armas químicas e bacteriológicas, agora ao alcance de todos."
[471] YAR, Majid. "Online Crime", *op. cit.*
[472] SIEGEL, Larry J. *Criminology*, *op. cit.*, p. 480.
[473] COLLIN, Barry C. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", *op. cit.*, grifos no original.
[474] YAR, Majid. "Online Crime", *op. cit.*
[475] THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *op. cit.*, p. 115.
[476] BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *op. cit.*

nem um único caso de ciberterrorismo real foi registrado.[477] Isso levanta a questão: o quão real é a ameaça?" Ataques a componentes críticos da infraestrutura nacional não são incomuns, prossegue Weimann, mas eles não têm sido conduzidos por terroristas e não têm buscado infligir o tipo de dano que os qualificaria como ciberterrorismo. Talvez se experimente um maior temor pelo ciberterrorismo porque ele reúne dois dos grandes medos dos tempos modernos: o medo da fortuita vitimização violenta e a desconfiança com relação às novas tecnologias. "Uma ameaça desconhecida é percebida como mais ameaçadora do que uma ameaça conhecida".[478] Sobre essa questão, Berner explica que esse temor decorre de sua própria natureza arcana: a tecnologia é complexa, abstrata e indireta em seu impacto sobre os indivíduos, e, como ela assume funções anteriormente executadas por pessoas, ela ainda é temível pela possibilidade da perda de controle.[479] Os medos cibernéticos (*cyberfears*) têm sido irracionais, desarrazoados ou altamente exagerados – o que de forma alguma quer dizer que devemos negar ou ignorar o ciberterrorismo. Nas palavras de Weimann: "assim como os eventos do 9/11 pegaram o mundo de surpresa, assim poderia um ataque *cyber* maior".[480]

(É óbvio que, oportunisticamente, as ansiedades com relação ao ciberterrorismo foram fomentadas por interesses econômicos. Uma indústria inteira – de *think tanks*, experts e empresas privadas de segurança – tem ganhado força, propagando as ameaças de, e as soluções para, eventuais ataques. Berner alerta que a guerra ao ciberterrorismo pode se tornar a justificativa perfeita para governos instituírem mais controle no evasivo ciberespaço.[481])

Berner argumenta que terroristas podem não estar inclinados a tentar novos métodos de terrorismo até que eles vejam seus próprios métodos tradicionais como inadequados.[482] O que é bastante evidente, porém, é a utilização dessa tecnologia como suporte para os atos terroristas: planejamento; comunicação e coordenação; recrutamento, publicidade e propaganda; captação de recursos e financiamento; etc.[483] – o que torna possível a sua reclassificação como crime tradicional.

---

[477] WEIMANN, Gabriel. *Cyberterrorism*, *op. cit.*
[478] *Ibid*., p. 3.
[479] BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *op. cit.*
[480] WEIMANN, Gabriel. *Cyberterrorism*, *op. cit.*, p. 11.
[481] BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *op. cit.*
[482] *Ibidem.*
[483] FREIBURGER, Tina; CRANE, Jeffrey S. "A Systematic Examination of Terrorist Use of the Internet", *International Journal of Cyber Criminology*, v. 2, i. 1, 2008, p. 310-311; THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *op. cit.*; YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 57-60.

> Os terroristas têm acesso, como muitos americanos, a dados imagéticos de alvos potenciais, tal como mapas, diagramas e outros dados cruciais sobre importantes instalações ou redes. Dados imagéticos também permitem que terroristas vejam atividades contraterroristas em um local visado. Um computador da Al-Qaeda capturado continha informações arquitetônicas de engenharia e estrutura de uma barragem, permitindo que engenheiros e planejadores da Al-Qaeda simulassem falhas catastróficas.
> Com relação à coleta de informações na internet, em 15 de janeiro de 2003, o Secretário de Defesa Donald Rumsfeld observou que um manual da Al-Qaeda, recuperado no Afeganistão, dizia "Utilizando abertamente fontes públicas, e sem recorrer a meios ilegais, é possível reunir pelo menos 80 por cento de todas as informações necessárias sobre o inimigo".[484]

Thomas argumenta que o *cyberplanning* pode ser uma ferramenta de comunicação terrorista mais importante do que a opção tão disseminada e temida dos ataques contra informações e sistemas que resultem em violência contra alvos não combatentes.[485] Para o autor, o *cyberplanning* – que não é definido em qualquer outro lugar – se refere à coordenação digital de um plano integrado, que se estende além de fronteiras geográficas, que pode ou não resultar em derramamento de sangue.[486] Thomas cita alguns exemplos de como grupos terroristas podem utilizar a tecnologia da informação para o planejamento de atos terroristas:

- *Coleta de informações* [profiling]: A internet amplia as possibilidades de identificação de perfis pessoais – potenciais simpatizantes e apoiadores – e perfis estruturais – dos meios projetados para prevenir atos terroristas e das vulnerabilidades reconhecidas em sistemas diversos. "A exposição das prioridades das agências de aplicação da lei permite que o terrorista altere seus procedimentos de operação".[487] E, enquanto muitas das informações publicadas possam não ser sensíveis, elas podem ser muito úteis para grupos terroristas, podendo assistir o comando e o controle de suas operações.

- *Propaganda ideológica* [ideological weapon]: Em razão do menor controle do ciberespaço, a internet permite a transmissão de informações (ou versões delas), praticamente sem filtros ou censura, para todo o globo, induzindo ou instigando uma guerra ideológica.

---

[484] THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *op. cit.*, p. 118.
[485] *Ibid*., p. 112.
[486] *Ibid*., p. 113.
[487] *Ibid*., p. 114.

- *Produção de um clima de medo virtual* [virtual fear atmosphere]: A internet pode ser utilizada para propagar desinformações, mensagens ameaçadoras ou imagens horríveis de atividades criminosas (basta se lembrar do recurso terrorista a vídeos de execuções).

- *Distância segura*: "Terroristas que planejam ataques nos Estados Unidos podem fazê-lo do estrangeiro, com risco limitado, especialmente se seus locais de comando e controle estiverem localizados em países outros que seus próprios. Traçar a rota de sua atividade é particularmente difícil. A rede proporciona aos terroristas um local para planejar sem os riscos normalmente associados aos telefones celulares ou por satélites".[488]

De fato, grupos terroristas tiram o maior proveito possível das oportunidades que a internet oferece.[489] Weimann identificou que todos os grupos terroristas ativos tinham presença na internet e haviam desenvolvido seus próprios *websites*.[490]

4.2.2 Violações auxiliadas pela tecnologia de informação

Uma segunda categoria de violações híbridas no ciberespaço são crimes auxiliados pela tecnologia de informação. Brenner considera-as *cybercrimes* instrumentais, onde a tecnologia de informação serve de implemento à ação desviante.[491]

4.2.2.1 Ciberfraude

Diferente dos crimes que utilizam violência ou constrangimento, as fraudes retiram bens ou valores de vítimas por meio de desinformação ou trapaça. Elas ocorrem

[488] *Ibid*., p. 119.
[489] FREIBURGER, Tina; CRANE, Jeffrey S. "A Systematic Examination of Terrorist Use of the Internet", *op. cit*.
[490] WEIMANN, Gabriel. *www.terror.net*: how modern terrorism uses the internet. Washington: United States Institute of Peace, 2004. Sobre a Al Qaeda, ver THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *op. cit.*
[491] *Apud* PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*, *op. cit.*, p. 36.

na internet de formas variadas, mas geralmente reproduzem esquemas de golpes tradicionais.

As ciberfraudes, por exemplo, são muito comuns no varejo online e ocorrem na venda de bens roubados, falsificados, danificados ou enganosamente representados em termos de suas características e qualidades, tal como na não entrega do produto ao consumidor.[492]

Os ataques de *salame slicing* também são comumente referidos como *cybercrimes*[493]: por meio de operações realizadas pela internet, criminosos executam transferências de centavos de muitas contas bancárias ou fazem compras parceladas em valores inexpressivos, que passam indetectáveis pelas vítimas (bancos e correntistas), mas somam lucros significativos aos atuantes. No entanto, há registros anteriores desse tipo de fraude, fora do contexto telemático. *Salame slicing* é um tipo de fraude executada numa série de muitas ações pequenas e praticamente imperceptíveis que envolvem sutis alterações de valores: o operador de caixa de mercado ou de banco que subtrai pequenas quantias a cada dia de trabalho; o posto de combustível que altera a leitura das bombas de combustível, enganando os clientes quanto a quantidade realmente abastecida; a locadora de veículos que fraudulentamente adiciona alguns litros à capacidade real do tanque de combustível, fazendo com que os clientes que devolvem os automóveis sem tanque cheio paguem valores inflacionados para um total falsamente inflacionado do tanque. O fato de esses exemplos serem baseados em casos reais evidencia que a tecnologia da informação teve meramente um papel auxiliar nas violações tradicionalmente cometidas, seja pela facilidade ou pela maior amplitude oferecida na execução da fraude.

Uma forma adaptada é a fraude realizada por meio de dados de entrada, que se refere à "obtenção fraudulenta de informações para solicitar linhas de crédito, incluindo o ato de fazer solicitações ilegais de cartão de crédito ou de usar informação pessoal subtraída para assumir o controle da conta de alguém".[494] As informações financeiras pessoais podem ser obtidas por meio de *trashing*, *phishing* ou *pharming*. Repare que essas são novas formas de obtenção fraudulenta de dados, oportunizadas pela tecnologia de informação, porém o fundamento ludibrioso é o mesmo das fraudes tradicionais. Brenner aplica o mesmo raciocínio relatado anteriormente, argumentando que fraudes e

[492] YAR, Majid. "Online Crime", *op. cit.*
[493] Por exemplo, MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*, *op. cit.*, p. 67.
[494] WALL, David S. *Cybercrime*, *op. cit.*, p. 72.

falsificações on-line são extensões de crimes concretos tradicionais.[495] E, como nas fraudes tradicionais, os valores subtraídos podem ser utilizados tanto para o enriquecimento ilícito do fraudador como para o financiamento de atividades criminosas. Thomas cita que muitos planos terroristas na Europa e na América do Norte foram financiados por meio de fraudes em cartões de créditos.[496]

Ciberfraudes também podem operar contra mercados de títulos. Siegel cita algumas dessas operações.[497] A *manipulação do mercado de ações* ocorre quando um atuante tenta controlar o preço das ações, interferindo nas forças naturais de oferta e procura. Uma informação enganosa pode ser postada online para aumentar o interesse de investidores em determinadas ações (*pump and dump*), enquanto os responsáveis pela publicação da informação vendem as ações, previamente adquiridas, a preços inflacionados; ou uma informação negativa (*cyber smear*) sobre determinadas ações pode ser publicada online, derrubando seu preço e permitindo que atuantes as comprem por um preço artificialmente baixo antes que as refutações dos funcionários da empresa restabeleçam o valor de mercado. A *oferta fraudulenta de títulos* ocorre quando são vendidos títulos fraudulentos em *websites* especialmente projetados para tornar a oferta mais atrativa do que realmente é, prometer vantagens excessivas e atenuar riscos. Nesse tipo de fraude, em geral, nenhum investimento é feito de verdade. Os primeiros investidores recebem lucros provenientes dos investimentos posteriores, levando o sistema ao colapso e fazendo com que os últimos investidores não recebam dividendos e percam seus investimentos iniciais. E, obviamente, parte dos valores é desviada em prol dos fraudadores.

4.2.2.2 Golpe virtual

Tal como as fraudes financeiras, os golpes também encontraram um espaço privilegiado na tecnologia da informação: uso de cartões de crédito falsos ou clonados; exploração de mercados cinzas; exploração de sistemas de gerenciamento de reputação (perfis de vendedores no comércio eletrônico, *fanpages* do Facebook); esquemas de pirâmide financeiras, golpes de investimento direto ("trabalhe em casa" etc.); *dating* ou

[495] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 51-58.
[496] THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *op. cit.*, p. 117.
[497] SIEGEL, Larry J. *Criminology*, *op. cit.*, p. 472.

romance scams (golpistas simulam romance e exploram o investimento emocional da vítima na relação para obter dinheiro e presentes).

4.2.2.3 Apropriação e pirataria de propriedade intelectual

A propriedade digital tem a peculiar característica de poder ser armazenada como código e, assim, ser reproduzida em seu formato original. Diferente das cópias analógicas, que perdem qualidade a cada geração de cópia, as reproduções digitais são idênticas. Isso traz uma novidade um bocado complexa: no caso em que a vítima se vê privada da informação subtraída, trata-se de uma clara variação do tradicional crime de furto; quando o criminoso copia as informações (uma música, um livro, um filme, um software), o resultado deixa de ser uma "soma zero" que identifica a clássica subtração e, então, ocorre uma indevida diluição da propriedade porque a vítima já não é a única em posse das informações. Comparando com os crimes terrestres, Brenner afirma que, de qualquer forma, os elementos constitutivos do crime tradicional restam preservados na apropriação cibernética.[498]

Yar também faz essa distinção e faz também uma denúncia de que a comparação entre a subtração (terrestre) e a apropriação (cibernética), utilizada nas campanhas antipirataria, pode ser enganosa e de interesse exclusivo de grandes corporações que controlam o acesso a bens culturais, e não necessariamente de interesse de artistas e consumidores.[499] Válido apontar que alguns pesquisadores contestaram o argumento de prejuízo econômico apontando que o compartilhamento P2P de arquivos digitais afetou minimamente (estatisticamente próximo a zero) o mercado da indústria musical.[500] No mesmo sentido, Hayward afirma que, apesar de argumentos em contrário, conglomerados da mídia continuam a crescer, particularmente porque eles se adaptaram e adotaram novos modelos de negócios que trabalham com, e não contra, a "geração download".[501]

O que parece ser uma novidade é a ubiquidade da apropriação de propriedades intelectuais na era digital: um percentual significativo de usuários utiliza softwares sem pagar pela licença de uso, baixa músicas e filmes regularmente e, no mundo acadêmico,

[498] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 44-47.
[499] YAR, Majid. *Cybercrime and society, op. cit.*, p. 74-76.
[500] Ver OBERHOLZER, Felix; STRUMPF, Koleman. *The effect of file sharing on record sales*: an empirical analysis. 2005.
[501] HAYWARD, Keith. "Five Spaces of Cultural Criminology", *op. cit.*, p. 455.

consegue obter gratuitamente cópias integrais de livros em sites especializados. A prática generalizada e cotidiana pode ter "normalizado" o comportamento a tal ponto que é difícil algum usuário apresentar uma objeção moral a isso ou a perceber a conduta como criminosa. Enquanto a pirataria de propriedade intelectual é motivada pelo ganho financeiro, a apropriação e o compartilhamento ilegais podem ser justificados por razões libertárias, artísticas, morais, educacionais etc.

O desenvolvimento tecnológico claramente potencializou esses tipos de violações. A possibilidade de armazenamento no disco rígido de computadores (sem necessidade de gravação em outros meios físicos como o CD e o DVD), o desenvolvimento de tecnologias de compressão de arquivos (MP3 e MP4/MPEG-4) e de compartilhamento (softwares P2P) revolucionou a apropriação de propriedades intelectuais. E junto com outras tecnologias (surgimentos dos CDs, do iTunes e dos telefones celulares), a fácil disponibilidade de arquivos individuais chegou a modificar o próprio consumo cultural, encerrando, por exemplo, uma era de produção de grandes álbuns musicais. Footman considera que *OK Computer* (Radiohead, 1997) talvez tenha sido o último grande álbum do rock, exatamente o álbum que aproveita, revela e denuncia os efeitos da tecnologia moderna sobre os indivíduos[502] – argumento que se adéqua com a sentença de Kerckhove: "A arte é a face metafórica das mesmas tecnologias que ela própria usa e critica".[503]

4.2.3 Violações de conteúdo

E existem ainda *violações de conteúdo*, vinculadas à comercialização e à distribuição de material ilícito. Yar concorda que violações auxiliadas pela tecnologia da informação (acima) e violações de conteúdo, embora possam "revestir" tipos já conhecidos de comportamento desviante, ao fazê-lo, mudam a natureza dessas infrações

[502] FOOTMAN, Tim. *Radiohead – welcome to the machine*: OK Computer and the death of the classic album. New Malden: Chrome Dreams, 2007.

[503] O argumento completo é este: "A arte nasce da tecnologia. É o contrapeso que equilibra os efeitos disruptivos das novas tecnologias na cultura. A arte é a face metafórica das mesmas tecnologias que ela própria usa e critica. Por exemplo, enquanto a imprensa foi inventada para representar e distribuir a informação, o teatro, os romances e a poesia, mas também a pintura perspectivista, a escultura e a arquitectura foram desenvolvidas como metáforas da condição humana sujeita à literacia. Como ocidentais, devemos a estrutura da nossa consciência à literacia. Mas devemos a matéria da nossa sensibilidade, o conteúdo da máscara psicológica aos trabalhos de Da Vinci, Shakespeare, Racine, Voltaire, Espinosa, Rembrandt, Vermeer, Dostoievski e a muitos artistas que pacientemente construíram as paredes da nossa consciência privada e as decoraram." (KERCKHOVE, Derrick de. *A pele da cultura*, *op. cit.*, p. 232.)

e criam novas dinâmicas que desafiam o controle do crime. "Ele podem não ser sem precedentes, mas seu deslocamento ao espaço de comunicação digital de fato os transforma de modo significativo, o que deve ser reconhecido".[504]

4.2.3.1 Pornografia infantil

A pornografia em si não constitui um crime. Suas representações já foram questionadas sob argumentos diversos: sua censura pelas elites vitorianas após a multiplicação do material nas classes operárias, sua reprodução de valores machistas, sua influência na objetificação da condição feminina, a exploração industrial de seus atores etc. Mas, a resposta do controle jurídico, ao menos na maior parte dos países democráticos contemporâneos, determinou que, enquanto consensual e envolvendo participantes maiores de idade, a pornografia não implica em atividade criminalizada.

Mas a pornografia, como sua própria história demonstra, é construída e cambiante. Então, como o controle jurídico responderá ao fenômeno do *cyberporn*? A tecnologia da informação oferece uma nova estrutura para a produção pornográfica e, com ela, surgem novas ambivalências. Sem entrar na questão da produção pornográfica na internet, que alçou essa atividade a um dos mercados mais lucrativos do ciberespaço, há outros desafios referentes ao controle da pornografia no ambiente virtual. É claro que é difícil transcender o mundo real e adentrar o ciberespaço sem um certo grau de bagagem ideológica e cultural – e encontraremos no *cyberporn* alguns dos mesmos construtos sem sentido ou novas cibervulgaridades "de macho". Mas, o que importa a essa reflexão é o que vem de novo. O direito não consegue acomodar facilmente identidades, sexualidades e realidades plurais em razão de sua dependência em estruturas binárias. Diante das potencialidades do *cyberporn*, tradicionais dicotomias – sujeito/objeto, causa/efeito, opressor/oprimido, ver/ser visto – podem estar indisponíveis. O *cyberporn* promete a fusão de identidades, a dissolução dos limites entre elas e a abertura de espaços para a exploração de novos prazeres. Chatterjee afirma que o perigo é que o direito tentará forçar estruturas inflexíveis num meio fluido e, assim, falhará na sua função de controle. "O direito apoia-se na certeza, mas o ciberespaço não ficará parado. Se a estrutura fluida da internet for reformulada em princípios fixos para os fins de regulação legal, o direito irá fundamentalmente fracassar

[504] YAR, Majid. "Online Crime", *op. cit.*

em compreender o que ele busca controlar"[505]. Isso corresponde a uma tarefa adaptativa do direito. Mas, ainda assim, isso não constitui uma preocupação imediatamente criminológica. Devemos nos preocupar com aquela pornografia que se traduz em violência e/ou implica pessoas vulneráveis.

A pornografia infantil não é um produto da internet e há evidências históricas para indicar que data de tempos antigos o interesse sexual de adultos em crianças. O que interessa saber, neste ponto, é se a internet teve algum impacto transformativo na promoção da pornografia infantil e em como ela ocorreu. Wall responde positivamente a essa questão, argumentando que

> as tecnologias de rede criam uma comunidade on-line, socialmente autojustificante, de consumidores de pornografia infantil na qual valores, de outro modo desviantes, são compartilhados ou mesmo encorajados […], a internet também permite que indivíduos tenham acesso a material pornográfico e se comuniquem com outros a partir da privacidade de suas próprias casas, dando-lhes uma impressão de segurança e também uma sensação de controle sobre o meio, [e que] o principal impacto das tecnologias de rede sobre a pornografia infantil foi proporcionar métodos novos e cada vez mais efetivos de distribuir imagens sexuais de crianças.[506]

Do mesmo modo, Brown argumenta ser evidente que, no caso de pornografia infantil, os *pixels* afetam a dignidade e as vidas de crianças reais; geram humilhações reais e dores humanas; reproduzem e reforçam reais relações de poder (patriarcal) e exploração.[507] Segundo ela, a interface entre humanos e máquina apresenta um problema não *por causa* da tecnologia, nem *por causa* do amplo e global apoio cultural (masculino) para práticas de abuso sexual infantil, mas precisamente *por causa* da interface: as linhas que conectam uma complexa rede de atuantes pedófilos de pessoas e coisas. "Uma delicada linha que pode ligar *web-cams* a *pixels*, os *pixels* à internet, a internet aos homens, os homens à economia, a economia à indústria do sexo, a indústria do sexo ao desejo, o desejo à pedofilia..."[508]

---

[505] CHATTERJEE, Bela Bonita. "'This is not Kate Moss': an exploration into the viewing of cyberpornography", *Proceedings of the 14th annual BILETA conference*, College of Ripon & York St. John, York (England), 1999.
[506] WALL, David S. *Cybercrime, op. cit.*, p. 112.
[507] BROWN, Sheila. "The criminology of hybrids: Rethinking crime and law in technosocial networks", *op. cit.*, p. 233.
[508] *Ibidem*.

4.2.3.2 Veiculação de conteúdo violento e perigoso

A expansão da comunicação na internet tem sido acompanhada:

- pela proliferação de *discursos de ódio* – consideradas como tais quaisquer formas de declaração ou representação depreciativa de indivíduos ou grupos, reproduzindo assim padrões de marginalização e exclusão social, política e cultural[509] –, promovidos por grupos intolerantes diversos (de extrema direita, ultranacionalistas, supremacistas, neonazistas, fundamentalistas cristãos *et al.*), e que têm se deslocado de espaços "marginais" associados com grupos extremistas para plataformas mais *mainstream* como YouTube e Facebook;

- pela *disseminação de imagens de violência*, como vídeos de mortes;

- pelo surgimento do *sexting* e da sua declinação hedionda, o *revenge porn*;

- pelo favorecimento do *cyber bullying*, no qual os agressores, implícita ou explicitamente, se satisfazem ou se favorecem por meio de maus tratos infligidos a suas vítimas,

- e do *cyber-stalking*[510], que pode hoje ser feito de modo anônimo e à distância, mediado pela internet, possibilitando uma prevalência de assédios provocados por pessoas não íntimas, o que constitui uma variação da perseguição obsessiva mais tradicional;

- e pela ampliação de oportunidades de *aliciamento de menores para abuso sexual*, que variam entre abusos comunicativos, restritos a trocas de

[509] YAR, Majid. "Online Crime", *op. cit.*

[510] O *stalking* descreve um assédio persistente em que uma pessoa repetidamente impõe comunicação e/ou contato indesejado a outra pessoa. O comportamento insistente inclui, por exemplo, ligações para a vítima; envio de cartas, presentes ou material ofensivo; perseguição e vigilância da vítima; invasão de propriedade; vagueação próxima da vítima; contatos e aproximação com a família, amigos e colegas da vítima. A preocupação maior repousa na constatação de que o *stalking* pode ser um prelúdio para comportamentos mais violentos. (YAR, Majid. "Online Crime", *op. cit.*)

mensagens (*virtual abuse*), e abusos reais, nos quais a internet serve como canal para atrair potenciais vítimas (*grooming*).

4.3 TERCEIRA GERAÇÃO: CYBERCRIMES PRÓPRIOS

A terceira geração de *cybercrimes* surgiu na virada do século, com a substituição do *modem* de discagem pela banda larga, e compreende os *cybercrimes próprios* (ou *verdadeiros*), de natureza distribuída e automatizada, quase totalmente mediados por tecnologia.

Os *cybercrimes* dessa geração são literalmente *sui generis*: são produtos das oportunidades criadas pela internet e somente podem ser perpetrados dentro do ciberespaço; excluída a tecnologia que os possibilitou acontecer, o crime, impossível de existir como atividade, desaparece. Yar segue também esse entendimento: é "a internet que proporciona o ambiente eletronicamente gerado crucial no qual o *cybercrime* acontece" e, sem ela, o *cybercrime* não pode existir.[511] O desenvolvimento da internet, escreveu Yar mais recentemente, "facilitou a emergência de uma ampla variedade de crimes que tomam forma nos espaços da comunicação virtual".[512] É desses crimes que tratarei neste tópico.

Wall compreende essa terceira geração de *cybercrimes* como um novo período em que infratores e vítimas não se conhecem e não pretendem se envolver, mas no qual se enredam em razão de vulnerabilidades e falhas de sistema, combinadas ao acaso.[513] Partindo da perspectiva da ontologia da técnica, a minha interpretação estende um pouco mais essa concepção, incluindo aqui as violações que acontecem exclusivamente a partir da tecnologia da informação e que por ela são governadas.

4.3.1 Hacktivismo

O hacktivismo consiste no ativismo e protesto político que lança mão de técnicas e ferramentas de *hacking*, interrompendo o normal funcionamento das operações e, assim, ganhando publicidade à causa dos atuantes. Brenner considera o hacktivismo

[511] YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 6.
[512] YAR, Majid. "Online Crime", *op. cit.*
[513] WALL, David S. *Cybercrime*, *op. cit.*, p. 131.

como uma nova forma de vigilantismo[514] – e não é raro encontrar a expressão "vigilantismo na internet".

Apesar de ser um termo ao qual se recorre corriqueiramente, raros foram (e são) os esforços em analisar e conceituar criminologicamente o *vigilantismo*.

> Há considerável disputa entre aqueles (poucos) autores que examinaram o fenômeno quanto a suas precisas características: se é ou não essencialmente violento, conservador, extralegal, organizado e dirigido apenas contra o crime; se ele pode ser executado por agentes que atuam em nome do estado (tal como a polícia), assim como por cidadãos particulares; e se ele é um movimento social genuíno ou uma mera reação social.[515]

Isso gera o problema de que todos têm uma opinião (moral) sobre o que é o vigilantismo, sem que ninguém tenha se dado o trabalho de defini-lo (criminologicamente), restringindo, por exemplo, que se faça uma análise sobre a experiência de ondas sem precedentes de atividades vigilantes, ou que se possa fazer uma comparação entre o comportamento vigilante urbano clássico e o vigilantismo no ciberespaço.

Uma referência mais criminológica ao vigilantismo já tinha aparecido na primeira apresentação de Wilson e Kelling sobre a teoria das *janelas quebradas*.[516] Nesse clássico artigo, os autores relatam que há duas tradições de envolvimento comunitário na manutenção da ordem. Primeiro, os vigias comunitários: voluntários que patrulham suas comunidades para manter a ordem, lançando mão de suas presenças para desencorajar a desordem ou alertar a comunidade de desordens que não poderiam ser impedidas. Segundo, os vigilantes: estes se diferenciavam da primeira tradição por fazerem justiça com as próprias mãos.

Mas, é Johnston quem empreendeu o estudo mais completo sobre o vigilantismo no âmbito da criminologia[517], argumentando que o vigilantismo apresenta seis características necessárias:

> 1. *Planning, premeditation, and organization*[518]. O vigilantismo envolve planejamento e premeditação mínimos por aqueles que se engajam nele –

[514] BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?", *op. cit.*, p. 95-98.
[515] JOHNSTON, Les. "What is vigilantism?", *British Journal of Criminology*, v. 36, n. 2, 1996. p. 221.
[516] WILSON, James Q.; KELLING, George L. "Broken Windows: The police and neighborhood safety", *The Atlantic*, mar 1982.
[517] JOHNSTON, Les. "What is vigilantism?", *op. cit.*

excluindo, portanto, as violências reativas e espontâneas, como a legítima defesa.

2. *Private voluntary agency*. Seus participantes são cidadãos particulares, cujo engajamento é voluntário. A voluntariedade no engajamento é aspecto fundamental do vigilantismo e o distingue de outras atividades executadas por indivíduos particulares com base contratual (por exemplo, seguranças privados).

Alguns autores sugerem que policiais podem participar de um vigilantismo no controle do crime. Por exemplo: policiais podem participar de atos vigilantes, como cidadãos particulares, quando fora de serviço (*off-duty*) e, no estudo de Johnston, é citado o caso do envolvimento de policiais brasileiros em "esquadrões da morte"; ou, pode ocorrer que um policial em serviço cometa atos que são ilegítimos, como um uso excessivo da força ao efetuar uma prisão; por fim, existe a possibilidade de que o policial se envolva em atos vigilantes ao se submeter a uma política de ações que constitui uma forma de violência, uma coerção ilegítima, executando, então, vigilância ilegal ou intimidação contra determinados grupos minoritários.

Johnston contesta essas possibilidades[519]: primeiro, ele argumenta que policiais, em serviço ou fora dele, continuam a ter poderes policiais plenos, não podendo suas ações *off-duty* ser desligadas de seus status, funções e responsabilidades públicas; segundo, Johnston afirma que, embora seja possível diferenciar entre práticas lícitas e ilícitas, é mais difícil distinguir atos policiais legítimos e ilegítimos, e que não há qualquer ganho conceitual em definir o abuso de poder policial (ou estatal) de vigilantismo, em razão da confusão de formas de violência e do problema da sobre-inclusividade (formulação de um conceito que, por sua natureza guarda-chuva, incorpora muito e explica pouco).

---

[518] Johnston faz uma cautelosa referência a um elemento além do planejamento e da premeditação: a *organização*. Uma primeira questão é se o engajamento no vigilantismo é organizado numa base recorrente ou *ad hoc*. Além disso, diferentes níveis de organização podem caracterizar uma atividade vigilante. E, embora as iniciativas mais recorrentes envolvam mobilização coletiva, existe possibilidade de que indivíduos isolados possam se dedicar a atividades vigilantes a longo prazo, de modo planejado e premeditado. (JOHNSTON, Les. "What is vigilantism?", *op. cit.*, p. 223-224.)

[519] JOHNSTON, Les. "What is vigilantism?", *op. cit.*, p. 224-225.

3. *Autonomous citizenship*. O vigilantismo é uma forma de "cidadania autônoma" porque é uma atividade voluntária na qual se envolvem cidadãos ativos, sem a autoridade ou o apoio do estado. Como tal, constitui um movimento social. Nesse sentido, conforme o entendimento de Johnston, os projetos de Neighbourhood Watch, como forma de "cidadania responsável" sancionada e patrocinada pelo Estado, não seriam atos vigilantes.[520]

4. *The use or threatened use of force*. A quarta característica refere-se ao uso ou à ameaça de uso de força. A violência é uma característica comum do vigilantismo, o que sugere que o exercício de força seja um elemento necessário em qualquer atividade vigilante. A violência exercida não deve ser confundida com punição. A punição, diz Johnston, "é premeditada, sistemática, calculada e geralmente apresenta características ritualísticas e quase judiciais".[521] Assim, a punição é uma variável, ao passo que a força é uma constante na ação vigilante.

5. *Reaction to crime and social deviance*. O vigilantismo emerge quando uma ordem estabelecida está sob ameaça de transgressão, de potencial transgressão ou de alegada transgressão a normas institucionalizadas. Com esse fator, num recorte normativo do vigilantismo, Johnston deixa claro que a concepção de vigilantismo elaborada por ele tem implicações criminológicas – e não políticas ou morais. Em outras palavras, o vigilantismo é uma reação ao desvio (normativo) real ou percebido.

É válida uma reflexão, neste ponto: como reação ao desvio (transgressão à norma) e ao crime (desvio criminalizado), sabendo-se que, num universo de desvios e crimes, somente alguns serão objeto de reação firme e concreta, o vigilantismo é seletivo e excludente. Outra questão importante é que o vigilantismo pode emergir não do fenômeno criminal concreto, mas de um "pânico moral orquestrado sobre a criminalidade"[522], permitindo que uma

[520] *Ibid*., p. 226.
[521] *Ibid*., p. 233.
[522] *Ibid*., p. 229.

> disputa por poder político se mascare de movimento vigilante com o emprego de uma "retórica de transgressão".[523]
>
> 6. *Personal and collective security*. O vigilantismo não é simplesmente um sinônimo de controle social; ele é "uma estratégia popularmente iniciada, surgindo como uma reação ao desvio social (real, ameaçado ou alegado), cujo objetivo é oferecer para as pessoas a garantia de que um sistema de ordem estabelecido prevalecerá".[524] Johnston argumenta que o foco do vigilantismo é invariavelmente local e que, na maior parte dos atos vigilantes, há uma preocupação em minimizar a ameaça objetiva a pessoas, propriedade ou valores, e de reduzir o medo associado.

Em suma, tem-se que o vigilantismo pode ser definido como (elemento 1) ações planejadas que são (2) executadas voluntariamente por cidadãos particulares, (3) sem a autoridade do Estado, e que (4) usa ou ameaça fazer uso da força, como (5) reação ao desvio real ou percebido e com o (6) objetivo de minimizar as ameaças às pessoas. Essa definição não pressupõe que a ação vigilante seja necessariamente ilegal ou extralegal – discussão que poderia ser apropriada no campo da política-criminal, mas que não faz sentido na seara criminológica.

O hacktivismo, como um vigilantismo na internet, carrega consigo as mesmas características? O seu recente histórico de atividades indica que a resposta pode ser afirmativa, desde que feitas algumas adaptações.

Primeiro, o hacktivismo envolve planejamento e premeditação. Ainda que algumas ações hacktivistas possam parecer uma reação espontânea, elas geralmente são discutidas em fóruns de discussão e muitos ataques são realizados com divisão de tarefas.[525]

Segundo, os hacktivistas atuam voluntariamente e isso é aspecto próprio do ativismo e protesto político.

Terceiro, o hacktivismo se manifesta como um movimento social independente de sanção ou apoio estatal; pelo contrário, o éthos anarquista dos hackers condena qualquer envolvimento com o Estado.

---

[523] *Ibid*., p. 230.
[524] *Ibid*., p. 231.
[525] Para a dinâmica organizacional do Anonymous, ver OLSON, Parmy. *We are Anonymous*, *op. cit.*

Quarto, por mais que os hacktivistas não recorram à força física real ou à ameaça de seu uso, é inegável que lançam mão de técnicas e ferramentas de *hacking* extremamente vigorosas que geram constrangimento e danos às pessoas ou instituições atingidas: invasão, desconfiguração e vandalismo de *websites*, sobrecarregamento de servidores por meio de DDoS, congestionamento da comunicação com *email bombs*; utilização de *malwares*.

Quinto, o hacktivismo também se opera de uma forma reativa – mas, não em relação à transgressão a normas institucionalizadas. O histórico de ações vigilantes no ciberespaço indica que as principais operações realizadas por coletivos hackers ou por atuantes individualizadas foram executadas como resposta a medidas de supressão do livre fluxo de informação (valor muito caro à cultura hacker): restrições de conteúdo (uma instituição que peça judicialmente a retirada de um conteúdo do ar), restrições de direitos autorais, ocultação de crimes de guerra, sigilos diplomáticos, sabotagens a grupos que promovem vazamento de informações, governos autoritários etc.

Por fim, o hacktivismo constitui-se numa estratégia de promover a segurança dos atuantes no ciberespaço (em especial, a preservação da privacidade individual), atribuindo a ameaça a comportamentos desviantes particulares (como, por exemplo, no caso de pedófilos), mas deslocando-a e ampliando-a principalmente aos governos e às grandes corporações. Nesse sentido, o vigilantismo *cyber* deixa de ser local e passa a ter o alcance do próprio ciberespaço.

Há vinte anos, Johnston concluía que ainda havia muito a ser pesquisado sobre o vigilantismo. Tudo indica que essa demanda ainda se apresenta, especialmente no vigilantismo *cyber*. Que tipos de atividades vigilantes prevalecem (individuais, em grupo, recorrentes, *ad hoc*)? Quem se envolve nele (por idade, gênero, classe, nível de instrução, tipo de comunidade)? O que motiva o engajamento dos participantes (vitimização, vingança, frustração com o sistema jurídico ou político, defesa de valores)? Como os grupos vigilantes se organizam? Quanto tempo duram? Quais os efeitos do vigilantismo (mera retribuição ou dissuasão contra ameaças futuras)? etc.

Retomando as explicações sobre o hacktivismo, de acordo com Sandor Vegh[526], o ciberativismo se expressa em três modos fundamentais, que podem ser traduzidos conforme a seguinte tipologia:

- conscientização/advocacia, quando se remete/recebe informação – o que pode ser ilustrado pelas denúncias de violação de direitos humanos por organizações não governamentais ou pelas petições públicas, nas quais se informa o público de determinada demanda, colhem-se assinaturas e o pedido é entregue a alguma autoridade ou instituição pública;

- organização/mobilização, quando se convoca/é chamado à ação – os protestos organizados em Porto Alegre e outras cidades, para a redução das tarifas dos ônibus ou a interrupção do corte de árvores, são exemplos próximos dessa categoria de ciberativismo;

- e ação/reação, quando se inicia uma ação ou se reage a ela (exemplos: invasão e vandalismo de páginas virtuais, *denial-of-service attacks*, envio de *email bombs*).

E, permeando essas três formas de atuação, identifica-se uma atividade que é, ao mesmo tempo, a condição e o instrumento para o ciberativismo: o hacktivismo.

> Hacktivismo é uma ação online e episódica, politicamente motivada, ou uma campanha daí decorrente, executada por agentes não estatais em retaliação para expressar desaprovação ou para chamar a atenção a uma questão defendida pelos ativistas. Hacktivismo tem sido diversamente rotulado como defesa online, ação direta virtual, desobediência civil eletrônica, arte performática, ou cibercrime, ciberterrorismo, e ciberguerra, dependendo do ponto de vista. De acordo com Tim Jordan, sociólogo britânico da comunidade hacker, hacktivismo é um movimento social, um novo tipo de ação direta, uma atividade, baseada na internet, centrada em política virtual.[527]

[526] VEGH, Sandor. "Classifying Forms of Online Activism: The Case of Cyberprotests agains the World Bank". In MCCAUGHEY, Martha; AYERS, Michael D. *Cyberactivism*: online activism in theory and practice. London: Routledge, 2003. p. 72 e ss.
[527] *Ibid*., p. 83.

Nos anos recentes, essa prática se tornou publicamente conhecida quando o *hacking* foi utilizado como importante instrumento nas mobilizações políticas da Primavera Árabe e a partir das *operações* executadas por notórios grupos hackers, como o coletivo Anonymous[528], sobre o qual se falará mais adiante. O ciberativismo pode se expressar de formas distintas, como: sobrecarregamento de servidores por meio de DDoS; congestionamento da comunicação com *email bombs*; desconfiguração e alteração de *websites*; utilização de *malwares* (softwares maliciosos).

Importante ressaltar, como o faz Weimann, que o hacktivismo, embora politicamente motivado, não pode ser equiparado ao ciberterrorismo.[529] Hacktivistas causam perturbação social, promovem aflições específicas e, ainda que raro, podem expor pessoas e/ou patrimônios a perigo. Não se verifica em suas ações, porém, a especial finalidade de provocar terror, e suas práticas não resultam em mortes ou mutilações de pessoas.

Assim, a aproximação desses fenômenos pode indicar duas possíveis abordagens. Primeiro, a confusão entre hacktivismo e ciberterrorismo pode revelar um esforço político de hostilização ou criminalização de determinado movimento contestador, no qual o "terror" é um recurso retórico de grande utilidade. Segundo, e num contexto bastante diverso, uma comparação entre os dois fenômenos pode servir de instrumento prognóstico para o desenvolvimento de políticas preventivas contra o terrorismo. Não é difícil perceber que o hacktivismo indica as potenciais ameaças do ciberterrorismo. Métodos similares àqueles utilizados por hacktivistas podem ser explorados para ações criminosas que provoquem terror. O importante, pois, é que, caso a caso, sejam feitas as distinções dos atuantes, conforme suas condutas no ciberespaço. Há quem argumente que essa categorização não é estanque, havendo a possibilidade de hacktivistas se tornarem ciberterroristas, quando são recrutados ou contratados por grupos terroristas, ou quando decidem escalar suas ações, tornando as consequências mais gravosas; contudo, é reconhecido que hackers não simpatizam com os objetivos de grupos terroristas.[530]

---

[528] OLSON, Parmy. *We are Anonymous*, *op. cit.*, p. 64; YAR, Majid. *Cybercrime and society*, *op. cit.*, p. 47.
[529] WEIMANN, Gabriel. *Cyberterrorism*, *op. cit.*, p. 5.
[530] Por todos, WEIMANN, Gabriel. *Cyberterrorism*, *op. cit.*

4.3.2 Ciber-bloqueio

Em contraste direto com o *hacking*, o principal objetivo desse congestionamento provocado na internet é evitar que usuários legítimos tenham acesso a sistemas de redes e computadores por meio do bombardeio de informações nas portas de entrada. Os ataques distribuídos por negação de serviço (*Distributed Denial of Service attack*, DDoS) interrompem serviços, deixando-os "fora do ar", inundando-os com um número não gerenciável de pedidos de comunicação.

Eles podem ser executados por grupos de pessoas socialmente engendradas, com acesso simultâneo a um sistema num curto espaço de tempo, com a finalidade de o sobrecarregar. Mas, seu maior poder de fogo vem da utilização de *botnets* (ver *infra*).

Os DDoS foram inicialmente executados com a finalidade de extorquir valores de empresas; contudo, a partir do fim da primeira década do século XXI, o DDoS se tornou uma forma popular de ciberativismo, especial e notoriamente presente nos ataques do coletivo Anonymous.

Outra forma de congestionar o tráfego de informações é a utilização de *email bombs*, técnica que sobrecarrega o sistema de emails pelo envio massivo de mensagens.

4.3.3 *Botnets*

As *robot networks* compreendem listas de endereços IP de computadores zumbis que foram infectados por ferramentas de administração remota e os quais, portanto, podem ser controlados por um atuante distante. *Botnets* são geralmente compostos por algo entre dez mil e cem mil computadores; alguns maiores, com capacidade suficiente para tirar do ar os servidores de grandes empresas e governos menores, têm a capacidade de controlar remotamente mais de um milhão de computadores.[531] Isso explica por que os *botnets* são mercadorias valiosas (podendo ser alugados por determinado tempo) e como a sua dimensão influencia no reconhecimento e, por consequência, no preço da locação: "Na cultura hacker *underground*, quanto maiores os *botnets*, maior a credibilidade dos controladores, ou *botmasters*".[532]

Enquanto os primeiros ataques DDoS foram executados por meio de ferramentas de *web* simples (como o LOIC), numa espécie de mutirão de atuantes, os *botnets*

[531] OLSON, Parmy. *We are Anonymous*, *op. cit.*, p. 74.
[532] *Ibid*., p. 75.

possibilitaram um maior poder de fogo reunido num único executor. Em dezembro de 2010, por exemplo, o ataque DDoS lançado pela AnonOps sobre o *site* PAYPAL.COM contou com 4.500 voluntários utilizando o software LOIC; no entanto, foi confirmado que cerca de 90% do poder de fogo tinha vindo de computadores zumbis. A *Operação Payback* (#OpPayBack) somente teve êxito quando um *botnet* tirou completamente o site do ar. O hacker Jake Leslie Davis (Topiary) "estimou que usuários do LOIC representaram em média 5% a 10% do dano causado nos *sites* da PayPal, da MasterCard e da Visa".[533]

Já se evidenciou que grupos antipirataria também utilizaram *botnets* para inundar *websites*. A empresa indiana de software Aiplex, trabalhando em prol dos estúdios de cinema de Bollywood, lançou ataques DDoS contra diversos *sites* de *torrents*, incluindo The Pirate Bay. Isso foi admitido pelo CEO da Aiplex, em setembro de 2010. Uma semana após essa admissão, o coletivo Anonymous iniciou uma campanha de derrubada dos servidores da Aiplex e de outras organizações, como Recording Industry Association of America e Motion Picture Association of America. A mensagem foi clara: "você me derruba, eu te derrubo".[534]

4.3.4 *Spamming*

Caracteriza-se pela distribuição em massa de emails não solicitados, que podem ser tanto legítimos (remetidos por empresas que anunciam suas ofertas comercias), como também ilegítimos (remetidos anônima ou dissimuladamente com ofertas ilícitas).

O *spamming* compreende um conjunto de três características básicas:

- *Impessoalidade*: A identidade pessoal do destinatário é irrelevante.
- *Não solicitação*: O destinatário não autorizou o envio de qualquer conteúdo para seu endereço de email.
- *Atratividade*: O conteúdo oferece um benefício (desproporcional) ao destinatário.

[533] *Ibid*., p. 121-122.
[534] *Ibid*., p. 103.

O *spamming* não pode ser comparado com a distribuição massiva de correspondências postais indesejadas, uma vez que estas sustentam o próprio serviço de entrega postal, ao passo que o *spamming* impede a eficiência da comunicação de emails, sufocando a largura de banda, reduzindo taxas de acesso e introduzindo novos riscos aos destinatários. (Curiosamente, é dessa mesma forma que o *telemarketing* é sustentado pela tecnologia da informação: bancos de dados compartilhados de informações pessoais; agendamento, discagem e mensagens automatizados por computador – geral e igualmente não solicitados.)

4.3.5 Distribuição de software malicioso (*malware*)

Entre as estratégias utilizadas por hackers para a consecução de seus planos, sejam eles justificados pela tradição ética hacker ou motivados por questões financeiras, estão a engenharia social (técnica para obter informação e códigos de acesso, por meio do estabelecimento de uma relação de confiança com aqueles que os detêm) e a utilização de softwares maliciosos: *logic bombs*, *spywares*, *trojans*, vírus, *worms* etc.

Os *malwares* são desenvolvidos a partir de códigos, dependem de conexão a um sistema computadorizado, aproveitam-se de falhas sistêmicas e vulnerabilidades dos usuários, e são projetados para provocar danos ou colher informações. Excluída a tecnologia da informação da equação criminosa, tais programas não têm qualquer utilidade e sequer poderiam ser criados.

O caso dos *malwares* explicita como é um desafio o dinâmico processo de complexificação dos *cybercrimes*. Criado por Evgeniy Mikhailovich Bogachev (aka Lucky 12345), o código malicioso *ZeuS* é um pacote *trojan* que permite a execução de diversas tarefas maliciosas ou criminosas, como o registro da digitação (*key logging*) ou a recuperação de formulários (*form grabbing*) para posteriores transações financeiras fraudulentas, e também a instalação do *ransomware* CryptoLocker. Na sua versão *Gameover*, o código também coloca o aparelho a serviço de uma rede controlada à distância (*botnet*). Esse é um exemplo, por suas distintas ações e possibilidade, do que tem sido chamado de *blended* ou *cross-protocol threats*, isto é, uma combinação de métodos diferentes para a realização de *cybercrimes*.

4.3.6 *Leaking*

O vazamento indevido de informações sensíveis não é algo novo. A novidade do *leaking* na era digital está, primeiro, no lançamento público de dados que deveriam ser confidenciais ou restritos a alguns indivíduos ou por determinado tempo. Essa ampla difusão, justificada pela tradição da liberdade de informação, diferencia o *leaking* da ciberespionagem (*warfare*/concorrência) e da pirataria (fins econômicos). Uma segunda característica é o modo como se opera o *leaking* contemporâneo: em vez do vazamento direto de quem tem acesso legítimo à informação, as informações são transmitidas por meio de comunicação criptografada (para a proteção das fontes) a organizações que analisam, editam e disponibilizam o conteúdo vazado. Informações de correspondência diplomática, registros militares, bancos de dados de empresas são alguns dos conteúdos mais vazados por hackers.

O caso paradigmático é o do WikiLeaks. Khatchadourian não o considera uma organização; para ele, que acompanhou de perto o vazamento "Collateral Murder", o Wikileaks "é melhor descrito como uma insurreição de mídia".[535]

Julian Assange, fundador do Wikileaks, ao narrar um breve histórico do caso Estados Unidos *versus* WikiLeaks, assim descreveu sua organização:

> A missão do WikiLeaks é receber informações de denunciantes e jornalistas censurados, divulgá-las ao público e defender-se dos inevitáveis ataques legais e políticos. Estados e organizações poderosas se empenham sistematicamente em abafar as publicações do WikiLeaks e, sendo um canal de publicação "de último caso", o WikiLeaks foi criado para resistir a esse tipo de dificuldade.[536]

Assange já chegou a argumentar que um movimento social para expor segredos poderia "derrubar muitas administrações que dependem da ocultação da realidade – incluindo a administração dos EUA".[537]

Assange chama o seu site WIKILEAKS.ORG de "um sistema incensurável para o vazamento irrastreável de documentos em massa e análise pública".[538] Para garantir isso, o conteúdo é mantido em mais de vinte servidores ao redor do mundo e sob

[535] KHATCHADOURIAN, Raffi. "No secrets: Julian Assange's mission for total transparency", *The New Yorker*, 7 jun 2010.
[536] ASSANGE, Julian. *Quando o Google encontrou o Wikileaks*, *op. cit.*, p. 153.
[537] *Apud* KHATCHADOURIAN, Raffi. "No secrets: Julian Assange's mission for total transparency", *op. cit.*
[538] *Ibidem*.

centenas de domínios, além de contar com o suporte de engenheiros excepcionalmente segredistas (que têm acesso exclusivo a certas partes do sistema, não acessíveis para outras pessoas como forma de proteção – nem mesmo para Assange em alguns casos) e com o apoio de *mirror sites* mantidos por simpatizantes independentes, de tal forma que, para que um governo ou uma empresa conseguisse remover o conteúdo do WikiLeaks, seria necessário desmantelar a própria internet.[539]

Assange também apresentou justificativas para os vazamentos:

> Na verdade, são duas justificativas básicas. A primeira é que a civilização, a parte boa dela, se baseia no registro intelectual, e o registro intelectual deve ser o mais completo possível para a humanidade poder avançar o máximo possível. A segunda é que, na prática, a divulgação da informação é positiva para as pessoas envolvidas em ações que contam com o apoio do público e negativa para as pessoas envolvidas em ações que não têm o apoio do público.[540]

E explicou a sua responsabilidade para com o registro da história intelectual:

> (...) nós, como seres humanos, influenciamos e criamos a história intelectual, como civilização. E é essa história intelectual guardada na estante que podemos tirar de lá para fazer as coisas e evitar repetir as idiotices, porque alguém já fez essa idiotice e escreveu sobre essa experiência para não precisarmos repetir o erro. Existem vários processos diferentes que estão criando esse registro histórico, outros processos em que as pessoas tentam destruir partes desse registro e outros que tentam impedir as pessoas de incluir coisas nesse registro. Nós dependemos desse registro intelectual para viver. Então, nós precisamos colocar o máximo possível de coisas nesse registro, evitar o máximo possível que outras coisas sejam retiradas e fazer com que esse registro seja o mais pesquisável possível. (...) A situação da grande imprensa, hoje, é tão terrível que eu não acho que ela tenha conserto. Não acho que ela seja possível. Acho que ela tem de ser eliminada e substituída por uma coisa melhor. (...) É. E eu defendo a ideia de um jornalismo científico – as coisas devem ser citadas com precisão, com a fonte original, e o maior número possível de informações deve ser de domínio público, para ficar disponível para as pessoas, da mesma forma como acontece na ciência, para você poder testar e ver se os dados experimentais de fato levam àquela conclusão. Caso contrário, provavelmente o jornalista só inventou a notícia. Na verdade, é isso que acontece: as pessoas simplesmente inventam as coisas. Inventam a ponto de a gente entrar em guerra. A maioria das guerras do século XX começou como mentiras amplificadas e espalhadas pela grande imprensa. Você pode dizer: 'Bom, isso é terrível; é terrível que todas essas guerras comecem com mentiras'. E eu digo que não, que isso é

[539] *Ibidem*.

[540] Trechos das respostas de Julian Assange, na entrevista concedida a Eric Schmidt (presidente do Conselho Executivo do Google), Jared Cohen (diretor do Google Ideas) *et al.*, na sua então prisão domiciliar em Norfolk, Inglaterra, em 23 de junho de 2011. (ASSANGE, Julian. *Quando o Google encontrou o Wikileaks*, *op. cit.*, p. 96-97.)

> uma oportunidade tremenda, porque significa que as populações não gostam de guerra e só entraram nela porque foram enganadas, porque mentiram para elas. E isso significa que, se souberem a verdade, elas podem fazer a paz. Isso é motivo de grande esperança.[541]

Com os vazamentos, Assange pretende estabelecer um novo padrão: o "jornalismo científico". Para o hacktivista Rop Gonggrijp, quem também integrou a equipe responsável pelo vazamento "Collateral Murder", o WikiLeaks não faz parte da imprensa; ele o considera um grupo de defesa de fontes; na estrutura do site "a fonte não mais é dependente de encontrar um jornalista que pode ou não fazer algo de bom com seu documento".[542]

Khatchadourian, todavia, faz uma advertência: "Em breve, Assange deve confrontar o paradoxo de sua criação: a coisa que ele mais detesta – poder sem responsabilidade – está codificada no DNA do site, e apenas se tornará mais evidente à medida que o WikiLeaks evoluir para uma instituição real".[543]

É importante deixar claro que o WikiLeaks não é único agente *whistleblower* (denunciante) e que a demanda pela liberdade de informação tem se expressado continuamente: a duas semanas de Assange completar um ano refugiado na embaixada do Equador (em Londres), Edward Snowden, ex-assistente técnico da Central Intellingence Agency (CIA), revelou o uso do programa de vigilância eletrônica PRISM/US-984XN, pela americana National Security Agency (NSA), a qual tem monitorado milhões de registros de telefonemas e informações de usuários da internet, nos Estados Unidos e no mundo.[544] A paradoxal valoração da informação (sigilosa x transparente, restrita x livre, vigilância x privatividade) também se apresenta neste caso: enquanto a NSA tem coletado informações privativas sob o argumento de segurança pública, Snowden decidiu "vazar" informações sigilosas sobre o programa estatal sob os argumentos da preservação da privacidade.

---

[541] *Ibid*., p. 91-92.
[542] *Apud* KHATCHADOURIAN, Raffi. "No secrets: Julian Assange's mission for total transparency", *op. cit.*
[543] KHATCHADOURIAN, Raffi. "No secrets: Julian Assange's mission for total transparency", *op. cit.*
[544] Julian Assange ingressou na embaixada equatoriana para pedir asilo político, em 19 de junho de 2012. A entrevista de Edward Snowden foi gravada em 6 de junho de 2013. Disponível em <http://www.guardian.co.uk/ world/the-nsa-files>.

4.4 O CASO DO COLETIVO ANONYMOUS

Quando foi inicialmente apresentado ao programa de pós-graduação, o anteprojeto desta tese tinha por objeto estudar o fenômeno do coletivo Anonymous, suas atividades, os conflitos inéditos que foram estabelecidos e as subsequentes reações de controle. O estudo disso, porém, revelou que era inadequado analisar esse fenômeno contemporâneo do ciberativismo tendo como fundamento o paradigma tradicional da criminologia, o que exigiu um passo-atrás reflexivo que culminou numa pesquisa mais ampla sobre a necessidade de novas criminologias para a compreensão dos *cybecrimes* próprios (ou, de terceira geração). É foi exatamente isso que foi desenvolvido nos capítulos anteriores. No entanto, a tese não ficaria completa sem um capítulo que explicasse a evolução do coletivo Anonymous, em especial porque ela revela novos modelos de comportamentos nos espaços públicos (tanto físicos, como virtuais) e novas disputas de interesses, que podem resultar na atribuição criminosa ao sentido de alguns eventos. Por esse motivo, esse derradeiro capítulo retoma a primeira inspiração dessa pesquisa e ilustra, com um caso paradigmático, como se desenvolveu o hacktivismo desse coletivo.

Superando a folclórica imagem, das décadas de 1980 e 1990, do jovem nerd solitário que, com recursos informáticos simples, empreendia embates com governos poderosos, regimes hostis ou corporações monopolistas, o princípio do século XXI tem registrado concretas e complexas operações hacktivistas, que envolveram vazamentos (*leakings*) de informações militares sigilosas e de comunicação entre autoridades diplomáticas, subtração e revelação de dados de consumidores de grandes empresas, apoio a protestos sociais e derrubadas de governos (o que foi bastante vigoroso na Primavera Árabe). E, ainda que vários grupos de ciberativistas tenham encenado múltiplas ações no ciberespaço, um grupo teve maior destaque: o coletivo Anonymous.

4.4.1 A criminalização do hacktivismo

Seus membros atuam como vigilantes; mas, são pertencentes a uma geração cibernética, não se adequando à categoria hobsbawmiana de bandidos sociais.[545] Seus atos ocuparam páginas e minutos caros à imprensa; todavia, a inexistência de uma

[545] Em sentido contrário, ver COLEMAN, Biella. "Our Weirdness is Free: The logic of Anonymous – online army, agent of chaos, and seeker of justice." *Triple Canopy*, n. 15. jan. 2012.

individualização impediu que se tornem celebridades. O Anonymous parece constituir uma terceira categoria criminosa que carrega consigo a exceção ao desejo de se ocultar, mas que se relaciona com o anonimato de uma forma peculiar: os seus participantes são anônimos na exata medida em que sua persona – representada por uma máscara ou por um homem sem cabeça – não o é. (Se não se pode transpor a explicação, é possível emprestar a caracterização, feita por Timm de Souza, de um Outro, a um tempo, perfeitamente presente e totalmente ausente.[546]) Essa hipótese é compartilhada por Biella Coleman:

> Poucos Anons vieram à tona para revelar detalhes sobre eles próprios, apesar das solicitações da mídia. Ao mesmo tempo, Anonymous foi bem sucedido em espalhar sua mensagem ao máximo possível, através de cada canal de mídia à sua disposição – em contraste com grupos criminosos que procuram permanecer escondidos a todo custo. O Anonymous administra para alcançar visibilidade espetacular e invisibilidade individual, ao mesmo tempo.[547]

Em suas ações, a persona do *Anonymous* sempre faz questão de se mostrar presente e garantir essa *spectacular visibility*. Nessas atividades, a máscara estilizada de Guy Fawkes tem menos a intenção de preservar o anonimato de quem a usa (que poderia ser quebrado pelo reconhecimento de outros elementos, como vestuário, cabelos, comportamento) do que afirmar a onipresença de uma legião de centenas, milhares, quiçá milhões de pessoas, que as vestem para o ativismo político. Ativismo nem sempre percebido como legítimo ou legal para as instâncias e autoridades do controle social. Se opta-se por inserir o coletivo Anonymous em categoria criminosa (atribuição sempre questionável), tal escolha não se faz como um pré-julgamento de seus atos – o que seria inaceitável em uma pesquisa criminológica –, mas pelo reconhecimento de que seus membros, quando identificados, têm sido tratados como tais. Coleman e Ralph compreenderam esta conflituosa rotulação:

> Hackers Anons são "criminosos" tal como qualquer hacker que tenha inevitavelmente violado as leis; alguns dos envolvidos podem até ter um histórico criminoso. Ainda assim, a maioria dos hackers, implícita ou explicitamente, têm críticas às leis que eles desejam transgredir.[548]

---

[546] SOUZA, Ricardo Timm de. *Totalidade & desagregação*: sobre as fronteiras do pensamento e suas alternativas. Porto Alegre: EDIPUCRS, 1996. p. 189.
[547] COLEMAN, Biella. "Our Weirdness is Free: The logic of Anonymous – online army, agent of chaos, and seeker of justice", *op. cit.*
[548] COLEMAN, Biella; RALPH, Michael. "Is it a crime? The Transgressive Politics of Hacking in Anonymous." *Social Text*, 28 set 2011.

O fato é que o ciberativismo tem sofrido uma forte reação do controle social punitivo, envolvendo processos e prisões:

- Aaron Swartz foi um prodígio programador de computadores e ciberativista. Swartz tornou-se conhecido pelo fato de, antes de seus vinte anos de idade, ter trabalhado no desenvolvido dos aplicativos e programas RSS, Creative Commons e Reddit. Como ciberativista, destacou-se pelos projetos Watchdog.net e Demand Progress – os quais, respectivamente, traziam informações sobre políticos e auxiliavam pessoas a se organizarem para exigir suas demandas políticas – e por sua luta contra o Stop Online Piracy Act (SOPA), o qual teve sua tramitação legislativa suspensa em razão da campanha pública promovida por Swartz. No que toca à disponibilização pública e livre de informações, Swartz disponibilizou toda a base de dados da Library of Congress (as obras não tinham restrições autorais, porém a biblioteca exigia uma taxa para acesso a elas) e publicou 2,7 milhões de documentos arquivados do registro dos processos federais PACER (o que não gerou resultados mais graves porque os processos eram, de fato, documentos públicos). Em 6 de janeiro de 2011, Swartz foi preso porque teria feito o download de um grande volume de artigos do JSTOR a partir da rede do MIT (a acusação afirmou que ele havia "roubado propriedade intelectual", utilizando-se de um laptop conectado a um dispositivo da rede do instituto). Swartz tornou-se réu de mais de uma dezena de acusações, vindas de diversas instâncias, com uma pena prevista em 35 anos e multa de US$ 1 milhão. Dois anos após a sua prisão, ainda no meio de uma pesada guerra judicial, Aaron Swartz se enforcou no seu apartamento, aos 26 anos.[549]

- Bradley Edward Manning foi preso e processado sob acusação de acesso e divulgação de material militar sigiloso. Dentre os documentos "vazados", destaca-se um vídeo, datado de 12 de julho de 2007, que mostra helicópteros Apaches atirando contra supostos soldados inimigos; após o ataque, constatou-se que as vítimas eram civis, sendo dois deles

[549] Por todos, vide NOGUEIRA, Bruno Torturra. "#SeJoga: Trip investiga o ativismo 3.0: o que há de novo na cabeça de quem sonha em mudar o mundo?". *Trip*. São Paulo, n. 220, p. 60-75, abr 2013.

correspondentes de guerra da agência Reuters. Bradley, atualmente Chelsea Elizabeth Manning, foi liberada após 10 anos de tortura psicológica em prisões militares, em 17 de maio de 2017.

- Julian Assange, já mencionado anteriormente, está sob asilo político na embaixada equatoriana em Londres, desde 2012.

- Acusadas de vinculação às operações do Anonymous, centenas de pessoas já foram presas, nos Estados Unidos, do Reino Unido, na Austrália, na Holanda, na Espanha e na Turquia.[550]

4.4.2 Sobre os movimentos sociais e a tecnologia da informação

A partir de um extenso estudo produzido por Charles Tilly, Patrick Underwood relatou que o movimento social é algo recente, tendo emergido nos séculos XVIII e XIX em decorrência de uma constelação de fatores sociais, políticos e econômicos.[551] Após o período das revoluções industriais e iluministas, os movimentos se desenvolveram como formas de comportamentos coletivos e, pelo efeito do processo de democratização em grandes nações ocidentais, nos séculos XIX e XX, foram assumindo a forma de importantes atores políticos. Essa construção histórica possibilitou fossem-lhe impressas algumas características importantes: esforços participativos e colaborativos; uso de demandas, identidade e programa comuns; reivindicação da soberania popular; tendência de proliferação, em caso de sucesso (o que é bastante evidente na luta pelo reconhecimento dos direitos civis iniciada no sul dos Estados Unidos e espalhada por outras arenas, posteriormente); fluidez para se adaptar a novos cenários e desafios (ao examinar as tendências dos movimentos, Tilly reconhece quatro padrões: internacionalização, declínio da democracia, profissionalização, triunfo).[552]

O impacto da tecnologia de comunicação (expansão dos grandes jornais, aderência da televisão ao cotidiano familiar, a disseminação da internet) nos movimentos sociais, em especial a partir da segunda metade do século XX, é um fator

[550] Atualmente, o mais completo relatório das prisões efetuadas sob acusação de pertencimento às operações do coletivo Anonymous encontra-se em OLSON, Parmy. *We are Anonymous*, *op. cit.*
[551] UNDERWOOD, P. C. *New directions in networked activism and online social movement mobilization*: the case of Anonymous and Project Chanology. 2009. Dissertação de Master of Arts – Department of Sociology and Anthropology, Ohio University, Ohio.
[552] *Ibid*., p. 56-60.

que merece atenção. Em primeiro lugar, pelo contexto de esfacelamento de muros classistas e ideológicos: o novo público, sumarizado a uma massa de consumidores, deu ensejo a um paradigma do movimento social, caracterizado por uma variedade de macro estruturalismos sem a fixação obsessiva com classes das concepções marxistas tradicionais. "Avesso a grêmios, estruturas partidárias ou sindicais, o indivíduo conectado começou a descobrir novos contextos para participar [do jogo político]", explicou Nogueira e prosseguiu: "Não era mais necessária a adesão a um panfleto, a uma ficha de filiação. Se tornou finalmente possível para uma pessoa desenvolver um discurso político essencialmente individual e de alcance público real".[553]

A *mass media* também provocou uma nova demanda no público; ao relacionar algumas das revoluções sociais experimentadas pelas democracias ocidentais, Garland destacou uma relevante consequência do impacto social da mídia de massa, em especial da difusão da tecnologia de comunicação televisiva: o surgimento de uma demanda social pela transparência e pela prestação de contas das instituições sociais e das administrações públicas, decorrente do interesse do público espectador no que ocorria nos bastidores (*backstage behaviour*) e que se traduzia no argumento de ordem: "o público tem o direito de saber".[554]

4.4.3 O caso WikiLeaks: pela liberdade de informação

Esse argumento de ordem ("o público tem o direito de saber"), se antes traduzia o interesse do público na prestação de contas das instituições públicas como uma exigência para um efetivo processo de democratização, a partir do desenvolvimento da internet, tornou-se uma demanda dos atores políticos cibernéticos contra a "nova distopia transnacional" da "vigilância pós-moderna".[555] O caso do WikiLeaks ilustra bem esse contexto. Sediado na Suécia, o WikiLeaks é uma organização transnacional que tem por função primordial "vazar" (publicar) informações e mídias, considerados confidenciais por governos e empresas, que envolvam temas relevantes, como crimes de guerra (*Baghdad airstrike*, 2007; *Afghan War Diary*, 2010; *Iraq War logs*, 2010),

[553] NOGUEIRA, Bruno Torturra. "#SeJoga: Trip investiga o ativismo 3.0: o que há de novo na cabeça de quem sonha em mudar o mundo?", *op. cit.*
[554] GARLAND, David. *The culture of control*. Chicago: University of Chicago Press, 2002. p. 86.
[555] Distopia, ou a antiutopia, é uma preocupação perene dos ciberativistas. Em seus escritos, eles denunciam que a rede mundial, sonhada como o grande instrumento de emancipação pessoal e social, revelou ser uma complexa transposição dos conflitos sociais para um ambiente virtual. Por todos, vide ASSANGE, Julian *et al. Cypherpunks*: freedom and the future of the internet. New York, London: OR Books, 2012.

violações de direitos humanos (*Guantanamo Bay procedures*, 2007; *Kenyan police*, 2008), corrupção e enriquecimento ilícito (Cientologia, 2008; *Peru Oil Scandal*, 2008), atividade política (*Sarah Palin*, 2008; *Diplomatic cables*, 2010; *Syria files*, 2012). O objetivo da organização, conforme relatado em sua página virtual, é "trazer notícias e informações importantes ao público".[556]

WikiLeaks e Anonymous, como bem o afirmou Coleman, pertencem à mesma família, mas, ao mesmo tempo, são o oposto um do outro.[557] Assemelham-se não só porque o coletivo promoveu ataques em decorrência do boicote financeiro feito ao WikiLeaks (como já visto) ou porque Julian Assange, editor e porta-voz do WikiLeaks, demonstra ser simpático às ações do Anonymous (tendo, inclusive, feito contato com alguns dos principais Anons[558] e usado a máscara de Guy Fawkes durante o *Occupy London Stock Exchange*[559]), mas porque comungam na atividade de lutar pela livre informação através do ciberativismo e do hacktivismo. Distinguem-se, todavia, porque, enquanto o coletivo é, por princípio e atividade, anônimo, o WikiLeaks se personaliza em Assange. Essa individualização *per se* foi suficiente para a forte persecução promovida contra o jornalista.

4.4.4 O desenvolvimento do Anonymous

The evolution of Anonymous as a political actor, uma rara monografia científica sobre o tema, de Max Halupka, destaca-se pela extensa revisão bibliográfica de uma literatura específica sobre comunidades virtuais, movimentos sociais e redes de comunicação descentralizadas e pela elaboração de uma linha do tempo do coletivo e das suas operações (uma vez que inexiste um repositório próprio e oficial da história e das atividades do *Anonymous*).[560]

O trabalho se inicia com a discussão sobre a dificuldade da transposição do conceito de *comunidade* – T. Erickson[561], por exemplo, exige: associação, relacionamento, compromisso, reciprocidade generalizada, compartilhamento de valores

[556] Disponível em <http://wikileaks.org/About.html>.
[557] COLEMAN, Biella. "Hacker Politics and Publics", *Public Culture*, n. 23, v. 3, 2011. p. 511.
[558] OLSON, Parmy. *We are Anonymous*, *op. cit.*
[559] WAITES, Rosie. "V for Vendetta masks: Who's behind them?", *BBC News Magazine*, London, 20 out 2011.
[560] HALUPKA, Max. *The evolution of Anonymous as a political actor*. 2011. Monografia de Bachelor of Arts – Honours Program in Political Studies, School of Social and Policy Studies, School of Social and Policy Studies, The Flinders University of South Australia, Camberra.
[561] *Apud* HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 16.

e práticas, bens coletivos e duração – ao ambiente *online*, uma vez que a virtualidade do meio não apresenta características clássicas como um território geográfico, uma história comum, comunicação face a face, deficiências que permitem interpretações de que a comunidade virtual é uma extensão da comunidade real, e não um sistema autônomo. No que refere ao território geográfico, pode-se antecipar que este pressuposto já não mais é exigível para o contexto das relações cibernéticas, pois as comunidades virtuais e comunicação estabelecida entre seus participantes oportunizam exatamente a realização e o fortalecimento de vínculos entre indivíduos geograficamente estranhos, numa dinâmica poliádica.[562] No que tange à comunicação, por sua vez, é preciso compreender que ela não se resume à expressão oral: a comunicação mediada por computador permite tanto a utilização de aplicativos de textos (e-mails, *bulletin boards*, salas virtuais de bate-papo) quanto de imagens e multimídia.[563] Halupka apoia-se na síntese, elaborada por M. Diani, da dinâmica do movimento social, segundo a qual se identificam: redes de interação informal, crenças compartilhadas e solidariedade, e ação coletiva diante de questões conflituais.[564]

De acordo com Chris Dishman, quem analisou a composição de grupos terroristas e criminais, há três formas de organização em relação à liderança: hierárquica, estrutura celular descentralizada e resistência sem liderança.[565] A estrutura do Anonymous indica a combinação desses dois últimos modelos: cada célula é funcionalmente independente das outras e trabalha com objetivos distintos, os quais contribuem, ao termo da ação, com o objetivo geral da organização; há uma proeminência do modelo celular descentralizado porque, ao contrário da resistência sem liderança (caracterizada pelos *lonely wolves*), o Anonymous demonstra uma constante comunicação, o que garante que todos trabalhem conforme um objetivo final comum.

Parmy Olson, jornalista da Forbes, investigou o grupo Anonymous mais a fundo. Segundo a autora do livro *We are Anonymous*, o Anonymous é uma comunidade amorfa de pessoas de diversos lugares que colaboram entre si, on-line, e seguem uma única regra de jamais revelar suas reais identidades. Olson, porém, encontrou uma definição mais precisa ao grupo ao lhe atribuir a característica de um processo, de um espaço dinâmico:

---

[562] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 19.
[563] *Ibid*., p. 18.
[564] *Ibid*., p. 24.
[565] DISHMAN, C. "The Leaderless Nexus: When Crime and Terror Converge", *Studies in Conflict & Terrorism*, n. 28, 2005. p. 237-252.

> Ele é essencialmente um campo de encontro no éter na rede. (...) Assim, Anonymous não é uma organização de hackers, mas uma nebulosa comunidade de pessoas que têm crescido com a internet, que entendem a cultura da internet e sabem alguns dos truques mais popularizados de subverter os meios de controle cibernético.[566]

Seus participantes – que podem ser qualquer pessoa (hackers, ativistas, defensores de direitos humanos, *geeks*), inexistindo qualquer rito de passagem oficial – se identificam como "Anons" e o seu reconhecimento se dá através de signos como a logo do homem engravatado sem cabeça e a máscara de Guy Fawkes (estilizada conforme o desenho de David Lloyd para os quadrinhos de Alan Moore, *V for Vendetta*). Sua *tagline* mais utilizada é a apresentação hostil: "*We are Anonymous. We do not forgive. We do not forget. Expect us.*"

Emblema do Anonymous

Máscara de Guy Fawkes

O histórico de suas atividades traduz dois aspectos importantes de sua estrutura. Primeiro, a assunção espontânea de objetivos – os quais mostram uma evolução: diversão, comprovação de capacidade técnica, justiçamento, luta contra a supressão de informação, causas específicas – comprova a ausência de um programa ideológico e de unidade corporativa, o que justifica a frequente conotação com a figura da Hidra de Lerna. Segundo, esse histórico é suficiente para demonstrar a intensificação e a

[566] "[3'44"] Anonymous is an amorphous community of people located all over the world who collaborate with witch other online while following the single rule that they never reveal their true identities. (…) [4'40"] It's essentially a meeting ground in the ether of the web. (…) [11'45"] As such, Anonymous is not an organization of hackers, but a nebulous community of people who've grown up with the internet, who understand internet culture and know some of the popularized tricks for subverting the internet spy ways." (OLSON, Parmy. *"We are Anonymous" Parmy Olson's Noblis presentation*. Disponível em <http://www.youtube.com/ watch?v=3pQjrZ0gJfo>.)

complexificação de suas atuações. A análise do desenvolvimento do coletivo Anonymous segue a estrutura sugerida por Max Halupka.[567]

4.4.4.1 Início (2003-2005)

A origem do movimento de Anonymous é associada ao *imageboard 4chan* (*chan* é a abreviação de *channel*), um fórum de discussão de destaque por sua interface simples, pela desnecessidade de cadastro e pela brevidade de seu histórico das discussões, as quais se compõem de postagens de imagens e textos. Lançado em 1º de outubro de 2003, o fórum tinha uma concepção original de ser um espaço para postagens de quadrinhos (mangás) e desenhos animados (animes) japoneses; no entanto, a fácil utilização e o anonimato de seus participantes oportunizaram que a página se tornasse campo fértil para manifestações subculturais[568] e ativistas.

O anonimato da participação nessa comunidade virtual era incidental: aos participantes era oportunizada a escolha de um pseudônimo na caixa *nickname*; na ausência de preenchimento, o sistema do *4chan* automaticamente atribuía a alcunha de *anonymous* ao participante.[569] A impossibilidade de identificação de autoria, a ausência de controle e de censura foram excelentes atrativos para os participantes, os quais passaram a desenvolver e utilizar um léxico próprio pela criação e propagação de *memes*.

Foi no fórum *random* (ou */b/*) desse espaço cibernético que nasceu o Anonymous, inicialmente voltado à criação de *memes* e à realização de *trolls*. Criado por Richard Dawkins, o termo *meme* consiste na unidade mínima de memória capaz de disseminar uma informação cultural e, por extensão de sentido no campo cibernético, é a ideia transmitida pela rede que se torna um fenômeno comunicativo.[570] Por sua vez, *troll*, do verbo inglês que descreve o recolhimento da linha com o peixe fisgado, é uma ideia lançada em fóruns ou páginas de relacionamento que objetivam provocar pessoas ou desestabilizar discussões – o termo *lulz*, derivado do acrônimo *lol* (*laugh out loud*),

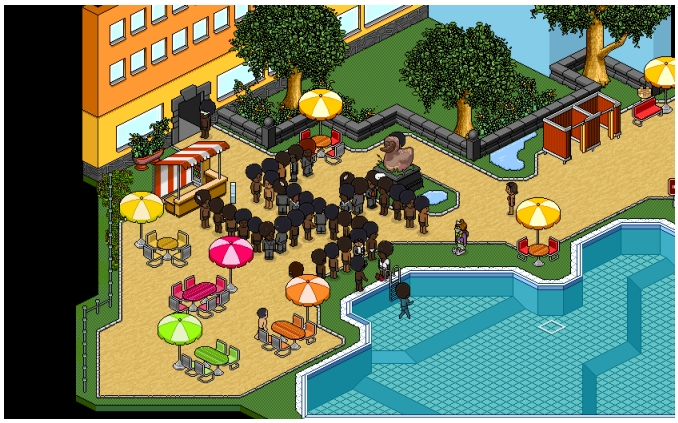
[567] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 32 e ss.
[568] A qualificação subcultural refere-se a uma cultura que se diferencia de uma cultura majoritária com a qual se relaciona e compete, conforme à designação tradicional das ciências sociais. A nomenclatura é merecidamente criticável por sugerir uma relação de inferioridade, porém, para esta tese, que não investiga essa valoração, preferiu-se a manutenção do termo mais usual.
[569] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 33.
[570] DAWKINS, Richard. *O gene egoísta*. trad. Rejane Rubino. São Paulo: Companhia das Letras, 2007.

porta o mesmo significado e representa tanto um éthos quanto um objetivo atual do grupo.[571]

4.4.4.2 Comunidade social progressiva (2006-2008)

Nos anos subsequentes, as ações do coletivo Anonymous se disseminaram por outras comunidades virtuais em razão do sucesso contagiante da comunicação decorrente das imagens provocativas e irônicas dos *memes*. Além disso, fatores importantes para a expansão do coletivo foram a orquestração e a coordenação de ataques repentinos (raides) a páginas e redes virtuais, o que destacou a funcionalidade do grupo na execução conjunta. Os primeiros raides não decorreram de uma agenda política, moral, ética ou filosófica; inicialmente eram campanhas espontâneas de retribuição à "seriedade" da internet.

Ainda nesse período, porém, é possível identificar algumas atividades *vigilantes* do coletivo *Anonymous*, dentre os quais se destacaram os ataques à comunidade virtual Habbo Hotel e a investigação e a denúncia do canadense Chris Forcand.[572] No contexto virtual de Habbo Hotel, adolescentes selecionam personagens e participam de encontros em hotéis (virtuais), espalhados pelo mundo. Após os usuários perceberem que havia restrições para o uso de avatares negros no programa e depois da divulgação da notícia de que uma criança de dois anos tinha sido impedida de usar uma piscina no Alabama, em razão de sua enfermidade (AIDS), membros do coletivo organizaram uma invasão de avatares de cabelos estilo afro no ambiente virtual e bloquearam o uso da piscina com dizeres "fechada devido à AIDS", com uma formação que remetia à suástica:



[571] COLEMAN, Biella. "Our Weirdness is Free: The logic of Anonymous – online army, agent of chaos, and seeker of justice", *op. cit.*
[572] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 43.

Em 2007, o coletivo identificou Chris Forcand como um pedófilo e, sob o disfarce de uma garota de treze anos chamada Jessica, gravou um extenso diálogo com conteúdo sexualmente explícito e troca de fotografias, denunciando-o posteriormente à autoridade policial; Forcand foi preso em sua residência, um mês depois.

Quanto a esta dinâmica, Halupka afirmou que foi nesse momento que ao Anonymous foi conferido, além de um marco comunal (que já se verificava no princípio de suas atividades), o sentido de um conceito filosófico.[573] O próprio coletivo foi conceitualizado e inúmeros argumentos daí decorreram: todos e ninguém poderiam participar do Anonymous; o Anonymous não teria forma senão existência na mente daqueles que participam do coletivo; o Anonymous não poderia ser derrotado, destruído ou vencido pelo tempo. Anonymous tornou-se mais que um coletivo para os seus membros; ele se tornou um ideal.[574]

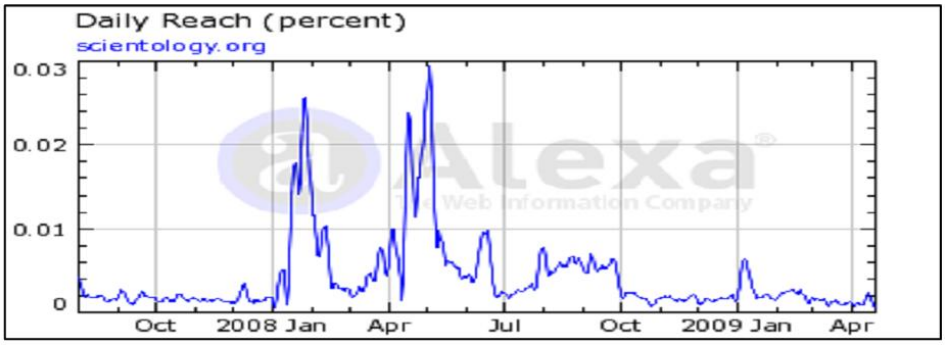
4.4.4.3 Movimento social (2008-2009)

O desenvolvimento do Anonymous como um movimento social teve como marco inicial a *Operation Chanology*, em janeiro de 2008. A partir da pressão imposta pela Igreja da Cientologia para retirar da internet um vídeo no qual o ator Tom Cruise discorria sobre questões cientológicas, o coletivo encontrou o argumento necessário (restrição à liberdade de informação) para empreender uma campanha contra a igreja. Halupka[575] e Underwood[576] argumentam que o coletivo aguardava um entretenimento mais complexo, um embate em que o adversário reagisse violentamente quando provocado – a Igreja da Cientologia cumpria bem esta expectativa –, mas que, no decorrer da campanha e dos ataques, uma agenda filosófica formatou-se em conjunto com a persona pública.

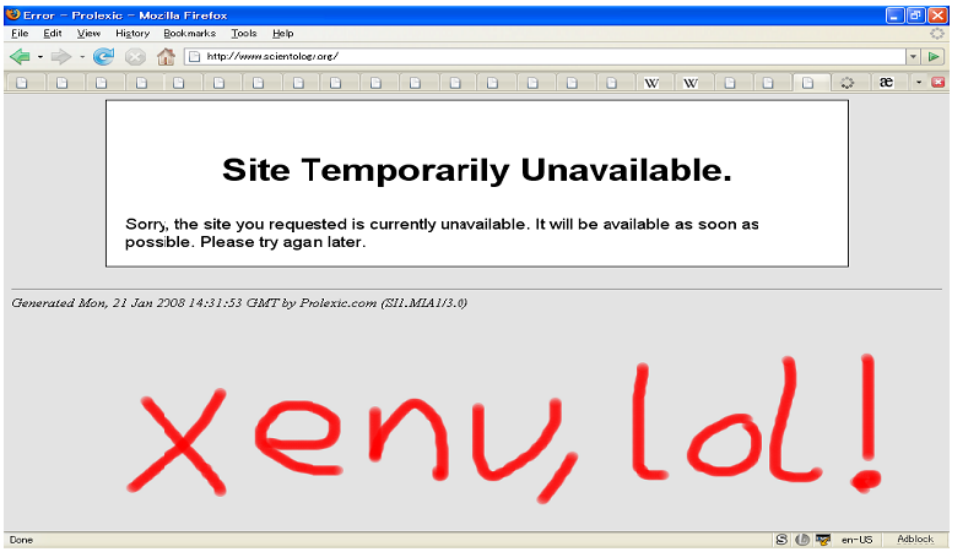
As primeiras ações realizadas foram ataques *denial-of-service* (DDoS), nos quais foram "derrubados" os servidores das páginas WWW.SCIENTOLOGY.ORG (primeiro e principal alvo), WWW.RTC.ORG (segundo alvo) e de 22 páginas virtuais afiliadas ao

[573] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 39.
[574] *Ibidem*.
[575] *Ibid*., p. 44.
[576] UNDERWOOD, P. C. *New directions in networked activism and online social movement mobilization*, *op. cit.*

grupo religioso. O gráfico[577] seguinte mostra o tráfego médio da página WWW.SCIENTOLOGY.ORG; os acentuados picos representam os raides realizados pelo Anonymous, que resultaram no desligamento da página:



A "queda" da página gerava a informação de inacessibilidade temporária[578], o que se tornou um troféu ao coletivo Anonymous:



Em 21 de janeiro de 2008, um vídeo-mensagem[579] foi divulgado, sob o título de *Message to Scientology*, no qual uma voz sintética de computador narrava:

> Hello, Leaders of Scientology. We are Anonymous.
> Over the years, we have been watching you. Your campaigns of misinformation; your suppression of dissent; your litigious nature, all of these things have caught our eye. With the leakage of your latest propaganda video

[577] *Ibid*., p. 131.
[578] *Ibid*., p. 132.
[579] Sobre o processo de elaboração da mensagem, vide UNDERWOOD, P. C. *New directions in networked activism and online social movement mobilization*, *op. cit.*, p. 136-137.

> into mainstream circulation, the extent of your malign influence over those who have come to trust you as leaders, has been made clear to us. Anonymous has therefore decided that your organization should be destroyed. For the good of your followers, for the good of mankind and for our own enjoyment. We shall proceed to expel you from the Internet and systematically dismantle the Church of Scientology in its present form. We recognize you as serious opponents, and do not expect our campaign to be completed in a short time frame. However, you will not prevail forever against the angry masses of the body politic. Your choice of methods, your hypocrisy and the general artlessness of your organization have sounded its death knell.
> You have nowhere to hide, because we are everywhere.
> You will find no recourse in attack, because for each of us that falls ten more will take his place.
> We are cognizant of the many who may decry our methods as parallel those of the Church of Scientology, those who espouse the obvious truth that your organization will use the actions of Anonymous as examples of the persecution of which you have for so long warned your followers. This is acceptable to Anonymous. In fact, it is encouraged. We are your SPs.
> Over time, as we begin to merge our pulse with that of your "Church", the suppression of your followers will become increasingly difficult to maintain. Believers will become aware that salvation needn't come at the expense of their livelihood. They will become aware that the stress and the frustration that they feel is not due to us, but a source far closer to each. Yes, we are SPs. But the sum of suppression we could ever muster is eclipsed by that of your own RTC.
> Knowledge is free.
> We are Anonymous.
> We are Legion.
> We do not forgive.
> We do not forget.
> Expect us.

Após um valioso conselho do anti-cientologista Mark Bunker[580], as ações *online* transmutaram-se em *offline*, quando o coletivo tomou as ruas. Manifestações públicas que chegaram a alcançar um público de 8 a 10 mil protestantes, foram realizadas diante de centros cientologistas, em 93 diferentes cidades pelo mundo, em 10 de fevereiro de 2009.[581] Sobre isso, escreveu Bunker, em sua página:

> A poucas semanas do início de suas atividades, eles [Anonymous] lançaram o seu primeiro piquete global e cerca de dez mil pessoas apareceram em suas cidades pelo mundo para protestar pacificamente contra a Cientologia. Eles construíram websites e espalharam fliers e deram discursos e assustaram os líderes da Cientologia, os quais não tiveram qualquer ideia de como constranger ou intimidar um grupo de pessoas sem nome, enorme, amorfo e sem líderes, todos usando a mesma máscara de Guy Fawkes. Pessoas têm protestado contra a Cientologia desde que a Cientologia foi criada, mas nunca nessa escala. E o Anonymous adicionou fantasias e temas e trouxeram o teatro de rua para seus eventos.

---

[580] BUNKER, Mark. *Scientology: XENU TV Speaks to Anonymous*. Disponível em <http://www.youtube.com/watch?v=zW466xcM0Yk>.
[581] UNDERWOOD, P. C. *New directions in networked activism and online social movement mobilization*, *op. cit.*, p. 153.

> Com o passar dos meses, os números diminuíram, mas isso era esperado. Alguns estavam nisso somente pela diversão [*lulz*]. Porém outros vieram para ver que havia uma razão real para agir e ajudar aqueles que estavam sendo abusados pela Cientologia e eles continuaram a protestar todos os meses, eles continuam a encher a rede com ótimos vídeos e construir websites e ajudar a causa.[582]

Para evitar serem reconhecidos (a igreja da Cientologia é notória por processar seus críticos e adversários), os manifestantes usaram lenços ou máscaras de gás e, nos últimos protestos, a máscara estilizada de Guy Fawkes, o que foi, a partir de então, adotado como símbolo do coletivo.

4.4.4.4 Rede celular descentralizada (2010-)

Em seus feitos, duas correntes surgiram no interior do coletivo: os puristas, segundo os quais o Anonymous deveria limitar-se ao humor agressivo original (*lulz*); e os moralistas, os quais passaram a defender intervenções em prol da liberdade de informação.[583] O momento atual, do Anonymous como uma rede celular descentralizada, é caracterizado pela ascensão da ideologia moralista.

Na Operação *Payback* (2010), instituições antipirataria e pró-direitos-autorais foram atacadas em prol da desregulamentação dos direitos autorais digitais. A operação foi renomeada, em dezembro de 2010, para *Avange Assange*, em razão do boicote promovido por várias empresas financeiras contra o WikiLeaks; essas empresas haviam cedido às pressões governamentais para a interrupção de transferência de doações à organização de Assange. Foram atacados os sistemas da Amazon, da Paypal, da MasterCard, da Visa e do banco suíço PostFinance.[584]

Em fevereiro de 2011, um artigo do Finantial Times (*Cyberactivists warned of arrest*, de Joseph Menn) citou que o CEO da HBGary Federal, Aaron Barr, havia anunciado que sua empresa tinha conseguido se infiltrar no Anonymous e que planejava revelar nome de seus participantes.[585] A reação do coletivo foi vigorosa: *Anonymous* conseguiu invadir o banco de dados da empresa e descarregou 66 mil e-mails internos; em confronto direto com Barr, o grupo obteve informações como o número de seu *social security*, endereço, telefone e senha de acesso ao seu Twitter; o coletivo também

---

[582] Disponível em <http://www.xenutv.com/blog/faq/about-anonymous/>.
[583] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 47-49.
[584] COLEMAN, Biella; RALPH, Michael. "Is it a crime? The Transgressive Politics of Hacking in Anonymous", *op. cit.*
[585] *Ibidem*.

inundou a comunicação da empresa (telefones e faxes) com chamadas vazias.[586] Da leitura das seus e-mails pessoais, o grupo descobriu que Barr pretendia vender os "dados obtidos" ao FBI; na carta-resposta que comunicou os ataques realizados, o Anonymous alegou que as informações que haviam sido coletadas eram *nonsense* e que o material não poderia ser vendido à autoridade policial:

> Então, por que você não pode vender essa informação ao FBI, como você pretendia? Porque nós a entregaremos a eles, de graça. O seu gloriosamente falacioso trabalho será uma maravilha para todos vasculharem, assim como serão todos os seus e-mails privados (mais de 66 mil belezuras para a alegria do público).[587]

Barr renunciou ao cargo. Este episódio transcendeu, porém, os ataques à empresa: muitos críticos do grupo, em especial os especialistas em TI, admitiram a proficiência técnica do coletivo e a seriedade do seu movimento; o episódio também revelou que os ataques partiram majoritariamente de distintas *células fantasmas*, e não de uma organização central.

Foi esse modelo de ataque que foi utilizado na Operação Tunísia. Após a notícia de censura cibernética por parte do regime autoritário posto em xeque pela população, o *Anonymous* iniciou uma campanha de raides contra as páginas do governo da Tunísia e seus afiliados. O *modus operandi* revelou que o coletivo tinha menos o interesse em provocar ou se vingar do governo do que revelar ao mundo o que estava acontecendo naquele território.

4.4.5 A irreverência (*lulz*) como fim ou a irreverência como instrumento de uma ação política ainda presente?

Em uma palestra sobre o seu livro, Olson declarou: "Eles parecem sérios, eles parecem perigosos, e, em grande parte, eles não são." Segundo a jornalista, haveria uma grave ingenuidade do coletivo: enquanto os verdadeiros criminosos cibernéticos, aqueles que lucram do furto de dados (números e senhas de cartões de créditos ou endereços de e-mails para destinos de spams), não anunciam suas atividades no Twitter ou através de notas à imprensa, permanecendo quietos para que possam prosseguir

---

[586] HALUPKA, Max. *The evolution of Anonymous as a political actor*, *op. cit.*, p. 53; OLSON, Parmy. *We are Anonymous*, *op. cit.*

[587] COLEMAN, Biella. "Our Weirdness is Free: The logic of Anonymous – online army, agent of chaos, and seeker of justice", *op. cit.*

fazendo negócios, os apoiadores do Anonymous tornam público cada ataque, provocam a polícia e, assim, praticamente assinam os seus próprios mandados de prisão no processo. E essa ingenuidade conduziria o coletivo a um inevitável desaparecimento. A conclusão foi antecipada.

Após o encerramento da pesquisa de Olson, o coletivo empreendeu algumas operações mais complexas e pesadas – ataque e publicação de dados dos clientes da Sony e de um milhão de números de identificação (*ID number*) de aparelhos da Apple; além de documentos sigilosos da OTAN – e dezenas de prisões começaram a ser realizadas, em especial nos Estados Unidos e na Europa, sob acusação de participação nas atividades do Anonymous. Desde então, as atividades do coletivo tornaram-se mais *underground* e difíceis de serem rastreadas. Paradoxalmente, a isso correspondeu a proliferação de sua presença simbólica – atuação informal, porém crucial – em protestos sociais como o *Occupy Wall Street*, modelo de protesto social que se espalhou por várias cidades do mundo e que demanda maior atenção à sociedade que não participa dos perigosos jogos financeiros que podem causar crises graves (por isso, o slogan "We are the 99%", em contraposição ao 1% que gerencia a economia global).[588]

O coletivo cibernético *Anonymous* pode chegar ao seu termo, como consequência natural do seu próprio desenvolvimento. A previsibilidade disso é arriscada porque as próprias características do grupo não permitem prognósticos precisos. O que é certo, porém, é que o ciberativismo e o hacktivismo, como práticas de ação política, deram somente seus primeiros passos. A irreversibilidade da tecnologia e da comunicação cibernética demonstra que ações como essas poderão ser interpeláveis, mas não plenamente evitáveis. Nesse sentido, Anonymous, findo ou não, tornou-se um paradigma de demandas e conflitos sociais na era da tecnologia da informação, empregando no seu ciberativismo muitos daqueles considerados *cybercrimes* próprios.

[588] COLEMAN, Biella. "Our Weirdness is Free: The logic of Anonymous – online army, agent of chaos, and seeker of justice", *op. cit.*

CONCLUSÕES

> Era uma vez, o amanhã nunca chegou. Seguramente protegido nas extensões de tempos distantes e remotas galáxias, o futuro era ficção científica e pertencia a outro mundo. Agora, ele está aqui, rompendo o infinito adiamento dos horizontes humanos, curto-circuitando a história, fazendo o download de suas imagens no hoje. Enquanto o homem histórico continua a olhar fixamente o espelho retrovisor da interface, guardando o presente como uma reprodução do passado, as areias do tempo afluem no silício, e a memória somente de leitura [*Read Only Memory*] chegou ao fim. A revolução *cyber* é virtualmente real.[589]

Esta tese não pretende apresentar um rol exaustivo dos *cybercrimes* e sua extensão não permite um maior aprofundamento sobre questões diversas que declinam da proposta de um novo olhar criminológico sobre o fenômeno *cyber*. E talvez isso sequer seja possível diante de tantas tendências e vulnerabilidades emergentes. Reflita, por um momento, no potencial de crimes, desvios e ameaças diante, por exemplo, do hoje comum armazenamento de dados em nuvens (iCloud, Google Drive, OneDrive, Dropbox) ou do contemporâneo processo de convergência digital, no qual, diferente do computador pessoal (PC), os aparelhos circulam por vários pontos de acesso à internet, numa circulação cujas medidas de segurança ainda estão em aperfeiçoamento. Ou, pense na implicação de algo mais cotidiano, a internet das coisas: implantes cirúrgicos, aparelhos de monitoramento anexos ao corpo, sistemas de automação residencial (calefação, ventilação, iluminação, sistemas de segurança, sistemas de entretenimento); eletronicamente conectados e remotamente controláveis, eles multiplicam oportunidades de vulnerabilidades de segurança e privacidade.

Hão de ser desenvolvidas muitas criminologias *cyber* sobre a autonomia e a arquitetura do ciberespaço, os atuantes cibernéticos, as suas causas e motivações, as identidades desincorporadas, as formas de expressão, controle e punição do comportamento desviante no contexto da tecnologia da informação. Aqui estão presentes os pressupostos fáticos e científicos que orientam um novo viés de estudo. E, com eles, se apresenta uma proposta de criminologias *cyber* que pressupõe a técnica como uma realidade ontológica temporal e dinâmica – um modo de revelação, um modo de saber – e a essência da técnica como um acontecimento condicionante (e não mero meio).

---

[589] PLANT, Sadie. "On the matrix: cyberfeminist simulations", *op. cit.*, p. 334.

A compreensão de que se está diante de um processo de adaptação da criminologia e de que perspectivas alternativas são necessárias faz com que categorização qualitativa do comportamento desviante (tradicionais, híbridos e próprios) seja mais do que uma divisão didática. Essa distinção evidencia como, para muitos casos, um conjunto de saberes tradicionais permanecem válidos ao ciberespaço, podendo ser transposto e aplicado à nova realidade (e, quando insuficiente, pode ser adaptado ou estendido para maior abrangência), enquanto que, para casos inéditos, na categoria de comportamentos estruturados e condicionados pela tecnologia da informação, há necessidade de uma articulação criminológica própria para o fenômeno *cyber*. Que seja esse o primeiro passo e que os próximos cliques não se demorem. Porque, como anunciou Plant, a revolução *cyber* é virtualmente real.

ANEXO I

GLOSSÁRIO

Anonymous Operations IRC (*AnonOps*) é uma plataforma internacional de comunicação frequentada pelos Anonymous e outros ativistas.

Bit (acrônimo de *binary digit*) é um dígito binário representado pelos algarismos 0 ou 1. Um agrupamento de 8 *bits* corresponde a um *byte* (*binary term*), também chamado de octeto. Os valores 0 e 1 em conjunto constituem a informação passível de processamento por um computador. Enquanto a notação para *bit* e seus múltiplos utiliza um *b* minúsculo – bit (b), quilobit (kb), megabit (Mb), gigabit (Gb) e Terabit (Tb) –, a notação para *byte* utiliza um *B* maiúsculo (kB, MB, GB, TB). No sentido da teoria da informação, *bits* conota "tal informação" (Assange 2015: 133).

Bitcoin "é um tipo de moeda digital baseado em criptografia. Como qualquer outra moeda, o Bitcoin pode ser trocado por dólares ou outras moedas, ou então usado para fazer compras, mas não está ligado a um banco central e, diferentemente das moedas fiduciárias, o Bitcoin não é controlado por poder de Estado. (...) O Bitcoin é uma rede *peer-to-peer*, sem nenhuma autoridade central por trás dela." Assim, para verificar se um Bitcoin é verdadeiro ou cópia, o histórico econômico do Bitcoin é distribuído a computadores não relacionados por todo o mundo. Essa verificação exige constante sincronização entre os computadores, possibilitando que todas as máquinas conectadas identifiquem quais transações de Bitcoin são válidas e quais são falsas. (Assange 2015: 136-137)

Cookie é um pequeno pacote de dados enviado por um *website* e depositado no navegador do usuário quando ele acessa determinada página. Os "*cookies* tornam possível que o computador autentique que é a mesma máquina que estava acessando um *website* um momento anterior" (Lessig 2006: 48).

Denial of service attack (ou *DDoS*), livremente traduzido como um *ataque de negação de serviço*, é "uma tentativa de tornar um site inacessível enviando tantas solicitações de acesso que o site é incapaz de atender todas. É uma maneira de censurar um site, atingindo sua fonte e tirando-o do ar." (Assange 2015: 132)

Facebook é um serviço de rede social online, lançado em 4 de fevereiro de 2004, operado e de propriedade privada da Facebook Inc.

FTP (*File Transfer Protocol*), traduzido como protocolo de transferência de arquivos, é um dos métodos utilizados para enviar arquivos pela internet.

Filtragem, ou *controle de conteúdo*, ocorre "quando um provedor bloqueia o acesso a um site. É uma maneira de censurar um site, colocando-se entre um usuário e um site e interferindo seletivamente no tráfego." (Assange 2015: 132)

Form grabbing é um *malware* que recupera credenciais de autorização e acesso de formulários da internet antes que sejam transferidas para um servidor seguro.

Hiperdocumento refere-se ao arquivo que apresenta recursos de hipermídia em formatos diversos (diagramas, textos, imagens, sons, vídeos, softwares etc.), interligado a outros documentos por meio de links programados em pontos-chave, de modo que o usuário possa passar de uma informação para outra, conforme seu interesse (Houaiss).

Hipertexto é uma forma de apresentação de informações, organizada de tal maneira que o leitor tem liberdade de escolher vários caminhos, a partir de sequências associativas possíveis entre blocos vinculados por remissões, sem estar preso a um encadeamento linear único; a prática da leitura de dicionários e enciclopédias (com seus índices, referências e remissões) e da pesquisa em bibliotecas (fichas e catálogos) já proporcionava este tipo de experiência. No caso de informações digitais, algum elemento é destacado e, quando acionado, provoca a exibição de um novo hipertexto com informações relativas ao referido elemento.

HTTPS (*Hypertext Transfer Protocol Secure*), traduzido como Protocolo Seguro de Transferência de Hipertexto, é "um protocolo que criptografa as conexões entre um navegador e um servidor". (Assange 2015: 132)

Infraestrutura crítica (*IC*): instalações, serviços e bens que são essenciais para o funcionamento de uma sociedade; a interrupção ou a destruição de uma IC pode ter um impacto debilitante no bem-estar social e econômico, e na segurança nacional. Exemplos de ICs: geração, transmissão e distribuição de energia elétrica; serviços financeiros; produção e distribuição de alimentos; produção, transporte e distribuição de combustíveis; saúde pública (hospitais, ambulâncias); serviços de segurança (policiais, militares); telecomunicação; sistemas de transporte; suprimento de água. As ICs podem incluir bens materiais cujo conteúdo simbólico ou significado inerente seja considerado importante para a coesão e o bem-estar nacional (ver Yar 2013: 51).

Interface é o elemento que proporciona uma ligação física ou lógica entre dois sistemas ou partes de um sistema que não poderiam ser conectados diretamente, ou o meio pelo qual o usuário interage com um programa ou sistema operacional (Houaiss); qualquer dispositivo que permite a interação entre o universo da informação digitalizada e o mundo ordinário (Lévy 2000: 19).

Internet é um conjunto de protocolos comuns de informação que permitem computadores pessoais comunicar-se por meio de redes.

Internet Protocol address (*IP*) é o número identificador único que dispositivos de rede utilizam para se identificar e se comunicar.

ISP (*Internet Service Provider*) é o provedor de acesso à internet.

Key logger é um *spyware* cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins.

Livestream, conhecido originalmente como Mogulus, é uma plataforma de *streaming* (fluxo de mídia, sem armazenamento) de vídeo que permite a seus usuários assistir e transmitir vídeos através da internet, utilizando uma câmera e um computador.

Logic bomb [bomba lógica] é um tipo de software malicioso que é ativado quando um critério predeterminado é satisfeito, tal como uma data específica, disparando uma função danosa (por exemplo: danificando uma rede de computadores ou apagando registros e discos rígidos). As *logic bombs* podem ser utilizadas para "ganharem tempo" e se espalharem antes de serem percebidas.

Low Orbit Ion Cannon (*LOIC*) é um teste de força de rede, servindo também como um aplicativo de ataque DDoS.

Mainframe é o computador de grande capacidade de processamento, geralmente capaz de ser utilizado por diversos usuários simultaneamente, concebido para atender às necessidades de grandes corporações. (Houaiss)

Peer-to-peer networks (*P2P*) caracteriza a arquitetura distribuída de aplicativos que compartilha tarefas ou cargas de trabalhos entre pares. Na rede P2P, "o *servidor* não desempenha um papel de armazenamento, ele apenas atua como intermediário de conexões, as quais serão efetivamente realizadas entre os *pares* – entre os *hosts* da rede de compartilhamento de arquivos – e não entre estes e o *servidor*. O *servidor* em uma rede *P2P* irá desempenhar um duplo papel: a) de *indexador*, armazenando os dados de *quem tem o quê*; b) de *guia*, informando, a cada pedido feito através de uma busca, onde está disponível o *arquivo* solicitado." (Colli 2009: 52, grifos no original)

Pharming é uma versão automatizada do *phishing*, que engana o Sistema de Nomes de Domínio (*DNS*) fazendo-o aceitar automaticamente dados de acesso incorretos. Ao alterar os registros armazenados do computador-alvo, as pessoas são automaticamente redirecionadas a *websites* fraudulentos: ao digitar o endereço do *site* (*URL*: Localizador Uniforme de Recursos) que deseja visitar, o servidor DNS contaminado pode apontar para um *site* falso, semelhante, por exemplo, à página virtual do banco da vítima (também chamado de clonagem estética de *website*). O *pharming* não depende de engenharia social para enganar pessoas.

Phishing é a utilização das comunicações na internet para a prática de engenharia social (enganar pessoas) com a finalidade de se obter informações financeiras pessoais. As mensagens sugerem ser de instituições financeiras, lojas virtuais, prestadores de serviços ou até de ofertas de emprego, e seus recursos gráficos podem fazer as vítimas acreditarem que o e-mail vem da empresa anunciada (Siegel 2010, p. 473). Geralmente, as vítimas são solicitadas para voluntariamente entrar no endereço URL fornecido no e-mail, confirmando informações pessoais. As solicitações mais comuns são *verificação de conta* e *confirmação de pagamento*. Além disso, é comum e-mails de *phishing* e *spam* utilizarem *spoofing* (a criação de mensagens de e-mails com um endereço de remetente forjado) para induzir em erro o destinatário sobre a origem da mensagem; a criação de campos "De:" forjados, porém verossímeis, nos e-mails torna maior a possibilidade de as mensagens serem abertas.

Ransomware é um software malicioso que sequestra um sistema de computador por meio de criptografia até que um resgate seja pago (preferencialmente, com criptomoeda, como Bitcoin) ou que a vítima concorde em infectar outros sistemas; o código de descriptografia é, então, liberado pelo chantagista.

Revenge porn (ou, pornografia de vingança) ocorre quando uma mídia (fotos ou vídeos) íntima é transformada em instrumento [*weaponized*] de vingança e é divulgada ou compartilhada sem consentimento da pessoa exposta, por um ex-companheiro, com o propósito de causar dano à vítima, geralmente do sexo feminino.

Reverse DNS look-up é a determinação de um nome de domínio associado a um endereço IP na Internet.

Sexting é a troca de mensagens, fotografias ou imagens sexualmente explícitas, principalmente entre aparelhos celulares. A prática disseminou-se ainda mais a partir de aplicativos de mensagens, como Snapchat e WhatsApp. A princípio, respeitadas a consensualidade e a confidencialidade, não se vislumbram relevantes conflitos pessoais, sociais ou legais. O *sexting* torna-se um dilema quando os atuantes são menores de idade e voluntariamente participam da comunicação eletrônica sexualmente orientada, com o compartilhamento de *nudes*, porque eventuais propostas de criminalização da conduta se voltam contra as próprias pessoas que as leis pretendem proteger.

SMS (Short Message Service) é um serviço disponível em telefones celulares digitais que permite o envio de mensagens curtas, de até 160 caracteres, conhecidas popularmente como mensagens de texto. (Wikipedia)

Spamming é a distribuição não solicitada de e-mails em massa, que transmitem convites para participar em esquemas para se ganhar dinheiro, adquirir/obter produtos e serviços etc. Atualmente, mensagens indesejadas de promoção ou propaganda, transmitidas via celulares também são compreendidas como *spams*. Argumenta-se que o termo *spam* deriva do esquete *Spam Song*, do grupo Monty Python, no qual *Spam* (fiambre enlatado da Hormel Foods: *sp*(*iced h*)*am*) domina o cardápio do café e é cantado repetidamente por um grupo de vikings (Colli 2009: 55, Wall 2007: 133).

Spyware é um software que secretamente vigia os arquivos de computador de um usuário para obter (mediante o registro dos toques no teclado da vítima ou pela busca por informações financeiras arquivadas no disco rígido) e retornar ao infectante informações pessoais sobre o usuário.

Tecnologia da informação "abrange todas as tecnologias que são utilizadas para digitalizar informação (entrada), armazená-la (memória), processá-la automaticamente, transportá-la e a colocar à disposição de um usuário final, seja humano ou máquina (saída)" (Lévy 2000: 15).

Torrent (*BitTorrent*) é um protocolo de comunicações de compartilhamento *peer-to-peer* de arquivos, utilizado para distribuir dados e arquivos eletrônicos na internet.

Trashing (ou *dumpster diving*) é a prática de procurar em sacos de lixo informações pessoais e documentos descartados para fraudes mediante personificação.

Trojan horse é "um programa que parece executar uma função benigna ou útil, mas, em verdade, possui alguns potenciais destrutivos ocultos que só se tornam aparentes depois que o usuário baixou e instalou o software" (Yar 2013: 31).

Tumblr é uma plataforma que permite aos usuários publicarem e compartilharem textos, imagens, vídeos, links, citações, áudios; o Tumblr está em uma categoria intermediária entre os blogs de formato convencional e o microblog Twitter.

Twitter é um serviço de rede social online que permite que usuários enviem e leiam mensagens curtas, de até 140 caracteres, chamadas *tweets*.

URL (*Uniform Resource Locator*), traduzido como *localizador padrão de recursos*, é "outra designação para um endereço de internet que pode ser lido por seres humanos" (Assange 2015: 133), como, por exemplo: www.ayresfranca.com.

Vírus é um software malicioso que se instala sem consentimento do usuário. Quando executado (ativado por ação humana), ele se autorreplica, copiando seu próprio código fonte ou infectando (e modificando) outros programas de computador.

Worms [vermes] são "fragmentos independentes de software capazes de autorreplicação e autotransmissão" (Yar 2013: 31). Diferente dos vírus, *worms* têm a capacidade de se autorreplicarem alastrarem sem qualquer ação humana.

YouTube é um site que permite que seus usuários carreguem e compartilhem vídeos em formato digital.

ANEXO II

LISTA DE VOCÁBULOS COM O MORFEMA *CYBER* DICIONARIZADOS[590]

cyber affair/cyber-romance: relacionamento romântico no qual todo contato acontece via internet.

cyber age: era marcada pelo desenvolvimento e pelo uso difundido da realidade virtual ou da internet.

cyberart: arte produzida através da tecnologia da computação.

ciberataque (*cyber-attack*): uso da tecnologia de informação para infiltrar ou romper sistemas de computadores.

ciberativismo (*cyberactivism*): ativismo desenvolvido ou exercido num espaço virtual ou por meio de rede internacional de computadores como militância política ou social.

ciberativista (*cyberactivist*): referente a ou relacionado com o ciberativismo.

cyberbabe: imagem ou personagem feminina atraente criada através de tecnologia da computação, ou uma hábil usuária feminina da tecnologia da computação.

cyber-bully: usuário experiente de computadores que intimida usuários novos, ou pessoa que empreende *cyber-bullying*.

cyber-bullying: uso da tecnologia de informação para cometer *bullying*, através de envio ou postagem e texto ou imagem de natureza intimidadora ou ameaçadora.

cibercafé (*cybercafe*): estabelecimento comercial onde clientes podem utilizar computadores com acesso à internet.

cybercash: fundos utilizados em transações financeiras eletrônicas, especialmente na internet, ou armazenados em *smart cards*.

cybercast/cybercasting: originalmente, publicação na internet de boletim de informações composto por texto eletrônico; atualmente, transmissão (*broadcast*) de programa ou evento na internet, geralmente ao vivo.

cyberchondriac: indivíduo que se preocupa irracionalmente sobre a condição de seu computador, ou indivíduo que busca obsessivamente informação sobre saúde na internet, geralmente para encontrar sintomas (reais ou imaginários) particulares que coincidam com alguma doença.

---

[590] Foram utilizados: *Cambridge advanced learner's dictionary*. Cambridge: Cambridge University Press, 2005; HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da Língua Portuguesa*, *op. cit.*; *Oxford advanced learner's dictionary of current English*. 7. ed. Oxford: Oxford University Press, 2005. Apesar de constar em todos os dicionários mais atualizados, o *cybercrime* (*crime ciber*) não é referido e definido neste rol para não criar conflito com conceituação apresentada neste trabalho.

cybercommunity: grupo de pessoas que interagem via rede de computador, em especial por meio da internet, em razão de um interesse comum.

cybercop: no âmbito da ficção científica, o agente policial ciberneticamente construído ou construído; o agente policial que lida com *cybercrime*.

cybercriminal/cybercrook: pessoa que comete o *cybercrime*.

cybercultural: referente à *cyberculture*.

cyberculture: mudanças sociais trazidas pelas disseminadas automação e computadorização; em acepção mais recente, a cultura que envolve computadores e internet.

cyberfeminism: movimento feminista voltado a enfrentar a perceptível dominância dos homens no uso e no desenvolvimento da tecnologia da informação.

cyberfraud: uso da internet pra obtenção de bens e valores de forma ilícita através de ilusão de outrem.

cybergeek: gíria que caracteriza o indivíduo que é extremamente bem informado sobre ou obsessivamente interessado na tecnologia da computação, usualmente considerado como sem outros interesses ou conhecimentos, pouco sociáveis etc.

cyberjournalist: jornalista cujo trabalho é principalmente publicado online.

cyber kid: no contexto da ficção científica, criança criada ou educada por robô ou computador; no sentido mais usual, jovem que é usuário habitual ou especialista de computadores.

cyberland: mundo imaginário controlado por máquinas ou computadores, ou ambiente gerado por computador (realidade virtual).

cyberlaw: legislação ou lei referente a infrações vinculadas a computadores e internet.

cyberlibertarian: pessoa que se opõe à regulamentação governamental da internet.

cyberlife: parte da vida de um indivíduo que é gasta em ambiente de realidade virtual ou na internet.

cybermall: *website* comercial por meio do qual uma variedade de produtos podem ser adquiridos.

Cyberman: com letra inicial maiúscula, refere-se a um tipo de *cyborg* apresentado na série televisiva britânica de ficção científica *Doctor Who*; por extensão, qualquer *cyborg* ou robô humanoide.

cybernate: controlar, especialmente, no processo industrial, por meio de máquinas ou computadores; introduzir a automação ou a *cybernation*.

cybernation: controle automatizado de processo ou operação através de computadores.

cibernauta (*cybernaut*): usuário de um espaço virtual ou de uma rede de telemática, ou aquele que utiliza instrumentos especiais para experimentar a realidade virtual; atualmente, referido como *netizen*.

cibernética (*cybernetics*): ciência que tem por objeto o estudo comparativo dos sistemas e mecanismos de controle automático, regulação e comunicação nos seres vivos e nas máquinas.

cibernética (*cybernetic*): adjetivo de cibernética.

cyberpet: brinquedo eletrônico que se comporta tal qual um animal de estimação, como o Tamagotchi™.

cyberphobe: indivíduo que sofre de *cyberphobia*.

cyberphobia: medo de ou aversão irracional a computadores, ou, mais genericamente, medo e/ou inabilidade em aprender sobre novas tecnologias.

ciberpirata: pessoa com conhecimentos não necessariamente profundos de informática que eventualmente os utiliza para violar sistemas ou exercer outras atividades ilegais; pirata eletrônico.

ciberpirataria: violação de sistemas e ações ilegais no meio da tecnologia da informação.

cyberporn/cybersmut: ponografia acessada por computador, especialmente via internet.

cyberpunk: histórias ambientadas num imaginário mundo controlado pela tecnologia e por computadores.

cyber school: instituição de ensino que promove educação via internet, ao invés de em tradicional espaço escolar.

cibersegurança (*cybersecurity*): conjunto de medidas de precaução contra a violação de sistemas e outras atividades ilegais de piratas eletrônicos.

cybersex: comunicação entre pessoas, através da internet, que as deixa sexualmente excitadas.[591]

ciberespacial (*cyberspatial*): referente ou pertencente ao *cyberspace*.

[591] Lévy (2001: 185) critica a indevida apropriação da palavra, em especial por jornalistas que abordam o tema e por célebres intelectuais que escrevem "páginas e páginas de prosa rebuscada", quando, em realidade, o *cybersex* não se constitui numa prática comum: "'*Cybersex*' é comumente definido como uma relação sexual que acontece remotamente através de uma rede por meio de um traje de realidade virtual que compreende óculos estereoscópicos, sensores de movimento e sondas nas zonas erógenas. É uma forma de telemasturbação mútua, envolvendo um *hardware* que se assemelha vagamente a uma roupa S/M. Todavia, com a exceção de algumas demonstrações durante exposições de tecnologia especializada ou instalações artísticas – as quais geralmente envolvem equipamentos muito caros e são sempre públicas –, *ninguém* está praticando *cybersex*."

ciberespaço (*cyberspace*): espaço das comunicações por redes de computação ou o espaço imaginário onde informação eletrônica existe enquanto é transmitida entre computadores.

cyberspeak: jargão referente a computadores ou à internet.

cybersphere: esfera da tecnologia da informação.

cybersquat: prática de *cybersquatting*.

cybersquatter: aquele que pratica *cybersquatting*.

cybersquatting: atividade ilegal de adquirir e registrar oficialmente um domínio da internet que está no nome de uma empresa existente ou de uma pessoa conhecida, com a intenção de o vender ao seu "dono" como forma de alto lucro.

cyberstalker: indivíduo que pratica *cyberstalking*.

cyberstalking: uso da tecnologia da informação para molestar outrem por envio ou postagem de texto ou imagem de natureza obsessiva, intimidadora ou ofensiva.

cyberstore: *cybershop*.

cybersurf : uso ou busca na internet ou em outra rede de computadores.

cybersurfer: pessoa que habitualmente usa ou navega a internet.

cybersurfing: ação ou prática de usar ou navegar a internet.

ciberterrorismo (*cyberterrorism*): uso da tecnologia da informação para causar dano, rompimento, terror e/ou prejuízo financeiro, geralmente com motivações políticas.

ciberterrorista (*cyberterrorist*): perpetrador ou participante do *cyberterrorism*.

cyber-thriller: romance ou filme do gênero de suspense cujo enredo envolve *cybercrime* ou tecnologia futurista.

cyberwar/cyberwarfare: infiltração ou rompimento de computadores ou outros sistemas da tecnologia da informação com objetivos militares ou estratégicos.

cyberworld: ambiente gerado por computador, realidade virtual, *cyberspace*.

REFERÊNCIAS BIBLIOGRÁFICAS

ADDAMS, Jane (ed.). *Hull-House maps and papers*: a presentation of nationalities and wages in a congested district of Chicago, together with comments and essays on problems growing out of the social conditions. New York: Thomas Y. Crowell & Co., 1895.

AGAMBEN, Giorgio. "O que é um dispositivo?", *outra travessia*, n. 5, 2005. p. 9-16.

ALBUQUERQUE, Roberto Chacon. *Criminalidade informática*. São Paulo: Juarez de Oliveira, 2006.

ASSANGE, Julian. *Quando o Google encontrou o Wikileaks*. trad. Cristina Yamagami. São Paulo: Boitempo, 2015.

ASSANGE, Julian *et al. Cypherpunks*: freedom and the future of the internet. New York, London: OR Books, 2012.

BERNER, Sam. "Cyber-Terrorism: Reality or Paranoia?", *South African Journal of Information Management*, v. 5, n. 1, 2003.

BRENNER, Susan W. "Is There Such a Thing as 'Virtual Crime'?" *California Criminal Law Review*, v. 4, i. 1, 2001.

BROWN, Sheila. "The criminology of hybrids: Rethinking crime and law in technosocial networks" *Theoretical Criminology*, v. 10, i. 2, 2006, p. 223-244.

BROWN, Sheila. "Virtual Criminology" In MCLAUGHLIN, Eugene; MUNCIE, John. *The SAGE dictionary of criminology*. 3. ed. London: SAGE, 2013. p. 486-488.

BURGESS, Ernest Watson. "The Growth of the City: An Introduction to a Research Project", In PARK, Robert Ezra; BURGESS, Ernest Watson; MCKENZIE, Roderick D. *The city*. Chicago: The University of Chicago Press, (1925) 1967. p. 47-62.

CALDEIRA, Teresa Pires do Rio. "Novas visibilidades e configurações do espaço público em São Paulo", *Novos Estudos – CEBRAP*, n. 94, 2012. p. 31-67.

CALDEIRA, Teresa Pires do Rio. "Qual a novidade dos rolezinhos?: Espaço público, desigualdade e mudança em São Paulo", *Novos Estudos – CEBRAP*, n. 98, 2014. p. 13-20.

Cambridge advanced learner's dictionary. Cambridge: Cambridge University Press, 2005

CAPELLER, Wanda. "Not Such a Neat Net: Some Comments on Virtual Criminality", trad. Serena Barkham-Huxley, *Social & Legal Studies*, v. 10, n. 2, 2001, p. 229-242.

CASTELLS, Manuel. *Networks of outrage and hope*: social movements in the internet age. Cambridge: Polity, 2014.

CHATTERJEE, Bela Bonita. "'This is not Kate Moss': an exploration into the viewing of cyberpornography", *Proceedings of the 14th annual BILETA conference*, College of Ripon & York St. John, York (England), 1999.

COLEMAN, Biella. "Hacker Politics and Publics", *Public Culture*, n. 23, v. 3, 2011.

COLEMAN, Biella. "Our Weirdness is Free: The logic of Anonymous – online army, agent of chaos, and seeker of justice." *Triple Canopy*, n. 15. jan. 2012.

COLEMAN, Biella; RALPH, Michael. "Is it a crime? The Transgressive Politics of Hacking in Anonymous." *Social Text*, 28 set 2011.

COLLI, Maciel. *Cibercrimes*: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009. 172 f. Dissertação (Mestrado em Ciências Criminais) – Programa de Pós-Graduação em Ciências Criminais, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2009.

COLLIN, Barry C. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", *Proceedings of 11th Annual International Symposium on Criminal Justice Issues*. The University of Illinois at Chicago, 1996.

COOLEY, Charles Horton. *Social organization*: a study of the larger mind. New York: Charles Scribner's Sons, 1910.

COPES, Heith. "Societal attachments, offending frequency, and techniques of neutralization", *Deviant Behavior: An Interdisciplinary Journal*, v. 24, n. 2, 2003, p. 101-127.

CRARY, Jonathan. *24/7*: capitalismo tardio e os fins do sono. trad. Joaquim Toledo Jr. 2. ed. São Paulo: Cosac Naify, 2015.

DALLA VIGNA, Pierre. "Guerra local e guerra total" In PERNIOLA, Mario; FORMENTI, Carlo; DALLA VIGNA, Pierre; VILLANI, Tiziana; GUATTARI, Felix; BAUDRILLARD, Jean. *Guerra virtual e guerra real*: reflexão sobre o conflito do Golfo. Lisboa: Vega/Passagens, 1991. p. 49-77.

DANT, Tim. "The Driver-car", *Theory, Culture & Society*, v. 21, n. 4/5, 2004, p. 61-79.

DAWKINS, Richard. *O gene egoísta*. trad. Rejane Rubino. São Paulo: Companhia das Letras, 2007.

DISHMAN, C. "The Leaderless Nexus: When Crime and Terror Converge", *Studies in Conflict & Terrorism*, n. 28, 2005. p. 237-252.

FERRELL, Jeff; HAYWARD, Keith. "Criminologia Cultural Continuada" In CARLEN, Pat; FRANÇA, Leandro Ayres. *Criminologias alternativas*. Porto Alegre: Canal Ciências Criminais, 2017. p. 35-54.

FOOTMAN, Tim. *Radiohead – welcome to the machine*: OK Computer and the death of the classic album. New Malden: Chrome Dreams, 2007.

FREIBURGER, Tina; CRANE, Jeffrey S. "A Systematic Examination of Terrorist Use of the Internet", *International Journal of Cyber Criminology*, v. 2, i. 1, 2008, p. 309-319.

GARCÍA MÁRQUEZ, Gabriel. *Cem anos de solidão*. trad. Eliane Zagury. 58. ed. Rio de Janeiro: Record, [1967] 2005.

GARCÍA-PABLOS DE MOLINA, Antonio. *Criminologia*: introdução a seus fundamentos teóricos; introdução às bases criminológicas da Lei 9.099/95, Lei dos Juizados Especiais Criminais. trad. Luiz Flávio Gomes e Davi Tangerino. 5. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2006.

GARLAND, David. *The culture of control*. Chicago: University of Chicago Press, 2002.

GARLAND, David; SPARKS, Richard. "Criminology, Social Theory and the Challenge of our Times", *The British Journal of Criminology*, v. 40, n. 2, 2000, p. 189-204.

GEIST, Michael. "Cyberlaw 2.0", *Boston College Law Review*, n. 323, 2003, p. 326-327.

GIACOIA JUNIOR, Oswaldo. *Heidegger urgente*: introdução a um novo pensar. São Paulo: Três Estrelas, 2013.

GIBSON, William. "Burning Chrome", *Omni*, jul 1982, p. 72-77, 102-107.

GIBSON, William. *Neuromancer*. trad. Fábio Fernandes. 4. ed. São Paulo: Aleph, [1984] 2008.

GRABOSKY, Peter N. "Virtual Criminality: Old Wine in new Bottles?", *Social & Legal Studies*, v. 10, n. 2, 2001, p. 243-249.

GRAHAM, Hannah; McNeill. "Desistência: Prevendo Futuros" In CARLEN, Pat; FRANÇA, Leandro Ayres. *Criminologias alternativas*. Porto Alegre: Canal Ciências Criminais, 2017. p. 573-593.

HALUPKA, Max. *The evolution of Anonymous as a political actor*. 2011. Monografia de Bachelor of Arts – Honours Program in Political Studies, School of Social and Policy Studies, School of Social and Policy Studies, The Flinders University of South Australia, Camberra.

HAMM, Mark S. "Apocalyptic violence: The seduction of terrorist subcultures", *Theoretical Criminology*, v. 8, n. 3, 2004. p. 323-39.

HARVEY, David. *Condição pós-moderna*: uma pesquisa sobre as origens da mudança cultural. trad. Adail Ubirajara Sobral e Maria Stela Gonçalves. 25. ed. São Paulo: Edições Loyola, 2014.

HAYWARD, Keith. "Five Spaces of Cultural Criminology", *The British Journal of Criminology*, v. 52, n. 3, 2012, p. 441-462.

HAYWARD, Keith J.; YOUNG, Jock. "Cultural Criminology: Some notes on the script", *Theoretical Criminology*, v. 8, n. 3, 2004. p. 259-73.

HEIDEGGER, Martin. *Carta sobre el Humanismo*. trad. Helena Cortés e Arturo Leyte. Madrid: Alianza Editorial, 2000. ["Brief über den Humanismus", *in Wegmarken*. Frankfurt am Main: Vittorio Klostermann GmbH, [1946] 1976.]

HEIDEGGER, Martin. *Discourse on thinking*. trad. John M. Anderson e E. Hans Freund. New York: Harper & Row, 1966. ["Gelassenheit", *in Reden und andere Zeugnisse eines Lebensweges*. Frankfurt am Main: Vittorio Klostermann GmbH, 1959.]

HEIDEGGER, Martin. *Parmenides*. trad. André Schuwer e Richard Rojcewicz. Bloomington: Indiana University Press, 1998. p. 71-87. ["Parmenides" [Freiburg: 1942-1943], *in Vorträge und Aufsätze*. Frankfurt am Main: Vittorio Klostermann GmbH, 1982.]

HEIDEGGER, Martin. "The Origin of the Work of Art", *in* YOUNG, Julian; HAYNES, Kenneth (eds.). *Off the beaten track*. trad. Julian Young e Kenneth Haynes. Cambridge: Cambridge University Press: 2002. ["Der Ursprung des Kunstwerkes", *in Holzwege*. Frankfurt am Main: Vittorio Klostermann GmbH, 1950.]

HEIDEGGER, Martin. *The question concerning technology, and other essays*. trad. William Lovitt. New York/London: Garland Publishing/Harper & Row Publishers: 1977. ["Die Frage nach der Technik", *in Vorträge und Aufsätze*. Frankfurt am Main: Vittorio Klostermann GmbH, 1953.]

HOLLINGER, Richard Clifton. "Computer Crime" In LUCKENBILL, David; PECK, Denis (eds.). *Encyclopedia of crime and juvenile delinquency (vol. II)*. Philadelphia: Taylor and Francis, 2001. p. 76-81.

HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da Língua Portuguesa*. Rio de Janeiro: Objetiva, 2001.

HOWARD, Philip N.; HUSSAIN, Muzammil M. *Democracy's fourth wave?*: information technology and the fuzzy causes of the Arab Spring. In: Meeting of the International Studies Association, 2012, San Diego. Artigo.

HUTCHINGS, Alice; CHUA, Yi Ting. "Gendering cybercrime", In HOLT, Thomas J. (ed.). *Cybercrime through an interdisciplinary lens*. London: Routledge, 2017. p. 167-188.

JAISHANKAR, K. "Cyber Criminology: Evolving a novel discipline with a new journal", *International Journal of Cyber Criminology*, v. 1, n. 1, 2007, p. 1-6.

JAISHANKAR, K. “Establishing a Theory of Cyber Crimes”, *International Journal of Cyber Criminology*, v. 1, n. 2, 2007, p. 7-9.

JAISHANKAR, K. “The Future of Cyber Criminology: Challenges and Opportunities”, *International Journal of Cyber Criminology*, v. 4, n. 1&2, 2010, p. 26-31.

JOHNSON, Steven. *How we got to now*: six innovations that made the modern world. New York: Riverhead Books, 2014.

JOHNSTON, Les. “What is vigilantism?”, *British Journal of Criminology*, v. 36, n. 2, 1996. p. 220-236.

KERCKHOVE, Derrick de. *A pele da cultura*: uma investigação sobre a nova realidade eletrónica. trad. Luís Soares e Catarina Carvalho. Lisboa: Relógio D’Água Editores, 1997.

KHATCHADOURIAN, Raffi. “No secrets: Julian Assange’s mission for total transparency”, *The New Yorker*, 7 jun 2010.

LATOUR, Bruno. *Pandora’s hope*: essays on the reality of science studies. Cambridge: Harvard University Press, 2000.

LESSIG, Lawrence. *Code*: version 2.0. New York: Basic Book, 2006.

LESSIG, Lawrence. *The laws of cyberspace*: draft 3. In: Taiwan Net ’98, 1998, Taipei. Artigo.

LÉVY, Pierre. *A conexão planetária*: o mercado, o ciberespaço, a consciência. trad. Maria Lúcia Homem e Ronaldo Entler. São Paulo: Ed. 34, 2001.

LÉVY, Pierre. *Cyberculture*. trad. Robert Bononno. Minneapolis: University of Minnesota Press, 2001.

LYOTARD, Jean-François. *O inumano*: considerações sobre o tempo. 2. ed. Lisboa: Editorial Estampa, 1997.

MCKENZIE, Roderick D. “The Ecological Approach to the Study of the Human Community”, *American Journal of Sociology*, v. 30, n. 3, 1924, p. 287-301.

MERTON, Robert K. “A profecia que se cumpre por si mesma”. In Idem. *Sociologia*: teoria e estrutura. trad. Miguel Maillet. São Paulo: Mestre Jou, 1968. p. 515-531.

MERTON, Robert K. “Continuidades na Teoria da Estrutura Social e da Anomia” In *Idem*. *Sociologia*: teoria e estrutura. São Paulo: Mestre Jou, 1970. p. 235-270.

MOORE, Robert; MCMULLAN, Elizabeth C. “Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students”, *International Journal of Cyber Criminology*, v. 3, n. 1, jan-jun 2009, p. 441-451.

MOREIRA DE OLIVEIRA, Felipe Cardoso. *Criminalidade informática*. 2002. 160 f. Dissertação (Mestrado em Ciências Criminais) – Programa de Pós-Graduação em Ciências Criminais, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2002.

MYTHEN, Gabe. "Criminologia e Terrorismo: rumo a uma abordagem crítica" In CARLEN, Pat; FRANÇA, Leandro Ayres. *Criminologias alternativas*. Porto Alegre: Canal de Ciências Criminais, 2017. p. 365-380.

NEWMAN, Oscar. *Architectural design for crime prevention*. Washington: U.S. Government Printing Office, U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, 1973.

NEWMAN, Oscar. *Creating Defensible Space*. Washington: U.S. Department of Housing and Urban Development, Office of Policy Development and Research, 1996.

NEWMAN, Oscar. "Defensible Space: A New Physical Planning Tool for Urban Revitalization", *Journal of the American Planning Association*, v. 61, i. 2, 1995, p. 149-155.

NEWMAN, Oscar. FRANCK, Karen A. "The Effects of Building Size on Personal Crime and Fear of Crime", *Population and Environment*, v. 5, i. 4, 1982, p. 203-220.

NOGUEIRA, Bruno Torturra. "#SeJoga: Trip investiga o ativismo 3.0: o que há de novo na cabeça de quem sonha em mudar o mundo?". *Trip*. São Paulo, n. 220, p. 60-75, abr 2013.

OBERHOLZER, Felix; STRUMPF, Koleman. *The effect of file sharing on record sales*: an empirical analysis. 2005. Disponível em <http://www.unc.edu/~cigar/papers/FileSharing_June2005_final.pdf>.

O'BRIEN, Martin. "What is *cultural* about cultural criminology?", *The British Journal of Criminology*, v. 45, n. 5, 2005. p. 599-612.

OED Online. Oxford: Oxford University Press, 2014.

OLSON, Parmy. *We are Anonymous*: inside the hacker world of LulzSec, Anonymous, and the Global Cyber Insurgency. New York: Little, Brown and Company, 2012.

Oxford advanced learner's dictionary of current English. 7. ed. Oxford: Oxford University Press, 2005.

PARK, Robert Ezra. "The City: Suggestions for the Investigation of Human Behavior in the City Environment", *American Journal of Sociology*, v. 20, n. 5, 1915, p. 577-612.

PATTISON, George. *Routledge philosophy guidebook to the later Heidegger*. London/New York: Routledge, 2000.

PÉREZ SUÁREZ, Jorge Ramiro. *We are cyborgs*: developing a theoretical model for understanding criminal behaviour on the internet. 2015. 333 f. Tese (Doutorado em Filosofia) – The University of Huddersfield, Huddersfield, 2015.

PFOHL, Stephen. "O delírio cibernético de Norbert Wiener", *Revista FAMECOS*, n. 15, ago 2001, p. 105-121.

PLANT, Sadie. "On the matrix: cyberfeminist simulations" In BELL, David; KENNEDY, Barbara M. *The cybercultures reader*. London, New York: Routledge, 2000. p. 325-336.

RÜDIGER, Francisco. *Martin Heidegger e a questão da técnica*: prospectos acerca do futuro do homem. 2. ed. Porto Alegre: Sulina, 2014.

SAUER, Carl Ortwin. "The Morphology of Landscape", *University of California Publications in Geography*, v. 2, n. 2, 1925, p. 19-53.

SHAW, Clifford R.; MCKAY, Henry D. "Are Broken Homes a Causative Factor in Juvenile Delinquency?", *Social Forces*, v. 10, n. 4, 1932, p. 514-524.

SIEGEL, Larry J. *Criminology*: theories, patterns, and typologies. 10. ed. Belmont: Wadsworth, 2010.

SNYDER, Francis. "Sites of Criminality and Sites of Governance", *Social & Legal Studies*, v. 10, i. 2, 2001, p. 251-256.

SOUZA, Bernardo de Azevedo e. *Direito, tecnologia e práticas punitivas*. Porto Alegre: Canal Ciências Criminais, 2016.

SOUZA, Ricardo Timm de. *Totalidade & desagregação*: sobre as fronteiras do pensamento e suas alternativas. Porto Alegre: EDIPUCRS, 1996.

SUTHERLAND, Edwin Hardin. "Is 'White Collar Crime' Crime?", *American Sociological Review*, v. 10, n. 2, 1945, p. 132-139.

SUTHERLAND, Edwin Hardin. *White collar crime*: the uncut version: with an introduction by Gilbert Geis and Colin Goff. New Haven/London: Yale University Press, (1949) 2012.

SYKES, Gresham M.; MATZA, David. (1957) "Techniques of Neutralization: A Theory of Delinquency", *American Sociological Review*, v. 22, n. 6, p. 664-670.

SYKES, Gresham M.; MATZA, David. (1961) "Juvenile Delinquency and Subterranean Values", *American Sociological Review*, v. 26, n. 5, p. 712-719.

THOMAS, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, v. 23, i. 1, 2003, p. 112-123.

THRASHER, Frederic M. "A Community Study", *Religious Education*, v. 25, 1930, p. 398-400.

THRASHER, Frederic M. “Ecological Aspects of the Boys’ Club Study”, *Journal of Educational Sociology*, v. 6, n. 1, 1932, p. 52-58.

THRASHER, Frederic M. “Juvenile Delinquency and Crime Prevention”, *Journal of Educational Sociology*, v. 6, n. 8, 1933, p. 500-509.

THRASHER, Frederic M. “The Boy’s Club Study”, *Journal of Educational Sociology*, v. 6, n. 1, 1932, p. 4-16.

THRASHER, Frederic M. “The Study of the Total Situation”, *Journal of Educational Sociology*, v. 1, n. 10, 1928, p. 599-612.

TURING, Alan Mathison. “Computing Machinery and Intelligence”, *Mind*, v. LIX, n. 236, 1950, p. 433-460.

UNDERWOOD, P. C. *New directions in networked activism and online social movement mobilization*: the case of Anonymous and Project Chanology. 2009. Dissertação de Master of Arts – Department of Sociology and Anthropology, Ohio University, Ohio.

VEGH, Sandor. “Classifying Forms of Online Activism: The Case of Cyberprotests agains the World Bank”. In MCCAUGHEY, Martha; AYERS, Michael D. *Cyberactivism*: online activism in theory and practice. London: Routledge, 2003.

VERISSIMO, Erico. *Um lugar ao sol*. 36. ed. São Paulo: Companhia das Letras, 2006.

VIRILIO, Paul. *A arte do motor*. trad. Paulo Roberto Pires. São Paulo: Estação Liberdade, 1996.

VIRILIO, Paul. *A inércia polar*. trad. Ana Luía Faria. Lisboa: Publicações Dom Quixote, 1993.

VIRILIO, Paul. “Da política do pior ao melhor das utopias e à globalização do terror”, *FAMECOS*, n. 16, dez. 2001. p. 7-18.

WAITES, Rosie. “V for Vendetta masks: Who’s behind them?”, *BBC News Magazine*, London, 20 out 2011.

WALL, David S. *Cybercrime*: the transformation of crime in the information age. Cambridge: Polity, 2007.

WEIMANN, Gabriel. *Cyberterrorism*: how real is the threat? Washington: United States Institute of Peace, 2004.

WEIMANN, Gabriel. *www.terror.net*: how modern terrorism uses the internet. Washington: United States Institute of Peace, 2004.

WIENER, Norbert. *Cybernetics, or control and communication in the animal and the machine*. Cambridge: MIT Press, 1948.

WILSON, James Q.; KELLING, George L. “Broken Windows: The police and neighborhood safety”, *The Atlantic*, mar 1982.

WINNER, Langdon. “Do Artifacts Have Politics”, *Daedalus*, v. 109, n. 1, Modern Technology: Problem or Opportunity?, 1980, p. 121-136.

WINNER, Langdon. *The whale and the reactor*: a search for limits in an age of high technology. Chicago: The University of Chicago Press, 1986.

WIRTH, Louis. “Urbanism as a Way of Life”, *American Journal of Sociology*, v. 44, n. 1, 1938, p. 1-24.

YAR, Majid. *Cybercrime and society*. 2. ed. London: SAGE, 2013.

YAR, Majid. “Online Crime”, *Oxford Research Encyclopedia of Criminology*, 2016.

YAR, Majid. “The Novelty of ‘Cybercrime’: As Assessment in Light of Routine Activity Theory”, *European Journal of Criminology*, v. 2, i. 4, 2005, p. 407-427.

ZEDNER, Lucia. “Pre-crime and post-criminology?”, *Theoretical Criminology*, v. 11, i. 2, 2007, p. 261-281.

ŽIŽEK, Slavoj. *Violência*: seis reflexões laterais. trad. Miguel Serras Pereira. São Paulo: Boitempo, 2014.

Pontifícia Universidade Católica do Rio Grande do Sul
Pró-Reitoria Acadêmica
Av. Ipiranga, 6681 - Prédio 1 - 3º. andar
Porto Alegre - RS - Brasil
Fone: (51) 3320-3500 - Fax: (51) 3339-1564
E-mail: proacad@pucrs.br
Site: www.pucrs.br/proacad