UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

ISABELLE SILVA MARQUES

A TEORIA DA ANOMIA NO PENSAMENTO DE DURKHEIM E MERTON E OS CRIMES CIBERNÉTICOS NO BRASIL

FORTALEZA
2023

ISABELLE SILVA MARQUES

A TEORIA DA ANOMIA NO PENSAMENTO DE DURKHEIM E MERTON E OS CRIMES CIBERNÉTICOS NO BRASIL

Trabalho de Conclusão de Curso apresentado à disciplina de Monografia Jurídica do Curso de Direito da Universidade Federal do Ceará (UFC), como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Samuel Miranda Arruda.

FORTALEZA

2023

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

M317t Marques, Isabelle Silva.
A teoria da anomia no pensamento de Durkheim e Merton e os crimes cibernéticos no Brasil / Isabelle Silva Marques. – 2023.
66 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2023.
Orientação: Prof. Dr. Samuel Miranda Arruda.

1. Anomia. 2. Crimes cibernéticos. 3. Durkheim. 4. Merton. I. Título.

CDD 340

ISABELLE SILVA MARQUES

A TEORIA DA ANOMIA NO PENSAMENTO DE DURKHEIM E MERTON E OS CRIMES CIBERNÉTICOS NO BRASIL

Trabalho de Conclusão de Curso apresentado à disciplina de Monografia Jurídica do Curso de Direito da Universidade Federal (UFC), como requisito parcial à obtenção do grau de Bacharel em Direito.

Aprovada em 12/07/2023.

BANCA EXAMINADORA

_____

Prof. Dr. Samuel Miranda Arruda (Orientador)

Universidade Federal do Ceará (UFC)

_____

Prof. Ma. Vanessa de Lima Marques Santiago Sousa

Universidade Federal do Ceará (UFC)

_____

Mariana Rodrigues Aragão

Universidade Federal do Ceará (UFC)

A Deus.

AGRADECIMENTOS

A Deus, primeiramente, por ter me dado o vigor necessário para vencer as adversidades.

À esta universidade, seu corpo docente e administrativo, pelos anos de disponibilização e dedicação.

Ao meu orientador, pelo apoio no pouco tempo que foi possível.

Aos meus pais, pelo suporte durante todo o tempo dos meus estudos.

À minha querida amiga, Beatriz Tavares, pelo apoio emocional.

"*Who can tell what magic spells we'll be doing for us?*" (KAY;SMITH, 1996).

RESUMO

Este trabalho foi escrito com o objetivo principal de examinar as interligações entre as teorias da anomia, elaboradas por Émile Durkheim e Robert King Merton, ao contexto dos crimes informáticos no Brasil. Para tanto, a metodologia adotada consistiu em uma pesquisa qualitativa com fundamento nas obras dos dois autores, e em uma pesquisa bibliográfica em livros, artigos, periódicos científicos, sítios virtuais, legislações e documentos sobre a temática. Os resultados revelaram que as teorias são aplicáveis ao cenário da delinquência cibernética no país, explicando parte da origem do comportamento criminoso digital, mas que, em relação ao ordenamento jurídico brasileiro, existem novos tipos penais e normas que buscam regular a recente realidade trazida pelas tecnologias da informação e comunicação, mesmo que ainda de uma forma incompleta. Diante disso, se chegou à conclusão de que súbitas, intensas e positivas mudanças na ordem coletiva, assim como as identificadas a partir da terceira revolução industrial, provocaram um estado de anomia que aumenta os crimes virtuais, e que as ênfases culturais que ocorrem digitalmente reforçam a tensão advinda das desproporções existentes na estrutura social brasileira.

Palavras-chaves: anomia; crimes cibernéticos; Émile Durkheim; Robert King Merton.

RESUMEN

Este trabajo se redactó con el objetivo principal de examinar las interconexiones entre las teorías de la anomia elaboradas por Émile Durkheim y Robert King Merton en el contexto de los delitos informáticos en Brasil. Por lo tanto, la metodología adoptada consistió en una investigación cualitativa basada en los trabajos de ambos autores, así como una investigación bibliográfica en libros, artículos, revistas científicas, sitios web, legislación y documentos relacionados con el tema. Los resultados revelaron que las teorías son aplicables al escenario del delito cibernético en el país, explicando parte del origen del comportamiento delictivo digital. Sin embargo, en relación con el ordenamiento jurídico brasileño, se observa la existencia de nuevos tipos penales y normas que buscan regular la realidad reciente que traen consigo las tecnologías de la información y la comunicación, aunque todavía de manera incompleta. En conclusión, se determinó que los cambios repentinos, intensos y positivos en el orden colectivo, así como los identificados a partir de la tercera revolución industrial, han provocado un estado de anomia que ha incrementado los delitos virtuales. Además, los énfasis culturales que se dan en el ámbito digital refuerzan la tensión derivada de las desproporciones existentes en la estructura social brasileña.

Palabras clave: anomia; delitos cibernéticos; Émile Durkheim; Robert King Merton.

LISTA DE ABREVIATURAS E SIGLAS

ARPA	Agência de Projetos de Pesquisa Avançada
ART	Artigo
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CDPC	Comitê Europeu para Problemas Criminais
CP	Código Penal
CSIRT	Grupos de Segurança e Resposta a Incidentes
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
FERMILAB	*Fermi National Accelerator Laboratory*
LGPD	Lei Geral de Proteção de Dados
MLAT	*Mutual Legal Assistance Treaty*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
OCDE	Organização para Cooperação e Desenvolvimento Econômico
OCX	Organização para Cooperação de Xangai
ONU	Organização das Nações Unidas
PL	Projeto de Lei
RNP	Rede Nacional de Pesquisa
STF	Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO 10

2 NOÇÕES FUNDAMENTAIS SOBRE CRIMES INFORMÁTICOS 12

2.1 Nomenclatura 12

2.2 Conceito e classificação 15

3 LEGISLAÇÃO BRASILEIRA EM MATÉRIA DE CRIMES INFORMÁTICOS E NORMAS EM ÂMBITO INTERNACIONAL 21

3.1 A Lei n° 12.735/12 e a Lei n° 12.737/12 21

3.2 A Lei n° 14.155/21 26

3.3 A Convenção de Budapeste e a adesão do Brasil ao tratado 28

3.4 A Convenção sobre Crimes Cibernéticos da ONU 33

4 A TEORIA DA ANOMIA NO PENSAMENTO DE DURKHEIM E MERTON 35

4.1 Solidariedade, divisão do trabalho e anomia 36

4.2 Suicídio anômico, perturbações da ordem coletiva e forma anormal do crime 39

4.3 Ênfase cultural e tipos de adaptações individuais 43

5 INTERLIGAÇÕES ENTRE A TEORIA DA ANOMIA E O CONTEXTO DOS CRIMES INFORMÁTICOS NO BRASIL 48

5.1 Revolução informacional e criminalidade informática 48

5.2 Adaptações individuais na realidade cibernética 53

6 CONCLUSÃO 58

REFERÊNCIAS 61

1 INTRODUÇÃO

Nos últimos anos, o Brasil tem testemunhado um aumento significativo nos casos de crimes cibernéticos. Golpes virtuais, invasões de sistemas, roubo de informações pessoais e financeiras, difamação e assédio online são apenas alguns exemplos das atividades criminosas que têm afetado tanto indivíduos quanto instituições no país. Diante desse panorama, surge a problemática central desta pesquisa: no âmbito cibernético, impera um grande estado de indisciplina que permite a amplificação da criminalidade? O uso de novas tecnologias permitiu a formação de uma terra sem leis digital no Brasil?

A pesquisa tem como objetivo analisar a relação entre a teoria da anomia desenvolvida por Durkheim e Merton e o contexto dos crimes cibernéticos no país. Pretende-se relacionar a hipótese da condição anômica ao cenário de surgimento das tecnologias da informação e da comunicação e suas características. Ainda, tem o objetivo de examinar formulações conceituais e classificatórias acerca dos crimes digitais e a recente legislação, em âmbito nacional e internacional, sobre o tema.

Para alcançar os objetivos propostos, o presente trabalho realiza uma pesquisa qualitativa, baseada no estudo da teoria da anomia em obras de Durkheim e Merton, bem como em uma pesquisa bibliográfica em livros, artigos, periódicos científicos, sítios virtuais, legislação brasileira e documentos sobre a teoria e a delinquência informática.

No segundo capítulo do trabalho, são examinadas algumas nomenclaturas existentes que denominam a criminalidade digital, dada a relevante quantidade de termos que são empregados para se referir aos atos ilícitos, e também são analisados conceitos e classificações desse tipo de delito, em virtude da percepção de que ainda não existe um consenso geral sobre as atividades cibernéticas que devem ser consideradas ilegais. No terceiro capítulo, por sua vez, é analisada a legislação nacional mais recente e relevante que trata de crimes informáticos e examinada a Convenção de Budapeste, sendo ainda apresentada a Convenção sobre Crimes Cibernéticos da Organização das Nações Unidas (ONU), que encontra-se em processo de elaboração e negociação do texto. No quarto capítulo, a teoria da anomia é investigada em duas das obras de Durkheim, em que ele trata da divisão do trabalho social e das causas sociais do suicídio, além disso é explorada a perspectiva posterior concebida por Merton em seus trabalhos. Por último, o quinto capítulo interliga a teoria

da anomia dos citados sociólogos ao contexto dos crimes virtuais, os conectando à realidade brasileira.

2 NOÇÕES FUNDAMENTAIS SOBRE CRIMES INFORMÁTICOS

A dificuldade de delimitação do crime perpetrado em ambiente cibernético é decorrente, dentre outros motivos, de uma variada gama de técnicas e novos conhecimentos empregados na sua execução, de múltiplos perfis de autores e vítimas, bem como de diferentes alvos e áreas que podem ser afetadas pelo delito, o qual agrega tanto condutas delituosas já bastante conhecidas pelo direito quanto condutas novas, permitidas por uma recente realidade tecnológica e social.

Essa característica polimórfica da criminalidade digital acaba por se refletir nas tentativas de sua conceituação da mesma maneira que influencia a classificação das condutas criminosas que engloba (MARTÍN, 2003). O resultado é a concepção de definições e classificações que tendem a serem muito amplas e que fomentam o desenvolvimento de distintas óticas de estudo, no que se inclui também a própria nomenclatura desse tipo de crimes. Diante disso, contudo, sobre o capítulo, importa dizer que não obstante essas três noções fundamentais possuam um conteúdo controverso, todas indispensavelmente giram em torno da reflexão sobre os bens que devem ser tutelados no contexto de uma sociedade digital.

2.1 Nomenclatura

Inicialmente, ao tratar da esfera terminológica, é relevante destacar que alguns nomes foram consolidados mais pela habitualidade do uso do que por uma análise aprofundada dos termos, ou mesmo por associações desacertadas e confusas, que fogem de um viés jurídico. A maioria das denominações referentes a delitos informáticos usam um vocabulário que faz alusão à novas tecnologias e possuem como base palavras estrangeiras, comumente de língua inglesa. Expressões como **crime eletrônico**, **crime digital**, **infocrime**, **crime perpetrado pela internet**, **crime virtual**, ***cybercrime***, ***computer-related crime***, ***cyberspace crime***, ***computing crime***, ***e-crime***, ***high-tech crime*** e uma abundante lista de termos são empregados evidenciando a ausência de um consenso sobre o assunto.

Apesar da existência dessas e tantas outras denominações, algumas são defendidas por se mostrarem mais apropriadas para a utilização como instituto do direito penal do que outras, à exemplo do termo **crime informático**:

> A ciência que tem como objeto de estudo as informações automatizadas (dados) é a Informática. Esta é a ciência que estuda os meios para armazenar, processar e transmitir dados, ou seja, para registrar, manipular e transmitir informações de forma automatizada. [...] Assim, está claro que a denominação mais precisa para os delitos ora em estudo é “crimes informáticos” ou “delitos informáticos”, por se basear no bem jurídico penalmente tutelado que é a inviolabilidade das informações automatizadas (dados). (VIANNA; MACHADO, 2013, p. 21).

A objetividade do termo delito informático também se dá porque ele não relaciona as condutas criminosas somente ao computador ou qualquer outra espécie de aparelho (como em *computer-related crime*), tampouco limita esse tipo de delinquência apenas à internet (à exemplo do nome *netcrime*), mas faz menção direta à informação automatizada, que é o fundamento através do qual os programas, os sistemas informáticos e as redes funcionam. Em raciocínio semelhante (entendendo a informação automatizada como parte da base de outros ramos), também não se julga equivocado o uso da expressão delitos informáticos no lugar de **delitos telemáticos**, apesar da criminalidade cibernética utilizar igualmente as telecomunicações em sua prática, posto que a telecomunicação depende da informática, sendo esta pressuposto daquela (CRESPO, 2011).

Por sua vez, a famosa denominação **crime cibernético**, que tem por base a palavra *cybercrime*, faz referência (com o prefixo *cyber*) à ciência cibernética, a qual trata, de forma interdisciplinar, da investigação ampla de modos de controle, comunicação e comportamento em sistemas de seres vivos, máquinas e elementos inanimados. Em razão disso, o uso dessa expressão sugere uma “amplitude que não se coaduna com o universo bem mais específico das condutas criminosas, as quais se relacionam com o bem jurídico a ser tutelado, que é bem mais restrito que toda uma ciência do controle.” (MOURA, 2021, p. 31). Portanto, resulta em uma indicação inexata.

Quanto ao termo **crime virtual**, segundo Vianna e Machado (2013, p. 20-21): “Vê-se, desde já, que a denominação [...] é completamente absurda, pois [...] não haveria qualquer sentido em se falar de um bem jurídico virtual.” Aqui a crítica reside na confusão que a palavra virtual gera, uma vez que seu significado é relacionado à ideia de uma realidade em potencial, uma simulação, ou mesmo algo inexistente, distinto do mundo real. No âmbito da informática, onde é muito recorrente, o termo é associado às estruturas e espaços formados através dos sistemas digitais. Já na esfera jurídica, contudo, a associação torna-se incoerente pois o bem jurídico que

deve ser protegido existe, bem como os crimes cometidos contra ele. Impossível escudar valores fictícios ou tratar de crimes irreais.

Por outro lado, diferente da noção de virtualidade, **crime digital** é uma nomenclatura que remete à um conceito técnico da ciência informática. O nome alude ao sistema binário, mais especificamente ao dígito binário, utilizado pelos computadores para traduzir um universo de imagens, sons, símbolos e significados:

> Os computadores representam a informação por meio de padrões de *bits*. Um *bit* (dígito binário) pode assumir os valores 0 e 1, os quais, por enquanto, consideraremos como meros símbolos, sem significado numérico. Na verdade, veremos que o significado de um *bit* varia de uma aplicação para outra. Algumas vezes, os padrões de *bits* são usados para representar valores numéricos e, em outras, para representar caracteres ou outros símbolos; também podem representar imagens ou sons. Armazenar um *bit* em um computador exige a presença de um dispositivo que possa assumir dois estados, como, por exemplo, um interruptor (ligado ou desligado), um relé (aberto ou fechado), ou um sinalizador de bandeira (erguida ou abaixada). Um dos estados representa 0 e o outro, 1 (BROOKSHEAR, 2008, p. 34).

Os *bits*, portanto, representam a informação na sua estrutura mais elementar e, por consequência, também constituem valores que se erguem com o avanço da tecnologia. Para Sydow (2015, p. 24-26), o surgimento de inovações elevou os *bits* a patamares dignos de proteção jurídica penal, dado que formam uma linguagem que é essencial para a sociedade:

> Novos conceitos passaram a existir com a tecnologia. Enquanto a maioria dos bens antigamente era representada por átomos, hoje boa parte deles é representada por *bits*. Os átomos formam a substância tangível, enquanto os *bits* compõem a linguagem (intangível) utilizada pela informática para compor os arquivos, programas e sinais de comunicação. [...] Bens compostos por *bits*, também, passam a existir e ser atingidos, graças às novas tecnologias. Segredos industriais, direitos autorais, dinheiro digital, bancos de dados, entre tantos outros valores, passam a existir na forma imaterial.

Diante do exposto, observa-se que dentre as variadas expressões utilizadas, os termos são mais pertinentes e juridicamente técnicos na medida em que se aproximam da elucidação do bem jurídico do qual dizem respeito, que é, neste caso, a informação automatizada (sua segurança, inviolabilidade, integridade...), traduzida por *bits* e expressa por aparelhos de tratamento de dados, como computadores, *tablets*, celulares, *smartphones*, *smartwatches*, óculos de realidade virtual e afins.

As denominações crime digital e crime informático, portanto, nos parecem mais precisas na indicação dos bens que devem ser tutelados pelo direito penal no

âmbito cibernético (contudo, ao longo da exposição desta pesquisa adverte-se que serão utilizados diferentes sinônimos para os crimes em questão).

2.2 Conceito e classificação

Para além da observação de novos bens erguidos pela tecnologia, é necessário perceber que valores tradicionalmente resguardados pelo direito também são atingidos por intermédio do espaço virtual, à exemplo do patrimônio, da honra e da dignidade sexual. Crimes como racismo, difamação, ameaça e todo tipo de delitos ocorrem no meio virtual ou através de ferramentas informáticas. Devido a isso, embora não exista unanimidade conceitual (tal qual a questão da nomenclatura), algumas definições de crimes cibernéticos já indicam uma diferenciação a respeito dos variados bens que podem ser atingidos pela tecnologia. Outras definições, porém, são vagas ou muito abrangentes.

Jesus e Milagre (2016), por exemplo, conceituam crime informático como o fato típico e antijurídico cometido mediante a informática em geral ou contra a tecnologia da informação, sendo esta um sistema, dispositivo informático ou rede de computadores. Em suma, na vertente da teoria bipartida do conceito analítico de crime, a delimitação dos autores discrimina a informática como sendo o bem lesionado ou como sendo o caminho para ofender outros bens.

De modo similar, a Convenção sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, celebrada em 2001, define crime digital como a "...ação dirigida contra a confidencialidade, integridade e disponibilidade de sistemas computacionais, redes e dados informáticos bem como o uso indevido de tais sistemas, redes e dados, providenciando a criminalização de tal conduta..." (COUNCIL OF EUROPE, 2001a, p. 1, tradução nossa). O conceito menciona três pilares da segurança informática, sendo estes a confidencialidade, atrelada ao sigilo das informações, a integridade, relacionada à completude dos dados, e a disponibilidade, ligada à acessibilidade ampla do conteúdo virtual para os usuários autorizados (SYDOW, 2015). Essas três qualidades da informação, que podem ser atingidas pelo ato criminoso, simultaneamente ou não, também são utilizadas para a prática de ofensas.

Por outro lado, de maneira bastante reduzida, a Organização para Cooperação de Xangai (OCX), em acordo de cooperação para garantir a segurança

da informação internacional entre os estados membros da organização, apenas considerou que “crime cibernético significa usar recursos da informação e/ou influenciá-los no espaço informacional para fins ilegais” (SHANGHAI COOPERATION ORGANIZATION, 2009, p. 9, tradução nossa). A definição se limita a distinguir o uso direito e indireto de mecanismos informáticos com objetivos ilegais, não especificando a hipótese de que possam ser atacados.

Já o Comitê Europeu para Problemas Criminais (CDPC), em atividades ocorridas entre 1985 e 1989 para estudar a questão dos crimes cibernéticos, optou por não desenvolver sua própria concepção, preferindo deixar aos vários Estados a tarefa de elaboração segundo seus respectivos sistemas legais e tradições históricas. Não obstante esse posicionamento, o comitê apontou o trabalho do grupo de especialistas da Organização para Cooperação e Desenvolvimento Econômico (OCDE), que estudou a temática e delimitou a seguinte definição em seu relatório (informe intitulado *Computer-related Crime: Analysis of Legal Politics*): “Considera-se abuso de computador qualquer comportamento ilícito, antiético ou sem autorização relacionado ao processamento automático e à transmissão de dados.” (1986 apud COUNCIL OF EUROPE, 1990, p. 13, tradução nossa).

O próprio comitê, porém, comentou que essa definição, considerada para os fins dos estudos na época, possui desvantagens, visto que também inclui comportamentos antiéticos e não autorizados, mesmo podendo estes não se configurarem crime, por mais censuráveis que sejam. Relatou ainda que o grupo de especialistas da OCDE julgou não ser útil ter como objetivo a busca de um conceito mais preciso, mas escolheu, no lugar, uma classificação funcional de crimes relacionados à computadores.

A amplitude de condutas que podem ser consideradas delitos informáticos e a grande evolução tecnológica em um curto período de tempo são fatores que dificultam a formulação de uma definição rigorosa, tornando-a vaga e até antiquada, o que abre caminho para o desenvolvimento de classificações que são mais explicativas do fenômeno da criminalidade informática. A mais conhecida linha classificatória dos crimes digitais está sustentada justamente na discriminação entre os delitos que atingem a informática e os que a utilizam como ferramenta. Essa forma de divisão é apresentada e interpretada sob perspectivas diferentes, porém mantém certa similaridade entre uma classificação e outra.

A exemplo disso, menciona-se duas classificações: a primeira divide os crimes informáticos em *cyber-dependent crimes* e *cyber-enabled crimes*, e a segunda os reparte em dois tipos de um mesmo espectro, chamando-os de tipo I e tipo II.

Os *cyber-dependent crimes*, ou crimes dependentes da cibernética, fazem referência àquelas ofensas que apenas podem ser praticadas com o uso de um computador ou alguma tecnologia da informação e da comunicação e têm como principal alvo o próprio computador e seus recursos (UNITED KINGDOM, 2013). Já os *cyber-enabled crimes*, ou crimes permitidos pela cibernética, são crimes tradicionais que são potencializados pelo uso do computador, mas não dependem deste nem de nenhum mecanismo da informação para serem praticados (UNITED KINGDOM, 2013).

Por seu turno, a classificação de Gordon e Ford (2006) é focada na ideia da existência de um espectro que se regula a partir da maior ou menor utilização da tecnologia no cometimento de um crime cibernético. O tipo I e tipo II não são categorias mas sim pontas opostas desse espectro, no qual o tipo I representa aqueles delitos que exigem maior conhecimento técnico e o emprego, sobretudo (mas não de forma exclusiva), de *crimewares*, *softwares* desenvolvidos e usados especificamente para a pratica de atividades ilícitas, como várias classes de vírus, *trojans* e *spywares*, enquanto o tipo II representa os crimes relacionados ao comportamento humano em sua execução (não excluindo, porém, o uso da tecnologia), geralmente sendo crimes que possuem persecução facilitada para os investigadores tradicionais, como fraudes ocorridas através de *e-mails* ou aplicativos de mensagens, com técnicas de *phishing*, *vishing* e *smishing*. Portanto, dentro dessa proposta, os crimes informáticos podem ser identificados como pertencentes à um desses dois polos, ou em alguma variação entre eles, de maneira flexível.

Também não se afastando dessas propostas de diferenciação, a Convenção de Budapeste (COUNCIL OF EUROPE, 2001a), no seu segundo capítulo, primeira seção, classifica as condutas consideradas como crimes cibernéticos em:

a) ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas do computador (nas quais se incluem as condutas de acesso e interceptação ilegal, interferência em dados e sistemas e uso indevido de dispositivos);
b) crimes relacionados ao computador (falsificações e fraudes relacionadas ao computador);

c) ofensas relacionadas ao conteúdo (crimes ligado à pornografia infantil); e

d) ofensas relacionadas à violações de direitos autorais e direitos conexos.

No ano de 2003, em um protocolo adicional à convenção, foi ainda acrescentada uma quinta categoria, que é formada por atos de disseminação de material racista e xenofóbico através de sistemas informáticos, por atos de ameaças e insultos motivados por racismo e xenofobia e pela conduta de distribuição de conteúdo que nega, minimiza, aprova ou justifica ações que constituem genocídio ou crimes contra a humanidade (COUNCIL OF EUROPE, 2003).

A classificação da convenção é pragmática pois lista, dentro dessas cinco espécies, as condutas que entende como crimes virtuais. Em síntese, a primeira categoria trata das ofensas contra os recursos informáticos, a segunda se refere à falsificações e fraudes dentro do meio informacional, e a terceira, quarta e quinta categorias têm como questão central a conduta criminosa relacionada ao próprio conteúdo da informação, dos *bits*, quando estes são os elementos que ferem o direito. Apesar de possuir mais categorias, nesta classificação é possível notar novamente a compreensão da distinção entre os delitos que são contra a tecnologia em questão e os que a instrumentaliza.

Vianna e Machado (2013), por sua vez, sobre o assunto, discorrem apenas sobre quatro categorias de delitos. A primeira é denominada por eles como crimes próprios (diferente dos crimes próprios que indicam a necessidade de uma qualidade individual do delinquente para realizar a ação) e trata-se dos delitos que transgridem a inviolabilidade da informação automatizada. O mero uso de um computador na execução de um crime não é suficiente para considerá-lo como um delito cibernético, uma vez que para realizar essa identificação é necessário que o bem atingido seja o bem jurídico informático, ou seja, é preciso tocar a informação, os dados. Por esse motivo, para os autores, os crimes próprios são tidos como os verdadeiros delitos informáticos. Um dos crimes apontados como exemplo desse grupo é o previsto no art. 154-A do Código Penal, que tipifica a conduta de invadir dispositivo informático alheio com o propósito de obter, adulterar ou destruir dados (BRASIL, 1940).

Apesar de sua posição sobre os crimes próprios, os professores também indicam outras três categorias de delitos virtuais. A segunda é designada crimes impróprios e trata-se dos delitos que utilizam o computador como instrumento na sua prática mas não lesionam a informação automatizada, e sim qualquer outro bem jurídico. Alguns exemplos são os delitos de estelionato, apologia ou incitação ao

crime, pornografia infantil e instigação ao suicídio, condutas que facilmente podem ser realizadas através das redes sociais. Os crimes impróprios constituem, portanto, um numeroso conjunto de condutas delituosas.

Já a terceira categoria indica aqueles crimes que além de infringirem a inviolabilidade das informações também atingem bens jurídicos de caráter distinto (a norma também tem por objetivo proteger esses outros bens, dado a sua relevância), eles são chamados de crimes mistos pelos autores. O exemplo apresentado desse tipo de delito é o que encontra-se previsto na Lei nº 9.504/97, em seu art. 72, inciso I, o qual versa sobre o acesso ao sistema de tratamento automático de dados do serviço eleitoral brasileiro com a intenção de mudar a apuração ou a contagem de votos (BRASIL, 1997).

Por último, nessa classificação, os crimes mediatos, ou indiretos, são aqueles delitos informáticos próprios que são praticados como meio para a consumação de um crime não informático, distinguindo-se dos crimes impróprios por haver, nessa categoria, ofensa à informação (portanto, trata-se de dois tipos penais diferentes). Nessa linha de pensamento, o delito-fim é entendido como um crime informático por conta do delito-meio, o qual é absolvido por aquele mediante a observância ao princípio da consunção. Seria o caso, por exemplo, da invasão de contas bancárias (crime informático próprio) para a subtração de quantias de dinheiro (crime patrimonial). Ação que pode ser um exemplo de crime mediato é a técnica criminosa conhecida como *salami slicing*, que consiste no cometimento de vários pequenos atos ilícitos, os quais geram, da sua soma, um grande ataque ou dano, normalmente de cunho financeiro.

Dessa classificação formulada por Vianna e Machado infere-se que a informação automatizada pode ser tanto o próprio bem jurídico que é lesionado pelo ato criminoso como pode ser o instrumento utilizado para ofender outros bens, o que é análogo às classificações dicotômicas já apresentadas anteriormente. Contudo, para além disso, a classificação indica também que os crimes digitais podem ser incidentais em uma conduta e até podem ofender simultaneamente bens jurídicos informáticos e bens que não fazem parte da seara cibernética. Crespo (2011) chama esse último tipo de crime de delitos pluriofensivos, tendo em vista que atingem, ao mesmo tempo, bens jurídicos distintos. Diante disso, portanto, observa-se que os conceitos e as classificações que consideram essas mencionadas características dos delitos informáticos mostram-se mais adequados e pertinentes.

Por fim, sob novos paradigmas e com propostas de diferentes agrupamentos, outras formas de caracterizar as condutas consideradas crimes informáticos também foram desenvolvidas. Sarre, Lau e Chang (2018), por exemplo, sugerem uma categoria de classificação de crimes que utilizam robôs, inteligências artificiais e mecanismos com tecnologia de *self-learning*. Já Phillips et al. (2022) propõem em sua categorização grupos de delitos que tratam de ataques contra dados pertencentes à estados e nações (como espionagem e interferências políticas), uma categoria para manipulação em massa de informações (como *fake news*, *deep fakes*, *cyber troops*, *misinformation* e *disinformation*), e categorias para crime organizado e terrorismo.

3 LEGISLAÇÃO BRASILEIRA EM MATÉRIA DE CRIMES INFORMÁTICOS E NORMAS EM ÂMBITO INTERNACIONAL

Os crimes previstos pelo art. 72 da Lei nº 9.504/97, os quais dizem respeito à condutas contra o sistema de tratamento automático de dados do serviço eleitoral brasileiro (BRASIL, 1997), bem como os crimes previstos nos arts. 313-A e 313-B do Código Penal, que tratam da inserção de dados falsos e modificação ou alteração não autorizada em sistemas de informações cometidos por funcionários públicos (BRASIL, 1940), são crimes informáticos que encontram-se tipificados no ordenamento jurídico do país há algum tempo. Em verdade, a legislação brasileira já tipificou algumas condutas delituosas cibernéticas, dentre as quais se incluem, especialmente, crimes informáticos impróprios e mistos. Apenas recentemente, contudo, é que houveram iniciativas mais significativas para tratar da matéria de forma exclusiva.

Neste capítulo serão destacadas as leis mais relevantes quanto à tipificação dos crimes em questão e seus principais pontos. Além disso, igualmente serão abordados tratados internacionais sobre o assunto e a relação do Brasil com esses acordos.

3.1 A Lei n° 12.735/12 e a Lei n° 12.737/12

Segundo Jesus e Milagre (2016), um dos primeiros esforços para legislar sobre crimes informáticos de forma específica no Brasil ocorreu com o Projeto de Lei n° 84/99, o qual tramitou por vários anos até resultar na Lei n° 12.735/12. Conforme os autores, o projeto foi bastante criticado por ter sido considerado punitivista e arriscado para o usuário comum dos espaços virtuais, por esse motivo sendo chamado de AI-5 digital.

Assim, nesse contexto, uma das reações à essa abordagem foi o incentivo às discussões sobre o Projeto de Lei n° 2.126/11, que viria a se tornar a Lei n° 12.965/14, ou o Marco Civil da Internet, o qual estabelece, na seara civil, princípios, garantias, direitos e deveres para o uso da internet no país (ARNAUDO, 2017).

Também como uma resposta ao PL n° 84/99, surgiu o PL n° 2.793/11, que igualmente tipificava conduta delituosas, porém em uma perspectiva mais neutra (JESUS; MILAGRE, 2016). Os dois projetos foram aprovados em 2012 e geraram a Lei n° 12.735 e 12.737, respectivamente.

Apesar da aprovação, anteriormente o PL n° 84/99 já tinha sido substancialmente alterado e reduzido, e a própria lei que concebeu, também conhecida como Lei Azeredo (por causa do deputado Eduardo Azeredo, um dos seus apoiadores), sofreu dois vetos (JESUS; MILAGRE, 2016). Do que restou, hoje a Lei n° 12.735 somente prevê, em seu art. 4°, a estruturação, por órgãos da polícia judiciária, de setores e equipes especializadas em crimes cibernéticos (BRASIL, 2012a) e, em seu art. 5°, acrescentando à Lei nº 7.716/89 (que trata de crimes resultantes do preconceito de raça ou cor), a possibilidade do juiz determinar a cessação das respectivas transmissões eletrônicas, ou de publicação por qualquer meio, quando o delito é cometido por intermédio de meios de comunicação social, de publicação em redes sociais, da rede mundial de computadores ou de publicação de qualquer natureza (BRASIL, 1989).

Por seu turno, a Lei n° 12.737, mais reconhecida pelo nome Lei Carolina Dieckmann (devido ao caso de vazamento de fotos íntimas da atriz, fato que foi bastante repercutido pela mídia na época e que impulsionou a aprovação do projeto de lei), trouxe maiores novidades legislativas. A lei alterou o Código Penal com a inserção do art. 154-A, que tipifica a conduta de invasão de dispositivo informático, e com a adição do art. 154-B, que determina a ação penal pública condicionada como regra para o crime em questão, a menos se o crime for cometido contra a administração pública de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (BRASIL, 2012b). Além disso, a lei modificou a redação do art. 266 do diploma penal, mudando o nome do tipo, que passou a incluir a interrupção ou perturbação de serviços informáticos, telemáticos ou de informação de utilidade pública, bem como acrescentou os §§1º e 2º no dispositivo (BRASIL, 2012b).

Recentes alterações promovidas pela Lei nº 14.155/21, contudo, modificaram o art. 154-A, que passou a ter o seguinte texto no Código Penal (BRASIL, 1940):

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: [Alterado pela Lei nº 14.155, de 2021]
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. [Alterado pela Lei nº 14.155, de 2021]

> § 1° Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2° Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. [Alterado pela Lei nº 14.155, de 2021]
> § 3° Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. [Alterado pela Lei nº 14.155, de 2021]
> § 4° Na hipótese do §3°, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5° Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Em 2021, a Lei nº 14.155, além de subir a pena do *caput*, da causa de aumento do §2°, e da qualificadora do §3°, também excluiu trecho do *caput* muito reprovado pela doutrina desde de 2012. Se trata da previsão anterior que exigia a violação indevida de mecanismo de segurança para o reconhecimento da invasão do dispositivo, o que notoriamente era uma lacuna legal grave, que tornava atípica, por exemplo, condutas como acessar através de um vírus um computador que não possuísse antivírus, ou acessar pessoalmente um aparelho sem senha (VIANNA; MACHADO, 2013). Com essa exclusão, observa-se que agora o verbo mais coerente para a norma seja acessar, no lugar de invadir.

Ademais, a Lei nº 14.155 também inseriu a expressão uso alheio, a fim de ser possível enquadrar o próprio proprietário do dispositivo como sujeito ativo do delito. Isto porque, como estava redigida anteriormente, a redação rechaçava essa hipótese, convertendo em atípica, por exemplo, a prática do delito por donos de *lan houses*, nos computadores locados, ou por empregadores, nos computadores utilizados pelos empregados no trabalho (VIANNA; MACHADO, 2013).

Quanto à sua classificação, aponta-se que o tipo previsto no art. 154-A é um crime informático próprio e tem como bem jurídico a inviolabilidade das informações automatizadas. Moura (2021) afirma que, tendo em vista a localização da norma no Código Penal, considerando o título, o capítulo e a seção que está situada, o bem jurídico que o legislador procurou proteger foi a liberdade individual da pessoa, tutelando sua intimidade e privacidade segundo o art. 5° da Constituição

Federal (BRASIL, 1988). O autor, porém, entende que melhor opção teria sido a elaboração de um capítulo específico para os crimes cibernéticos, já que sistematizaria a matéria e facilitaria a interpretação e aplicação da lei.

O objeto material do crime é evidentemente o dispositivo informático. Contudo, uma redação mais completa do artigo acrescentaria também programas ou sistemas informáticos, vez que a norma não visa proteger apenas o suporte físico do processamento de dados. Isso é notório na adição, já comentada, da expressão uso alheio no tipo, que teve como intenção resguardar as informações do usuário da máquina, não necessariamente o aparelho utilizado. Nesse aspecto, interessante mencionar que a figura equiparada prevista no §1° já traz a distinção, se referindo tanto a dispositivos quanto a programas de computador, enquanto o *caput* não.

Para além disso, é relevante mencionar que o legislador previu que a invasão pode ocorrer tanto *online* quanto *off-line*. Nucci (2021a, p. 295), sobre o assunto, nota que “faz-se menção expressa ao estado do dispositivo no tocante à rede de computadores, incluindo, por óbvio, a Internet (rede mundial de computadores): é indiferente haver conexão ou não”. Importante também é a exigência de elementos subjetivos específicos, que são a intenção de obter, adulterar ou destruir dados ou, no segundo núcleo da norma, a obtenção da vantagem ilícita. A presença desses elementos são imprescindíveis para não haver o risco de criminalizar condutas normais, como o trabalho e a pesquisa na área de segurança cibernética, as quais muitas vezes testam sistemas e estudam vulnerabilidades informáticas.

Por sua parte, os parágrafos do art. 154-A trazem ainda uma forma equiparada ao *caput*, uma forma qualificada e algumas causas de aumento. O §1° tem o objetivo de desestimular o crescimento do crime e de punir aquele que se beneficia de sua proliferação. Previsão semelhante há na Convenção de Budapeste, no seu art. 6°, n°1, a), que entende como infração a produção, a venda, a obtenção para utilização, a importação, a distribuição e outras formas de disponibilização de dispositivos, programas informáticos, palavras-passe, códigos de acesso, ou similares, com os propósitos delituosos compreendidos pelo tratado (COUNCIL OF EUROPE, 2001a).

O §2°, por sua vez, prevê uma causa de aumento se a invasão de dispositivo informático resultar em prejuízo econômico. Já o §4° estabelece uma causa de aumento específica para o §3°. O parágrafo determina maior pena para a

forma qualificada do delito se houver a divulgação, a comercialização ou a transmissão para terceiro do conteúdo obtido.

A Lei n° 12.737 também trouxe como crime cibernético a forma equiparada do §1°do art. 266 do Código Penal. O *caput* do referido tipo criminaliza a ação de interromper ou perturbar o serviço telegráfico, radiotelegráfico ou telefônico, bem como impedir ou dificultar o restabelecimento desses serviços, definindo a pena de um a três anos de detenção e multa. O §1° veio para incluir o serviço telemático na proteção jurídica da norma, da seguinte forma: “Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento” (BRASIL, 1940).

Aqui o bem jurídico tutelado pela lei é a incolumidade pública. O delito em questão, portanto, abrange apenas os atos que são contra um número indeterminado de pessoas, ou seja, a coletividade, e não um indivíduo ou grupo específico (VIANNA; MACHADO, 2013). Ademais, os serviços mencionados na norma devem ser públicos, não abarcando os casos em que mesmo grandes redes privadas sejam atingidas, como *intranets* (VIANNA; MACHADO, 2013).

Na hipótese de interrupção ou perturbação de comunicação entre pessoas determinadas, Greco (2022) defende a aplicação do art. 151, §1°, III, do Código Penal ao caso. No entanto, o citado artigo indica taxativamente o impedimento de comunicação telegráfica, radioelétrica e telefônica, não incluindo comunicação telemática ou informática.

Os objetos materiais do art. 266 são o serviço telemático e o serviço de informação de utilidade pública. Nucci (2021b), porém, critica essa última possibilidade por considerar que a mesma é genérica e fere a taxatividade, dado que nessa lógica pode se dar em qualquer meio de transmissão. A respeito da figura do §1°, o autor também chama atenção para a referência ao serviço informático no título do crime mas aponta sua ausência no tipo penal, o que o excluiria da aplicação da norma. No entanto, entende que o termo telemático é suficiente para a finalidade pelo qual foi proposto. Citado em capítulo anterior dessa pesquisa, contudo, recorda-se que, apesar de interligadas, as expressões telemática e informática não são equivalentes e, em um caso mais específico podem gerar confusões.

Por fim, é importante apenas mencionar que as condutas dos art. 154-A e art. 266, §1° são distintas da conduta (que também é uma espécie de delito informático) prevista no art. 10 da Lei n° 9.296/96, que institui como crime “realizar

interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei" (BRASIL, 1996). Os verbos utilizados nos tipo são diferentes e apontam para ações diferentes: a ação trazida pelo artigo é de interceptar, ou captar, as comunicações, diferente da invasão, acesso ou interrupção.

3.2 A Lei n° 14.155/21

A Lei n° 14.155/21 foi aprovada em meio ao contexto de isolamento social provocado pela pandemia de covid-19, o qual gerou uma intensificação das atividades virtuais de um modo geral, inclusive em diversas áreas profissionais, que passaram a funcionar de maneira remota. Junto com essas mudanças, contudo, também surgiram notícias sobre o aumento vertiginoso de condutas criminosas cibernéticas, além de casos de fraudes e golpes envolvendo o auxílio emergencial.

Assim, no intento de suprir algumas demandas originadas desse cenário, a Lei n° 14.155 (BRASIL, 2021b), mais do que somente agravar penas (citadas no tópico anterior), também acrescentou os §§4°-B e 4°-C ao art. 155 do Código Penal, para tratar do furto mediante fraude cometido por intermédio de dispositivos eletrônicos ou informáticos. Também foram adicionados os §§2°-A, 2°-B, e o §4° ao art. 171 do diploma penal, prevendo o estelionato mediante fraude eletrônica. Ambos os delitos, inseridos ao mesmo tempo na legislação brasileira, têm como bem jurídico protegido o patrimônio e são crimes informáticos impróprios.

O furto mediante fraude, que está estabelecido no §4°, inciso II, do art. 155 é uma forma qualificada do delito em questão. A intenção do legislador nesse dispositivo é punir com maior severidade a subtração de coisa alheia móvel praticada através do engano da vítima, diminuindo sua vigilância. Assim, o §4°-B, que também é outra qualificadora, apresenta uma espécie ainda mais grave de furto cometido por meio de fraude, sendo, nas palavras de Moura (2021), "um furto qualificado 'mais' qualificado, já que a pena não é somente de 2 a 8 anos [de reclusão] e multa como prevê os furtos qualificados do §4° do artigo 155, CP, mas sim de 4 a 8 anos e multa".

Bitencourt (2022) explica que a norma criou três hipóteses dessa qualificadora, que são: a) a subtração cometida mediante fraude cibernética; b) a subtração cometida com a utilização de programas maliciosos; e c) a subtração praticada através de qualquer outro meio fraudulento análogo.

O primeiro caso é aquele em que o dispositivo eletrônico ou informático é utilizado para o cometimento do furto, sendo desnecessária, como o legislador deixou bem evidente, a conexão com a internet ou a violação de mecanismos de segurança preexistentes. A segunda situação fraudulenta trata do uso de programas (*malwares*) que têm a função de realizar ações viciadas e danosas em um computador, deixando-o vulnerável e, assim, reduzindo a vigilância da vítima. Por último, a terceira hipótese de subtração é uma autorização de equiparação feita pelo legislador para identificar furtos fraudulentos que não foram previsto pelo parágrafo, os quais precisam, devido ao uso da palavra análogo, ser equivalentes aos que foram anteriormente apontados.

Já os incisos do §4°-C do art. 155 cuidam de duas causas de aumento que são aplicadas, se for o caso, de acordo com a relevância do resultado gravoso. A primeira delas, presente no inciso I, ocorre quando o furto é efetuado com o uso de um servidor mantido fora do território nacional, circunstância que revela não apenas maior culpabilidade por parte do infrator como também mais dificuldade na persecução penal, dado o aspecto transnacional da conduta (MOURA, 2021). Já o inciso II trata da causa de aumento aplicada quando a subtração é cometida contra idosos ou vulneráveis, vez que, em geral, devido a sua pouca expertise com aparelhos informáticos, são mais suscetíveis de serem alvos fáceis, condição que é explorada por criminosos (MOURA, 2021).

A outra forma qualificada que foi introduzida pela Lei n° 14.155 é o estelionato cometido mediante fraude eletrônica, que possui a pena de quatro a oito anos de reclusão e multa. Nessa qualificadora a obtenção da vantagem ilícita acontece com a indução ou manutenção da vítima em erro por meio de fraude realizada através de redes sociais, contatos telefônicos, correio eletrônico ou outro meio fraudulento análogo. Frisa-se que nesta situação a vítima (ou terceiros), ludibriada, entrega voluntariamente suas informações ao delinquente e esses dados são utilizados para a obtenção da vantagem. Não trata-se, pois, do crime de furto.

Enquadra-se nessa qualificadora, por exemplo, golpes em que a vítima, acreditando estar em uma loja virtual, ou site comercial, envia suas informações bancárias a fim de adquirir um produto mas acaba descobrindo que tais sites não correspondem a negócios reais e percebe que quantias foram retiradas de sua conta. Golpes que também podem ser incluídos são aqueles onde o criminoso liga para a vítima, informando ser representante do seu banco, e lhe pede informações e senha do seu cartão alegando que o mesmo foi clonado e sugerindo uma solução para o

problema. Ou, ainda, casos de ofertas de emprego falsas feitas via *Whatsapp* com a intenção de induzir os alvos a fornecerem informações que serão usadas para a obtenção da vantagem ilícita. Comumente para a realização dessas fraudes é usada a chamada engenharia social, um conjunto de técnicas que consistem em persuasão e manipulação para convencer as vítimas.

Por último, menciona-se que o §2°-B e o §4° do art. 171 trazem causas de aumento de pena idênticas às presentes nos incisos I e II do §4°-C do art. 155, os quais já foram abordados.

3.3 A Convenção de Budapeste e a adesão do Brasil ao tratado

A Convenção sobre Crimes Cibernéticos, ou Convenção de Budapeste, é um tratado internacional de direito penal e direito processual penal cujo texto foi aberto para assinaturas e adesões na data de 23 de novembro de 2001, em Budapeste, na Hungria, dentro da esfera do Conselho da Europa. Atualmente são partes da convenção 68 países, nos quais se incluem 45 membros do próprio conselho e 23 que não são integrantes da organização, como o Canadá, o Japão, a Argentina e o Chile, havendo ainda 2 países que não ratificaram o documento e 18 que foram convidados à aderir.

O tratado é o primeiro e mais citado mecanismo internacional em matéria de crimes informáticos, versando sobre a harmonização de legislações nacionais, a produção de provas digitais e a cooperação internacional em procedimentos e investigações. O diploma também conta com dois protocolos adicionais, o primeiro aberto para assinaturas em 2003, tratando de crimes de natureza racista e xenofóbica cometidos no ambiente cibernético, e o segundo, aberto em 2022, tratando do reforço à cooperação e da divulgação de provas eletrônicas.

O surgimento das discussões sobre a criminalidade informática no Conselho da Europa, assim como em outras iniciativas internacionais, está atrelado à natureza transnacional de muitas conduta praticadas no ambiente virtual, fator que foi determinante para buscar trabalhar o tema de maneira mais ampla.

Uma das primeiras menções relacionadas aos crimes cibernéticos dentro do conselho ocorreu de modo muito breve em 1981, associando condutas como roubo de informações e manipulação de dados ao estudo das problemáticas dos crimes econômicos (COUNCIL OF EUROPE, 1981). Conduto, segundo o relatório explicativo

da convenção, mais tarde, em 1996, o Comitê Europeu para Problemas Criminais (CDPC) decidiu formar um comitê específico de especialistas a fim de abordar os crimes digitais, ato que, somado às sugestões de criação de uma convenção sobre o assunto, por recomendações e relatórios anteriores (como o relatório elaborado pelo professor H.W.K. Kaspersen, o relatório anexado à Recomendação Nº R (89) 9 e a Recomendação Nº R (95) 13), bem como acrescido à um longo processo de negociação do texto do tratado, resultou na adoção e abertura da convenção de Budapeste no ano de 2001 (COUNCIL OF EUROPE, 2001b).

Conforme o relatório explicativo do tratado, uma das mais emergentes circunstâncias que impulsionou essas mencionadas ações, direcionando-as à criação de um instrumento internacional para lidar com o cibercrime, foi a constatação do caráter transfronteiriço do comportamento criminoso no ciberespaço e a percepção das limitações dos países, quando sozinhos e apenas com suas legislações domésticas, em confrontá-lo (COUNCIL OF EUROPE, 2001b).

Conscientes disso, e compreendendo as profundas transformações geradas pela tecnologia da informação e pela sua duradoura intensificação e globalização, os elaboradores da convenção, no preâmbulo do documento, apontaram como objetivo da iniciativa a defesa da sociedade contra os crimes cibernéticos, por meio da formulação de normas apropriadas para uma nova realidade tecnológica e pelo incremento da colaboração entre os países, tudo dentro de uma política criminal conjunta (COUNCIL OF EUROPE, 2001a).

O tratado possui quatro capítulos, que discorrem, respectivamente, sobre:

a) algumas terminologias essenciais à interpretação e aplicação do texto (possibilitando a delimitação de alguns elementos intrínsecos à pratica de cibercrimes e indicando entidades que podem ser alvos, colaboradores, ou que figurem em procedimentos do interesse das partes);
b) medidas a serem tomadas em nível nacional pelos países, tratando do direito material (quando aponta um padrão mínimo de tipificações de condutas informáticas criminosas, mencionadas no capítulo anterior desta pesquisa, bem como quando trata das sanções e da responsabilização de pessoas jurídicas) e processual (versando sobre pontos como competência, salvaguardas, busca e apreensão de informações, e conservação, recolha e interceptação de dados);

c) cooperação internacional, abordando tópicos como princípios e procedimentos relativos ao auxílio mútuo (principalmente na obtenção de evidências eletrônicas e em investigações), à extradição, à medidas provisórias e à rede 24/7 de assistência imediata; e

d) as disposições finais (COUNCIL OF EUROPE, 2001a).

Apesar da necessidade de um arcabouço jurídico mais consistente quanto à crimes cibernéticos no Brasil e da dificuldade em processos e investigações que envolvam dados, informações e conexões com o estrangeiro, a adesão à convenção apenas foi aprovada em 2021, através do decreto legislativo n° 37, de dezembro do mencionado ano, estimulada pelo Ministério Público Federal e outras autoridades, sendo promulgada em 2023 por meio do decreto n° 11.491.

Com a aderência, a expectativa é de que a produção probatória relativa à crimes cibernéticos próprios e impróprios seja positivamente impactada, vez que tem o condão de facilitar a obtenção de provas no exterior e influenciar a elaboração de efetivos e novos métodos de forense digital frente à uma nova realidade tecnológica (WEBINAR, 2022).

Nesse sentido, sobre os meios de obtenção de provas, ressalta-se que a aprovação da adesão à convenção ocorreu durante o curso do julgamento da Ação Declaratória de Constitucionalidade 51, no Supremo Tribunal Federal (STF), o qual discutiu a constitucionalidade do *Mutual Legal Assistance Treaty* (MLAT), acordo de colaboração em investigações criminais celebrado entre o Brasil e os Estados Unidos e promulgado pelo Decreto Federal 3.810/2001. O julgamento, que versou sobre o compartilhamento de dados com provedores sediados fora do Brasil, resultou na declaração de constitucionalidade das normas que tratam dos mecanismos de cooperação internacional do MLAT e da expedição de carta rogatória, mas também resultou no reconhecimento da possibilidade de autoridades brasileiras requisitarem de forma direta dados dos representantes de empresas de tecnologia no país, com fundamento no art. 11 da Lei n° 12.965 e no art. 18 da Convenção de Budapeste.

O art. 18 do tratado estabelece que cada parte adote medidas legislativas e providências a fim de dar poderes às autoridades para ordenar qualquer pessoa residente em seu território e provedor de serviço que atue no país a entregar dados de computador e fornecer informações cadastrais de assinantes de tais serviços, que estejam sob a detenção ou controle do provedor (COUNCIL OF EUROPE, 2001a).

Além dessa situação, através do tratado, a própria interpretação de textos legais referentes à matéria pode ser aprimorada, à exemplo da Lei nº 14.155 que, dentre outras alterações, estabeleceu causas de aumento de pena em crimes que usam servidores fora do território nacional, mas não definiu a que tipo de servidores fazem referência (WEBINAR, 2022). O entendimento de termos e conceitos, especialmente aqueles atrelados às novas tecnologias, são fundamentais para a aplicação da lei, a vista disso a convenção pode contribuir para a supressão de algumas ausências de definições.

Ainda, a adesão possibilita que o Brasil integre mecanismos de auxílio como a rede 24/7 e o comitê específico da convenção, chamado de Comitê T-CY. A rede 24/7 é uma rede de contatos entre os estados que foi instituída por meio do art. 35 do tratado com o propósito de prestar ajuda rápida para investigações, recolha de provas e outros trâmites (COUNCIL OF EUROPE, 2001a). Já o Comitê T-CY tem como principais finalidades a troca de informações sobre a aplicação do tratado nos países, a realização de discussões sobre novidades tecnológicas e legislativas pertinentes à convenção e a produção de notas de orientação sobre temas como *botnets*, ataques de DDoS (*distributed denial of service*), *spam* (*unsolicited usually commercial messages*) e terrorismo (SANTOS, 2022).

Por outro lado, a despeito desses inegáveis benefícios, alertas realizados principalmente por organizações da sociedade civil e grupos de pesquisa focados na internet enfatizam que a adesão à convenção também pode representar perigos à legislação nacional, à proteção de dados e à direitos fundamentais correlatos. Um desses grandes pontos de preocupação reside na aprovação sucinta do texto do tratado, que foi realizada sem a apresentação de reservas pelo Brasil.

Conforme o Instituto de Referência em Internet e Sociedade, a entrada do texto no ordenamento jurídico brasileiro, em caráter total e irrestrito, torna-se um risco às normas internas do país, com consequências para o âmbito nacional de proteção de direitos digitais e com possibilidade de choque entre disposições legais, como as presentes no Marco Civil da Internet, na Lei Geral de Proteção de Dados (LGPD), na Lei de Direitos Autorais, na Lei de Interceptações, no Código Penal e na Lei nº 11.829/2008 (RODRIGUES, 2021).

A rapidez do processo que aprovou o decreto legislativo nº 255/2021 (posterior decreto nº 37, de 2021), bem como um debate pouco participativo e não multisetorial sobre a questão são alguns dos fatores apontados como causas dessa

ausência de reservas e declarações por parte do Brasil, o que mostra-se preocupante visto que esses são importantes instrumentos que auxiliam a implementação da convenção e sua conformidade com normas internacionais sobre direitos humanos (RODRIGUES, 2021). Apesar disso, importa lembrar que, mesmo com a utilização desses importantes mecanismos, que mitigam os atritos com a legislação nacional, ainda há possibilidade de conflito entre normas.

Moura (2021), por exemplo, mesmo considerado a adesão uma ação benéfica para o enfrentamento aos crimes cibernéticos no Brasil, chama a atenção para alguns tópicos do texto do tratado, remetendo-os à legislação brasileira. Um deles trata-se da previsão de responsabilidade por omissão de supervisão, ou falta de controle, por parte de pessoa singular, previsto no item 2 do art. 12 do tratado. Nesse caso o dispositivo poderia ser interpretado para responsabilizar a figura do *compliance officer*, situação que no Brasil ainda não existe legislação específica sobre o assunto. Outro tópico mencionado pelo autor trata da necessidade de mudança nos prazos de conservação de dados informáticos previstos no Marco Civil da Internet, pois eles são maiores (um ano para registros de conexão e seis meses para registros de acesso, de acordo com os arts. 13 e 15) e divergem do prazo trazido pela convenção no seu art. 16 (noventa dias, no máximo).

Em adição à observação desses pontos, menciona-se que a Associação Data Privacy Brasil de Pesquisa, sobre a adesão à convenção, destaca a necessidade de haver o impulso e debates relativos ao anteprojeto da Lei Geral de Proteção de Dados na seara penal, vez que este deve defender o equilíbrio da persecução penal de crimes cibernéticos, com o reforço de salvaguardas e limites para a atuação estatal, a fim de evitar práticas como *government hacking* ou *fishing expedition*, garantindo assim a defesa de direitos fundamentais ligados à proteção de dados (EILBERG et al., 2021).

Em suma, observa-se que a aprovação da adesão do Brasil ao tratado de Budapeste, ainda que tardiamente, é essencial para o combate aos crimes digitais pois inicia um processo de delimitação e formação de interpretações sobre conceitos e termos relevantes, bem como apresenta um norte para a realização de tipificações de condutas criminosas na área cibernética e incrementa as noções de produção probatória, além de propiciar melhor cooperação em nível internacional. Contudo, ainda existem questões a serem trabalhadas, sobretudo as relacionadas com os possíveis conflitos entre normas, com a proteção de direitos fundamentais ligados à

dados pessoais e com o estabelecimento de garantias na persecução criminal que não inviabilizem as investigações de crimes cibernéticos.

3.4 A Convenção sobre Crimes Cibernéticos da ONU

Em 2019, a assembleia geral da Organização das Nações Unidas (ONU), através da Resolução 74/247, estabeleceu um comitê intergovernamental de especialistas para formular uma convenção sobre o combate ao uso de tecnologias da informação e da comunicação para fins criminosos (UNITED NATIONS, 2019). Até o momento o comitê já promoveu cinco sessões de debates e negociações do texto, com a participação de diversos Estados-membros e entidades da sociedade civil. O grupo tem a previsão de finalizar o rascunho do tratado e encerrar os seus trabalhos no ano de 2024.

A proposta de elaboração de um tratado sobre crimes digitais no âmbito da ONU surgiu principalmente como uma iniciativa da Rússia para substituir a Convenção de Budapeste, tratado que o país não participa pois alega que desrespeita o princípio da soberania estatal no tratamento de operações transfronteiriças (PAGE, 2022). Contudo, em meio ao conflito que atualmente ocorre na Ucrânia e diante de notícias sobre ataques cibernéticos russos direcionados à sites ucranianos, a Rússia foi bastante criticada durante as reuniões do comitê, sendo acusada de violar princípios do direito internacional, bem como de contrariar os objetivos do próprio tratado em discussão (PIGATTO; ZANATTA, 2022).

Além disso, também foi criticado o posicionamento russo sobre a definição de crimes cibernéticos, o qual é compartilhado por países como Indonésia e Malásia, defendendo a adoção de um conceito expansivo, que inclui o máximo possível de tipos penais (PIGATTO; ZANATTA, 2022). O uso dessa ampla definição traz preocupações no sentido de poder abrir meios para uma indevida repressão estatal, especialmente em países onde as legislações são mais severas quanto à utilização da internet (OHANIAN, 2022). Países como Alemanha, México e Estados Unidos, em contrapartida, foram contrários à esse conceito abrangente, destacando a cooperação e o respeito ao devido processo legal em crimes transnacionais (PIGATTO; ZANATTA, 2022).

Outro foco de preocupações referentes ao tratado são propostas como as apresentadas pela Índia e pelo Egito, em que não foram incluídas a necessidade de

uma intenção delitiva em normas que tipificam condutas, o que pode gerar, se aprovado nesses termos, um tratado que ameaça pesquisadores e profissionais da área de segurança cibernética (ou os conhecidos *white-hat hackers*, ou *hackers* éticos), além de empresas de tecnologia e outras atividades e pessoas que lidam com informação e comunicação (OHANIAN, 2022).

Apesar dessas observações e preocupações, é importante destacar que, se bem-sucedida, uma convenção elaborada no âmbito da ONU tem o potencial de se tornar o tratado sobre crimes cibernéticos mais amplamente adotado do mundo, perpassando e complementando os esforços da Convenção de Budapeste, Ademais, diferente da mera adesão, a participação do Brasil na negociação do texto, como está ocorrendo, é de maior interesse para uma alinhamento com os posicionamentos e a legislação do país.

4 A TEORIA DA ANOMIA NO PENSAMENTO DE DURKHEIM E MERTON

De origem grega, a palavra anomia literalmente significa ausência de normas (*a* indica ausência e *nomos*, lei), mas pode representar também, em muitos casos, a ideia de desordem, injustiça ou iniquidade (SHECAIRA, 2014). Relacionada à esse significado, a teoria versa justamente sobre conjunturas em que há uma falta de leis para disciplinar a vida em sociedade, tratando de estados de inexistência ou enfraquecimento de regras.

Ao longo do tempo, hipóteses e explicações sobre o surgimento de uma situação anômica na sociedade foram formuladas por muitos autores, tendo sido adotados diferentes enfoques de análise. Os maiores expoentes relacionados a essas reflexões foram Émile Durkheim, dentro da sociologia, e Robert King Merton, que trouxe a anomia mais especificamente para o campo da criminologia.

A teoria é considerada como pertencente ao grupo das teorias criminológicas macrossociológicas, porque adota um olhar global sobre a sociedade em detrimento de uma visão a partir do indivíduo. Além disso, é funcionalista. O funcionalismo entende a coletividade como um sistema que tem por base funções, as quais, sendo confluentes, permitem a continuidade da vida social. Como explicam Maíllo e Prado (2013, p. 266):

> A proposição de Durkheim é claramente funcionalista: a estrutura de uma sociedade, em vez de os distintos elementos que a constituem, se inter-relacionam sem graves atritos, harmonizando-se de maneira disfuncional ou anômica. Recorre a forças de nível social para explicar comportamentos personalíssimos, aplicando a metodologia quantitativa própria das ciências naturais.

Apesar de posteriormente ter sido estudada e ampliada por outros autores, um dos primeiros a formular a teoria foi o sociólogo francês Émile Durkheim, que viveu no século XIX e buscou analisar objetivamente as transformações da sociedade da sua época. Ele tratou da anomia em duas de suas principais obras: em *Da divisão do trabalho social*, de 1893, e em *O suicídio*, de 1897. Na primeira delas, observou a anomia dentro do estudo das sociedades diferenciadas e da especialização das funções, entendendo-a como uma forma anormal de configuração dos órgãos sociais que resulta em desarmonia social. Já na segunda, ele a abordou na explicação das causas do fenômeno do suicídio, apresentando-a como um estado de desregramento coletivo provocado por grandes perturbações da ordem.

O sociólogo americano Robert King Merton, por seu turno, influenciado pelas suas observações da sociedade americana já no século XX, aprofunda o pensamento sobre a anomia e a relaciona com a tensão existente entre o que denomina metas culturais e meios institucionalizados. Ele afirma que a sociedade possui objetivos culturalmente desejáveis e meios legais para alcançá-los, porém também possui contradições e desigualdades entre essas mesmas metas e meios, o que fomenta o crime e um estado social anômico.

Dado esse quadro, no presente capítulo ambas as perspectivas de Durkheim serão expostas, em conjunto com a visão do autor sobre o crime, e com a concepção de anomia de Merton, para que, em capítulo subsequente, todas sejam relacionados ao contexto dos delitos cibernéticos no Brasil.

4.1 Solidariedade, divisão do trabalho e anomia

Antes de entender propriamente a ligação entre anomia e divisão do trabalho no pensamento de Durkheim, é necessário compreender a noção de consciência coletiva, bem como distinguir as espécies de sociedade e os dois tipos de solidariedade social. A consciência coletiva nada mais é do uma consciência comum à maioria dos integrantes de um dado grupo social que, ao mesmo tempo em que não se confunde com a consciência singular dos seus membros, existe e atua neles (DURKHEIM, 1999). Há, portanto, nessa lógica, duas consciências: essa consciência comum, que vive em todos os indivíduos, e a consciência particular, que representa pessoalmente e distingue cada sujeito (DURKHEIM, 1999).

A consciência coletiva é constituída por um conjunto de crenças e sentimentos que são compartilhados pela média dos membros de uma determinada sociedade, permanecendo através de gerações sucessivas e, inclusive, sendo um elo entre as mesmas (DURKHEIM, 1999). Ela, contudo, não é uniforme e pode abarcar uma maior ou menor extensão (DURKHEIM, 1999). Nas sociedades arcaicas, essa extensão da cobertura da consciência comum é maior porque os seus membros são menos singulares e são mais semelhantes entre si, é nessas organizações sociais que funciona a solidariedade mecânica (DURKHEIM, 1999). Já nas sociedades diferenciadas, que são mais modernas, a consciência comum é reduzida e seus integrantes são mais individualizados, é nelas que se manifesta a solidariedade orgânica (DURKHEIM, 1999).

Para Durkheim (1999, p. 31) “quanto mais os membros de uma sociedade são solidários, mais mantêm relações diversas seja uns com os outros, seja com o grupo tomado coletivamente”, fato que promove a coesão no grupo. O que conclui o sociólogo, consequentemente, é que a integração social, permitida pela solidariedade mecânica, tem como base uma forte consciência coletiva, que ocupa grande espaço nos indivíduos e não os permite se diferenciar muito. Ele compara a situação ao movimento de moléculas em corpos inorgânicos, corpos brutos, vez que a consciência individual majoritariamente apenas segue os movimentos do coletivo, por isso usa a palavra mecânica.

Bastante diferente é a coesão promovida pela solidariedade orgânica, que tem por base a divisão do trabalho. Aqui, apesar de existir uma consciência coletiva reduzida, não significa dizer que a integração é menor, pelo contrário, quanto mais individualização, mais há coesão. Durkheim (1999, p. 108) justifica essa aparente contradição afirmando que “de um lado, cada um depende tanto mais estreitamente da sociedade quanto mais dividido for o trabalho nela e, de outro, a atividade de cada um é tanto mais pessoal quanto mais for especializada”. Ele compara essa solidariedade à órgãos que, com a sua autonomia e individuação, possibilitam a unidade do organismo, ou seja, havendo movimento próprio dos membros de um grupo, este, por consequência, torna-se apto a mover-se em conjunto. Daí a explicação para a palavra orgânica.

A divisão do trabalho e a especialização das funções são típicas da modernidade e foram acentuadas pela chegada da era da máquina, a qual gerou diferentes áreas de atividades, tanto sociais como econômicas (SELL, 2017). Aron (2003, p. 472) explica resumidamente que a causa da divisão do trabalho nas sociedades modernas somente pode ser esclarecida através de outros fenômenos sociais combinados, sendo eles o volume, a densidade material e a densidade moral:

> Para que o volume, isto é, o aumento do número dos indivíduos, se torne uma causa da diferenciação, é preciso acrescentar a densidade, nos dois sentidos, o material e o moral. A densidade material é o número dos indivíduos em relação a uma superfície dada do solo. A densidade moral é a intensidade das comunicações e trocas entre esses indivíduos. Quanto mais intenso o relacionamento entre os indivíduos, maior a densidade. A diferenciação social resulta da combinação dos fenômenos do volume e da densidade material e moral.

Entendida esta causa, é fundamental também compreender a função da divisão do trabalho. Segundo Durkheim (1999), em um primeiro olhar, o papel da

divisão do trabalho é, por óbvio, aumentar a força produtiva e a habilidade do trabalhador, bem como desenvolver intelectualmente e materialmente as sociedades. A despeito de não negar esses papéis, ele também aponta que muito mais do que os serviços econômicos que ela presta, a divisão do trabalho tem sua função baseada no efeito moral que gera. Nas sociedades diferenciadas, ao mesmo tempo em que o indivíduo recebe o que precisa da sociedade, visto que ele não se basta, ele também trabalha para o grupo. Por meio dessa interdependência, o sujeito tanto valora a si mesmo, se encontrando no organismo, como a sociedade deixa de ver seus membros como coisas e os assume como cooperadores, com os quais tem deveres.

Essa conjuntura, porém, é considerada dentro de uma perspectiva de normalidade, a qual nem sempre existe. A divisão do trabalho, apesar de comumente criar solidariedade, também pode apresentar formas patológicas. Dentro dessa noção, Durkheim se debruça sobre o que chamou de divisão do trabalho anômica. Casos em que existe anomia ocorrem, por exemplo, nas crises industriais e comerciais, nas falências, no antagonismo entre o trabalho e o capital e, até mesmo, quando a ciência se ramifica. Esse estado anômico se caracteriza pela ausência de regras, quando as ligações entre os órgãos da sociedade não estão reguladas. Nas próprias palavras de Durkheim (1999, p. 383): “[a] regulamentação ou não existe, ou não tem relação com o grau de desenvolvimento da divisão do trabalho”.

O autor explica que a solidariedade orgânica exige não apenas a existência de um sistema de órgãos que se vinculam entre si, mas também uma maneira predeterminada de como eles devem convergir. Em uma situação normal, as regras do organismo surgem por si mesmas da divisão do trabalho, visto que, dentro da sua dinâmica, são resultantes de reiteradas maneiras de reagir, as quais se tornam hábitos e posteriormente normas de conduta. É dessa forma que elas permitem a harmonia habitual das funções.

A anomia não se instala, portanto, quando os órgãos da sociedade estão em contato suficiente e de forma suficientemente prolongada. Se esses órgãos forem próximos uns dos outros, eles terão consciência de seus anseios e facilmente realizarão trocas entre si, havendo a constituição de regras. Mas, se a conexão entre os órgãos tiver durado pouco tempo, ainda é possível que um estado de anomia se estabeleça. A anomia pode ser, portanto, um fenômeno transitório. Para exemplificar, são apontados dois casos.

O primeiro se trata da mudança brusca das formas de mercados entre uma sociedade simples e uma sociedade diferenciada. Anteriormente, nas sociedades simples, os produtores facilmente compreendiam as demandas de seus consumidores e as satisfaziam, devido ao fato de que ambos estavam próximos um do outro. Com a mudança do tipo de sociedade, contudo, o mercado se expandiu, englobando outros e abarcando, inclusive, mercados estrangeiros, em uma escala que afastou produtores e consumidores. Dessa maneira, as necessidades destes últimos não pôde mais ser vista pelo produtor e a indústria, fato que permitiu uma falta de freio na produção e a ausência de regras.

O segundo exemplo, do mesmo modo, trata do surgimento da indústria e das rápidas mudanças provocadas nas relações entre operário e empregador. O homem, que até então trabalhava em pequenas oficinas, passou a trabalhar em manufaturas, vivendo um novo estilo de vida, longe da sua família e separado do próprio patrão, muitas vezes sendo substituído por máquinas. Devido a essas transformações súbitas, não houve tempo suficiente para equilibrar os interesses nos conflitos que surgiam, nem formar uma nova organização, o que, conforme Durkheim, gerou anomia.

4.2 Suicídio anômico, perturbações da ordem coletiva e forma anormal do crime

Aplicando as regras do método sociológico, Durkheim afasta as explicações psicológicas do fenômeno do suicídio e lhe atribui uma causa que é externa ao indivíduo, ou seja, que possui um caráter predominantemente social. O autor analisa o fato não meramente como acontecimentos particulares e pontuais dentro de uma coletividade, mas sim como um todo, observando os suicídios ocorridos em uma determinada sociedade, ao longo de um específico período de tempo (DURKHEIM, 2000).

Durkheim (2000, p.14) define suicídio como qualquer “caso de morte que resulta direta ou indiretamente de um ato positivo ou negativo, realizado pela própria vítima e que ela saiba que produziria esse resultado”. Isto significa dizer que o suicídio, na visão dele, além de ser um ato tomado conscientemente, é uma ação comissiva ou omissiva produzida pela vítima, que pode ter uma relação de casualidade imediata ou mediata com o indivíduo. Por exemplo, uma pessoa pode matar a si mesma através

de uma abstenção, como uma greve de fome, ou se expondo à uma conduta violenta realizada por terceiros.

O suicídio é, portanto, um ato que conscientemente parte do indivíduo mas tem sua causa fora dele, na sociedade. Não é produto de causas extra-sociais, como fatores psíquicos, psicopatológicos ou ambientais; está relacionado sobretudo com a coesão social e os graus de integração e regulação do corpo coletivo. Baseado nisso, Durkheim classifica o suicídio em quatro tipos que podem ser entendidos dentro de duas dualidades: a primeira refere-se à uma escassez ou excesso de integração social, correspondendo ao suicídio egoísta e ao suicídio altruísta, respectivamente; e a segunda é relacionada à existência de uma maior ou menor regulação dos indivíduos, que diz respeito aos denominados suicídio fatalista e suicídio anômico.

O suicídio egoísta é assim designado porque faz referência à um processo de individualização descomedido, que desconecta a pessoa da vida social e a faz se sentir isolada do grupo (DURKHEIM, 2000). É o caso em que a personalidade individual tende a se sobrepor à personalidade coletiva, tendo em vista o enfraquecimento de grupos a que pertence o sujeito, como por exemplo a família e a igreja (DURKHEIM, 2000). Frisa-se, contudo, que a individualização somente é um problema para Durkheim quando ela se torna excessiva e às custas do eu social, não sendo considerada algo ruim em seu estado normal (DURKHEIM, 2000).

Já o suicídio altruísta é o oposto do suicídio egoísta. Nesse segundo tipo, a personalidade coletiva se torna muito mais forte do que a individual e a problemática reside em uma individualização fraca e uma integração social excessiva. Aqui, o homem se sacrifica devido à essa integração intensa. O suicídio altruísta, portanto, é mais comum para os povos primitivos, visto que possuem uma moral coletiva mais forte e seus membros são mais semelhantes entre si (DURKHEIM, 2000). Exemplos dessa espécie de suicídio são casos em que o homem tira sua própria vida porque se encontra muito doente ou com idade avançada, devido à um senso de honra e de dever ante a sociedade (DURKHEIM, 2000). Exemplos que ocorrem nas sociedades contemporâneas são aqueles atos suicidas cometidos por mártires cristãos ou por alguns oficiais, devido ao espírito militar no qual encontram-se submersos (DURKHEIM, 2000).

O terceiro tipo de suicídio, por sua vez, é o denominado fatalista. Este é justificado pelo estabelecimento de uma grande opressão sobre o indivíduo, que vê suas vontades violentamente reprimidas por um regramento excessivo (DURKHEIM,

2000). Ele acontece, por exemplo, entre pessoas que vivem sob domínios materiais ou morais sufocantes, como os escravos (DURKHEIM, 2000).

O suicídio anômico, por fim, é justamente aquele que ocorre quando a disciplina sobre os indivíduos não é suficiente, ou seja, quando o regramento é frouxo ou inexiste. Situações anômicas são provocadas por grandes perturbações na ordem coletiva que deixam a sociedade, momentaneamente, sem a capacidade para regular os seus membros, não lhes impondo limites (DURKHEIM, 2000). Dessa maneira há uma propensão de aumento de suicídios, visto que muitos indivíduos se encontram sem orientação e, por conseguinte, sem perspectivas ou objetivos. Crises industriais e financeiras são exemplos de períodos em que pode surgir um estado anômico na sociedade, porque estes momentos forçam os homens à uma circunstância abaixo do que estavam acostumados (DURKHEIM, 2000). A sociedade, nessas épocas, precisa de tempo para ensinar as pessoas a reduzirem suas exigências e refazer sua moral, o que resulta, enquanto isso, em um período sem disciplina (DURKHEIM, 2000).

Durkheim (2000, p. 320) frisa, contudo, que os momentos de crises maléficas não são os únicos a provocarem anomia e abalos morais, mas também tempos de crises de prosperidade:

> O que homem tem de característico é que o freio ao qual está submetido não é físico, mas moral, ou seja, social. Ele recebe a lei não de um meio material que se lhe impõe brutalmente, mas de uma consciência superior à sua e cuja superioridade ele sente. Porque a maior e a melhor parte de sua vida ultrapassa o corpo, ele escapa ao jugo do corpo, mas é submetido ao da sociedade. Só que, quando a sociedade é perturbada, seja por uma crise dolorosa ou por transformações favoráveis mas por demais repentinas, ela fica provisoriamente incapaz de exercer essa ação; e daí provêm as bruscas ascensões da curva de suicídios...

Mudanças muito repentinas que rearranjem profundamente o corpo social podem desequilibrar a sociedade e gerar anomia. Assim, as denominadas crises de prosperidade, isto é, momentos súbitos de transformações sociais benéficas, também influenciam o aumento de números de casos de suicídio. Durkheim (2000) explica, por exemplo, que um período de desenvolvimento pode favorecer determinada classe social, o que aumentaria suas exigências e estimularia nas pessoas insaciáveis e constantes ambições diante de melhores possibilidades. Além disso, tornaria os homens menos submissos à qualquer tipo de regramento justamente quando este está em falta. Dessa maneira, a insatisfação frequente levaria-os ao suicídio.

Para o autor, essa situação de insatisfação em ambas as crises ocorre porque deve existir uma proporcionalidade entre as necessidades do ser humano e os meios para satisfazê-las, logo, se houverem muitas necessidades que não podem ser saciadas, haverá também um conflito contínuo entre esses polos.

Nesse sentido, Durkheim chega à conclusão de que a sociedade, na sua época, vivia um estado crônico de anomia em relação ao mundo do comércio e da indústria. Isso, para ele, se devia ao fato de que a indústria com o tempo passou a se libertar das regulamentações e tornou-se um fim supremo da sociedade, e não mais um meio. Dessa forma, os desejos e as paixões relacionadas à indústria e ao comércio ficaram cada vez mais livres:

> A realidade parece não ter valor em comparação com o que as imaginações febris vislumbram como possível; desligamo-nos dela, portanto, mas para nos desligar do possível quando, por sua vez, ele se torna realidade. Temos sede de coisas novas, de prazeres ignorados, de sensações inominadas, mas que perdem todo o sabor assim que se tornam conhecidas. (DURKHEIM, 2000, p. 325).

Durkheim defende que, dentro da sua lógica de diferenciação entre fenômenos normais e patológicos, uma taxa moderada de suicídios não é problemática, nem mórbida. A individualização, o espírito de renúncia e o amor pelo progresso podem resultar em suicídios que ocorrem dentro de determinados limites, os quais mudam de acordo com cada sociedade, em um certo período de tempo (DURKHEIM, 2000). Não ultrapassados esses limites, o suicídio é algo normal.

Do mesmo modo também é considerada a questão da criminalidade. Em seus critérios para identificar a normalidade de um fato social, Durkheim (2007) considerou o crime como um fenômeno normal, visto que além de ser encontrado em todas as sociedades (mesmo que de formas diferentes), ele também está relacionado às condições de toda vida coletiva. Apesar de ser entendido como uma conduta que ofende certos sentimentos coletivos (e que é definido pela consciência coletiva), o crime tem a capacidade de igualmente fortalecer esses mesmos sentimentos por meio da reação social que gera, o que ajuda a consolidar o pensamento geral sobre eles e a própria consciência comum. O crime é, portanto, regular e útil. Isso, porém, não significa dizer que não deva ser repreendido. A repreensão ao crime é tão normal quanto ele próprio. Inclusive, a criminalidade pode existir em formas patológicas.

O problema dela reside justamente nessas suas formas anormais, instaladas quando quebra determinados limites, os quais podem estar relacionadas a

perturbações da ordem social e estados de anomia, já que “qualquer afrouxamento anormal do sistema repressivo tem por efeito estimular a criminalidade e lhe conferir um grau de intensidade anormal” (DURKHEIM, 2000, p. 473). Sobre essa quebra de limites, Durkheim (2007, p. 67) esclarece bem que:

> Certamente pode ocorrer que o próprio crime tenha formas anormais; é o que acontece quando, por exemplo, ele atinge um índice exagerado. Não é duvidoso, com efeito, que esse excesso seja de natureza mórbida. O que é normal é simplesmente que haja uma criminalidade, contanto que esta atinja e não ultrapasse, para cada tipo social, certo nível...

Portanto, o crime é normal e em determinados patamares até desejável, pois tem uma função. Ele somente é patológico no momento em que excede em quantidade, quando existe criminalidade de forma demasiada, o que pode acontecer, por exemplo, quando se existe uma conturbação social significativa.

4.3 Ênfase cultural e tipos de adaptações individuais

A teoria da anomia desenvolvida por Merton, apesar de ser grandemente influenciada pelo pensamento de Durkheim, assumiu contornos diferentes daqueles propostos pelo autor francês, vez que observando a sociedade norte-americana do século XX ela se atém na análise da estrutura social e, principalmente, dos valores culturais considerados predominantes.

O sociólogo americano, em explicita oposição às teorias e doutrinas inspiradas por Freud (que defendem que a ordem social é um instrumento para lidar com as tensões e os instintos advindos do impulsos biológicos do homem), critica a ideia de que o desvio de comportamento somente surge da natureza inconformista arraigada no ser humano, que por vezes se sobrepõe ao controle social (MERTON, 1970). Isso porque ele acredita que a sociedade tem um papel muito mais atuante na geração de motivações que induzam o desvio e o crime. De acordo com as próprias palavras de Merton (1970, p. 191): “Se a estrutura social restringe algumas disposições para agir, [pode] cria[r] outras”.

Antes, porém, de entender como são criadas essas disposições para agir, é relevante distinguir a estrutura social da estrutura cultural. Para Merton (1970), a estrutura social é compreendida como um conjunto ordenado de relações sociais em que os indivíduos fazem parte de diferentes formas, enquanto que a estrutura cultural é a reunião dos valores normativos que guiam o comportamento normal das pessoas

na sociedade. A diferenciação dessas estruturas é fundamental para assimilar a relação entre o que o autor chama de objetivos culturalmente definidos e normas institucionalizadas.

Em toda sociedade existe uma cultura e propósitos que foram traçados por essa própria cultura para serem atingidos pelos indivíduos. São objetivos, ou metas desejáveis, consideradas legítimas para todos alcançarem, se constituindo como verdadeiras referências aspiracionais da sociedade (MERTON, 1970). Não existe somente uma meta cultural, há uma hierarquia de valores mais ou menos organizada, e nem todas elas são relacionadas aos impulsos biológicos do ser humano, muito menos definidas por eles (MERTON, 1970).

Também existe na sociedade as normas institucionalizadas, que são regulamentos de procedimentos que definem e controlam os meios usados para se chegar aos objetivos culturais, sendo eles presentes através dos costumes e das instituições sociais (MERTON, 1970). Essas normas institucionalizadas são consideradas legítimas e se diferenciam de procedimentos que, embora sejam até mais eficientes em alcançar as metas, são entendidos como ilegítimos dentro da sociedade (MERTON, 1970).

Para haver equilíbrio, as metas culturais devem ser associadas equivalentemente com os meios institucionalizados, formando uma sociedade integrada e razoavelmente estável, mesmo que seja sujeita à transformações. Do contrário, a ênfase cultural variando em relação à ênfase dada sobre os meios legítimos, pode acabar gerando uma tensão muito forte entre esses dois elementos (MERTON, 1970). A anomia ocorreria então nesse momento, “...quando há uma disjunção aguda entre as normas e metas culturais e as capacidades socialmente estruturadas dos membros do grupo em agir de acordo com as primeiras” (MERTON, 1970, p. 237). A tensão, portanto, conduziria ao rompimento das normas ou ao seu descaso (MERTON, 1970). Desse modo, contraditoriamente, a sociedade e sua cultura contribuiriam para que surjam comportamentos que estão em oposição aos seus próprios valores (MERTON, 1970).

Merton (1970) trata especificamente de um tipo de sociedade que sofre com a supracitada tensão, ela é caracterizada pela ênfase pesada sobre alguns objetivos culturais sem semelhante ênfase sobre os caminhos institucionalizados. O autor identifica a sociedade americana da sua época como sendo esse tipo de sociedade, visto que, envolta pela cultura do *american dream*, coloca ênfase

excessiva na ascensão social e no êxito monetário, isto é, no ganho de dinheiro e de riqueza, e não são consideradas a situação inicial ou posição social do indivíduo.

Nessa conjuntura, os americanos são bombardeados por variados meios pelos preceitos culturais que fortalecem o direito e o dever de atingir as metas de sucesso econômico, sendo eles reforçados e intensificados, inclusive, por organismos importantes como a família, a escola e o local de trabalho (MERTON, 1970). Além desses organismos, o reforço cultural também é feito por meios de comunicação e formas de entretenimento, como menciona o sociólogo:

> É apenas o fato de que no púlpito e na imprensa, na ficção e nos filmes cinematográficos, no decurso da educação formal e da socialização informal, nos variados meios de comunicação públicos e particulares que atraem a atenção dos norte-americanos há uma ênfase relativamente acentuada sobre a obrigação moral, assim como sobre a possibilidade efetiva de lutar pelo êxito monetário e de consegui-lo. (MERTON, 1970, p. 242).

Merton (1970) adverte, contudo, que não apenas a grande ênfase no sucesso econômico gera tensão e tem o potencial de atenuar a conformidade com as normas condutoras do comportamento das pessoas mas também qualquer outra ênfase cultural extrema.

Um dos pontos centrais da teoria de Merton se encontra justamente na indicação dos tipos de adaptação das pessoas (que estão em distintas posições na estrutura social) aos valores culturais excessivamente enfatizados e à tensão gerada disso. As cinco formas de adaptações individuais são: a conformidade, a inovação, o ritualismo, o retraimento e a rebelião. Essas reações, porém, não são imutáveis e podem se converter em outra alternativa a depender das mudanças de âmbitos de atividades sociais assumidas pelas pessoas (MERTON, 1970). Ademais, essas categorias não devem ser confundidas com a personalidade, dado que são formas de comportamento surgidas de determinadas circunstâncias (MERTON, 1970).

A primeira delas, a conformidade, é a reação mais comum dentro de uma sociedade equilibrada, pois nessa situação o indivíduo aceita tanto as metas culturais quanto os caminhos institucionais, sendo este o comportamento modal, a referência que contrasta com os outros quatro tipos de reações, que são comportamentos divergentes (MERTON, 1970). O indivíduo conformado não tem problemas com as normas e verdadeiramente acredita e busca alcançar os objetivos culturais.

Já a segunda maneira de adaptação é a inovação. Esse tipo de reação é caracterizada pela incorporação no indivíduo das aspirações culturais ao mesmo

tempo em que há a rejeição aos procedimentos institucionais (MERTON, 1970). Neste caso, a pessoa é considerada inovadora porque busca meios novos, e proibidos, para chegar aos propósitos culturalmente definidos, ou ao menos alcançar um simulacro de sucesso. Portanto, ela adota caminhos ilícitos, propriamente criminosos, os considerando mais eficientes. Merton adverte, porém, que em sua teoria os comportamentos divergentes, ou desviados, não são necessariamente disfuncionais para o grupo e que a inovação é normal e, por exemplo, pode desencadear o surgimento de melhores padrões institucionalizados. O problema, assim, acontece quando a inovação é decorrente da ênfase cultural intensa.

Ainda sobre o comportamento inovador, é relevante apontar que Merton identifica que as camadas inferiores da sociedade sofrem maior pressão das tensões existentes entre metas e meios, já que as oportunidades para este grupo são mais distantes, o que induziria o comportamento desviante. Simultaneamente, os mesmos valores culturais que induzem tais reações na sociedade americana, também são aqueles que inspiram admiração aos homens bem sucedidos que utilizam de meios astutos, e até criminosos, nos negócios.

Por sua vez, a terceira forma de adaptação individual é oposta ao comportamento inovador. O ritualismo é a reação definida pelo abandono dos propósitos culturais, ou redução do interesse neles, ao mesmo tempo em que há a manutenção do apego às normas institucionalizadas (MERTON, 1970). A forte tensão acaba por gerar medo, ansiedade, frustações, senso de perigo e desconfiança, induzindo uma adaptação em que o indivíduo é desestimulado, desesperançado. Nessa situação, contudo, não são adotados comportamentos criminosos, diferente da inovação. Merton (1970) esclarece, inclusive, que a sua teoria aponta formas diferentes de comportamento divergente que podem estar bastante longe de caracterizar violações legais.

O próximo tipo de comportamento desviado é aquele em que existe uma renúncia tanto das metas culturais quanto dos meios e, devido a isso, é chamado de retraimento. Os indivíduos que se adaptaram dessa maneira não se ajustam às normas institucionalizadas e são provavelmente a categoria mais antissocial porque, em muitos casos, se encontram excluídos. Merton (1970, p. 227) afirma, por exemplo, que “pertencem a esta categoria algumas das atividades adaptativas dos psicóticos, artistas, párias, proscritos, errantes, mendigos, bêbados crônicos e viciados em

drogas”. O indivíduo retraído é relacionado à uma fuga das demandas sociais, exprimindo seu derrotismo, quietismo e resignação (MERTON, 1970).

O quinto e último modo de adaptação é a rebelião. Nesse tipo de reação ocorre a rejeição de ambos os objetivos culturais e os meios institucionalizados. No entanto, o indivíduo não assume uma postura retraída e sim de denúncia aos valores vigentes: os rebeldes desejam substituir as atuais metas e normas, vez que as consideram ilegítimas, e buscam mudanças sociais. Interessante dizer que para Merton (1970) se a rebelião está ligada a apenas alguns elementos pequenos de uma comunidade, ela pode produzir subgrupos na sociedade. Se, contudo, a rebelião é endêmica em parcela significativa da sociedade, pode desencadear uma grande revolução, transformando a sua estrutura normativa e social.

5 INTERLIGAÇÕES ENTRE A TEORIA DA ANOMIA E O CONTEXTO DOS CRIMES INFORMÁTICOS NO BRASIL

A teoria da anomia trata de quadros ou situações em que impera a ausência de normas. Durkheim as identificou na sociedade de sua época, bem como Merton as reconheceu nas estruturas da sociedade norte-americana. Sabendo disso, para a aplicação da teoria ao contexto da realidade brasileira relacionada à criminalidade cibernética, é necessário tanto observar algumas características do meio digital, e as possibilidades que proporciona, quanto voltar o olhar para a sociedade brasileira, em seu aspecto social e jurídico.

5.1 Revolução informacional e criminalidade informática

Em termos históricos a criminalidade cibernética é evidentemente um fenômeno bastante atual, o qual somente pôde surgir devido à criação e ao desenvolvimento de ferramentas e tecnologias específicas, sendo elas as propulsoras de profundas transformações sociais e econômicas. Essas transformações são semelhantes àquelas observadas por Durkheim no século XIX, que estavam relacionadas com o surgimento de novas invenções, da indústria e da expansão dos mercados. Analisando o cenário daquela época, Durkheim identificou uma súbita e intensa perturbação na ordem coletiva, que seria capaz de provocar a falta de regulamentações, ou o afrouxamento das normas, ainda que transitoriamente.

Realizando uma correlação com o contexto dos crimes informáticos, é possível afirmar que as mudanças geradas pelo recente crescimento da tecnologia, que se iniciou com a terceira revolução industrial, criou um período que, de fato, não possuía razoáveis regramentos e legislações que disciplinassem o meio digital, vez que o seu surgimento e desenvolvimento aconteceram de uma forma muito acelerada.

A terceira revolução industrial, ou a revolução técnico-científica-informacional, como é mais conhecida, corresponde à um período de rápido crescimento da tecnologia e do conhecimento científico, no qual se destacou áreas como a eletrônica, as telecomunicações e a informática. Nesse período de avanço, as tecnologias da informação e da comunicação não apenas passaram a ser essenciais e partes integrantes do desenvolvimento de muitos outros campos da ciência, como

também transformaram de forma positiva o trabalho, a economia, a cultura, as relações sociais e o próprio modo como a realidade é entendida.

No contexto dessas grandes mudanças, aponta-se que foi a partir da década de 70 que a convergência de diferentes campos de estudo e o aprimoramento de invenções possibilitaram a otimização do computador e a criação da internet (CASTELLS, 1999). Até então os computadores existentes eram máquinas primitivas, grandes, com pouca capacidade de processamento e que não tinham uma operação simples, bastante diferente dos aparelhos que existem atualmente (CASTELLS, 1999). Porém, esse cenário começou a mudar com a invenção do microprocessador em 1971, o que representou um grande avanço para microeletrônica e permitiu o surgimento do microcomputador em 1975, com um maior poder de processamento de informações (CASTELLS, 1999). Por volta da mesma época a empresa Microsoft iniciou a produção de sistemas operacionais para microcomputadores e a fibra ótica foi produzida em escala industrial, invenções que juntas foram fundamentais para a consolidação da base do que hoje entendemos como o computador pessoal (CASTELLS, 1999).

A internet, por sua vez, foi consequência da convergência de diferentes interesses, nos quais se incluíram principalmente interesses militares e acadêmicos. Ela teve origem no âmbito dos trabalhos da Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos, e tinha a intenção inicial de ser um sistema de comunicação invulnerável a ataques nucleares (CASTELLS, 1999). A primeira rede de computadores criada, denominada ARPANET, começou a funcionar em 1969 e foi ligada à algumas universidades e centros de pesquisa (CASTELLS, 1999). Anos mais tarde, a rede que surgiu de um conjunto de pesquisas acadêmicas e esforços à parte, além de ter sido atrelada ao *world wide web* em 1990 (sistema que organizou os sítios da internet com base em suas informações), também recebeu maior funcionalidade com a criação dos primeiros navegadores *web*, por volta dos anos de 1993 e 1994 (CASTELLS, 1999).

No Brasil, a primeira conexão com a internet aconteceu em um evento isolado no ano de 1988, através de uma parceria entre a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e o *Fermi National Accelerator Laboratory* (Fermilab), um dos mais importantes laboratórios de pesquisa dos Estados Unidos (VIEIRA, 2018). No ano seguinte, em 1989, contudo, com a criação da Rede Nacional de Pesquisa (RNP), iniciou-se a construção de uma grande infraestrutura de cabos

para dar suporte à internet no país, sendo também espalhados pontos de conexão pelas principais capitais e disseminado o acesso à rede para universidades, fundações de pesquisa e órgãos do governo (VIEIRA, 2018).

Em 1995, com a eleição de Fernando Henrique Cardoso e a aplicação de uma agenda política que incluía a desestatização do setor de telecomunicações, afastou as intenções da Embratel (que na época era um braço da Telebrás) de abranger sozinha todo o mercado da internet no Brasil (VIEIRA, 2018). Nesse mesmo ano, o Ministério das Comunicações e o Ministério da Ciência e Tecnologia estabeleceram que o oferecimento do serviço de internet ao usuário final era de responsabilidade da iniciativa privada, cabendo às operadoras estatais apenas a obrigação de fornecer infraestrutura e recursos a fim de possibilitar a montagem dos provedores de acesso. (VIEIRA, 2018). O governo federal então criou em 1995 o Comitê Gestor da Internet que, dentre outras atribuições, tinha a responsabilidade de acompanhar a disponibilização da rede no país (VIEIRA, 2018). O ano de 1995, portanto, pode ser considerado o marco inicial da internet comercial no Brasil (VIEIRA, 2018).

Diante disso, percebe-se que a grande popularização da internet, e demais aparelhos como computadores e celulares, começou de fato na década de 90, ou seja, a pouquíssimo tempo. É assim compreensivo que o entendimento dessa recente realidade e o ajustamento à ela não seja imediato e exija tempo. Esta é, inclusive, uma situação que praticamente todas as nações precisam lidar quando se trata de tecnologias: o descompasso temporal entre novas conjunturas e a feitura da lei ou outros tipos de normas que as regule.

Contudo, mesmo compreendendo isso, não se pode negar que no Brasil demorou para entrar em vigor normas que tratavam especificamente de temas relacionados à essas novas tecnologias. Antes de 2012 é possível dizer que existia quase uma completa ausência de normas sobre a temática, embora houvesse a previsão de crimes informáticos impróprios e mistos. Foi no ano de 2012 que surgiram a Lei n° 12.735 e a Lei Carolina Dieckmann, que tipificou os primeiros crimes cibernéticos próprios. Em 2014, foi aprovado o Marco Civil da Internet e em 2018, a Lei Geral de Proteção de Dados. Já em 2021, por conta principalmente da pandemia de covid-19, foi aprovada a Lei n° 14.155, que se voltou para o furto mediante fraude eletrônica e o estelionato. Ainda, recentemente projetos de lei sobre o uso de sistemas de inteligência artificial apareceram, como o PL n° 2338/2023, de iniciativa do senador

Rodrigo Pacheco. Dessa forma, o Brasil começa a se envolver mais nessas questões. Nesse sentido, a adesão à Convenção de Budapeste, mesmo que tardiamente e com questões ainda a serem trabalhadas (como foi mencionado em capítulo anterior), representa um passo significativo no combate aos delitos virtuais.

Para além disso tudo, é necessário também se voltar para a compreensão de que o ambiente cibernético possui qualidades próprias, cujas particularidades acabam por serem aproveitadas pela criminalidade. Nesse esteira, Sydow (2015) enumera algumas características da delinquência informática, sendo elas a: interatividade, mobilidade, anonimidade, conectividade, globalização, velocidade, disponibilidade, ubiquidade, não territorialidade, conversabilidade entre aparelhos e a divisibilidade, pluralidade e intangibilidade de dados. Por causa desses e outros atributos os criminosos passaram a ter acesso à informações, ferramentas, serviços e comunicações de forma imediata e independente de distâncias geográficas, com aparelhos que facilmente podem ser transportados. Ademais, ganharam a opção de interagir com os outros e praticar atos de forma anônima, bem como passaram a poder assumir simultaneamente diferentes perfis virtuais, ser diferentes personas.

Em verdade, o mundo cibernético pode ser visto não apenas como um fator que transformou a realidade, mas como uma realidade diferente por si só, vez que ao mesmo tempo em que compartilha práticas, linguagens, culturas e símbolos com o ambiente *off-line*, também criou um espaço único com seus próprios significados e cultura. Desse modo, o contexto em que vivemos, há a coexistência da realidade física e da realidade virtual com uma realidade que é mista, que está entre as duas.

Essas citadas características e cenário, porém, por si só não são maléficos para a sociedade, pelo contrário, são grandes vantagens que, como já foi mencionado, mudaram positivamente a forma como as pessoas se relacionam e como acontece várias dinâmicas sociais, econômicas e culturais. A partir da visão de Durkheim, é possível considerar que as mudanças que aconteceram, e ainda acontecem, devido ao avanço das tecnologias da informação e da comunicação são grandes perturbações na ordem coletiva, porém são crises advindas da prosperidade. A telemedicina, o trabalho remoto, a facilitação do comércio, o melhor entrosamento dentro de empresas e de setores públicos, a convergência rápida de novos conhecimentos científicos, a desburocratização de serviços, enfim, uma infinidade de

melhoramentos foram introduzidos por causa das tecnologias da informação e da comunicação.

Dessa maneira, quanto ao ambiente cibernético, se infere que não somente está identificada a rapidez da perturbação da ordem coletiva, mas também seu caráter intenso e positivo. Tudo isso acaba por gerar um estado de anomia, isto é, a ausência de normas ou o afrouxamento delas (dado que no meio virtual há uma percepção, por parte de muitos criminosos, de que as normas não serão aplicadas, o que aumenta a confiança na impunidade). Primeiro porque a sociedade, na maioria dos casos, não tem a capacidade de regular instantaneamente um contexto sem precedentes na história, segundo porque, devido às características da realidade cibernética, explorada pelos criminosos, existe uma facilidade na execução delitos (somada à dificuldade de investigação) e, consequentemente, uma sensação de impunidade. Explicando a abordagem sociológica do suicídio de Durkheim, Sabadell (2013, p. 78) elucida bem os espaços digitais nesse sentido:

> ...quando se criam na sociedade “espaços anômicos”, ou seja, quando um indivíduo ou um grupo perde as referências normativas que orientavam a sua vida, então enfraquece a solidariedade social, destruindo-se o equilíbrio entre as necessidades e os meios para sua satisfação. O indivíduo sente-se “livre” de vínculos sociais, tendo, muitas vezes, um comportamento antissocial ou inclusive autodestrutivo.

Associado assim os crimes cibernéticos à um contexto anômico produzido pelo surgimento de novas tecnologias, agora questiona-se sobre a normalidade do crime informático sob a perspectiva de Durkheim. Teriam os crimes virtuais já assumido uma forma patológica? Para o sociólogo, a existência da criminalidade na sociedade é algo normal e o que a faz patológica é quando ela atinge níveis exagerados. Sabendo disso, se pode afirmar que sim, no Brasil este nível já foi alcançado, tendo em vista a tendência cada vez maior de crescimento desse tipo de criminalidade.

Corroborando essa posição, aponta-se que o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), registrou o recebimento de 457.270 notificações voluntárias de incidentes de segurança em sistemas computacionais, apenas em 2021, e 481.652 notificações, em 2022, reportados por Grupos de Segurança e Resposta a Incidentes (CSIRTs), administradores de redes e usuários da internet (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE

INCIDENTES DE SEGURANÇA NO BRASIL, 2023). Por seu vez, a *Fortinet*, empresa multinacional da área de segurança cibernética, através do seu laboratório de pesquisa de ameaças, o *FortiGuard Labs*, divulgou a informação de que o Brasil sofreu 31,5 bilhões de tentativas de ataques cibernéticos entre janeiro e junho de 2022, e que esse foi um aumento de 94% em relação ao mesmos meses do ano de 2021, sendo o segundo país mais visado da América Latina, o que o deixa atrás apenas do México (FORTINET, 2022).

À vista disso, se conclui que a anomia, da maneira que foi concebida por Durkheim, encontra-se caracterizada no meio informático: existe uma perturbação da ordem, súbita e profunda, e o crime que se surgiu a partir dela toma proporções ainda longe de serem controladas. É correto afirmar que será preciso um determinado tempo para compreender cada nova conjuntura que a tecnologia induzirá com suas inovações, porém é incerto assegurar que se trata de uma crise de prosperidade transitória ou não. Talvez, em reflexão semelhante feita por Durkheim, já vivemos em uma situação anômica crônica quanto às tecnologias da informação e da comunicação, e talvez isto esteja bastante associado com às ênfases culturais que existem no meio digital.

5.2 Adaptações individuais na realidade cibernética

A teoria da anomia de Durkheim, assim como foi mencionado em capítulo anterior, surgiu antes da teoria desenvolvida por Merton, tendo influenciado a mesma. Ambos os pensamentos possuem pontos em comum, como a consideração do crime como algo normal dentro da estrutura social e a identificação de uma problemática apenas em circunstâncias sociais específicas. Apesar disso, as duas teorias possuem significativas diferenças, como é bem esclarecido por Díaz (2010, p. 370, tradução nossa):

> ...enquanto Durkheim via na “anomia” uma situação de crise transitória do poder social de regulação, devido à acelerada e desorganizada mudança social imposta pelo processo de industrialização, Merton define aquela como uma disfunção estrutural endêmica, crônica, estável, inerente a certo modelo de sociedade (a norte-americana), cujas contradições internas produzem uma tendência à mesma, que incide de modo desigual nos diversos grupos sociais.

Em sua explicação da anomia, Merton destaca a questão da ênfase cultural desenfreada em relação ao triunfo econômico como geradora de uma tensão que estimularia o desrespeito às normas.

Em correlação com a realidade cibernética, é possível afirmar que igualmente existe uma grande ênfase em relação ao sucesso monetário no ambiente virtual, mas não somente esse é um objetivo desejável na sociedade de hoje. O aumento das tecnologias e ferramentas de comunicações permitiram a modificação profunda da forma como as pessoas se relacionam e criaram uma exaltação exaustiva de diversas metas culturais, nas quais se pode incluir a riqueza, a fama, a ostentação, um perfil *online* impecável, um número cada vez mais alto de *likes* e de seguidores, a aparência ideal, o parceiro perfeito, o acesso à conteúdos, informações e serviços exclusivos ou restritos, dentre outras.

A sociedade brasileira, contudo, é tanto altamente desigual economicamente como é diversa em vários sentidos, havendo diferenças consideráveis, por exemplo, com relação à posição social e profissional, ao nível educacional, à fisionomia e à raça. Não é, portanto, surpreendente perceber que vários indivíduos se encontram muito distantes de atingir certos padrões e passam assim a adotar comportamentos adaptativos no meio cibernético, diante das pressões que recaem sobre eles.

Nesta lógica, para interligar os tipos de adaptações descritas por Merton aos comportamentos assumidos no âmbito digital, é preciso primeiro começar com a forma de reação mais básica, que é a conformidade. O comportamento conformista é aquele observado no usuário comum do ambiente cibernético, da internet e das redes sociais. Este indivíduo é o modelo de cidadão digital, agindo de maneira legal e ética. Se ele não alcançou os objetivos culturais, ainda acredita neles e crê que os alcançará. Portanto, não realiza atividades divergentes ou criminosas e geralmente é mais transparente em suas práticas virtuais. Se incluem nesse tipo de comportamento, inclusive, os profissionais da área de tecnologias da informação e os *hackers* éticos.

Já o indivíduo inovador, pressionado pela tensão da extrema ênfase cultural, realiza condutas criminosas cibernéticas para atingir alvos tanto dentro do mundo digital quanto fora. Os avanços tecnológicos, o aumento da disponibilidade de ferramentas digitais e o aprimoramento do conhecimento técnico proporcionam meios eficientes, embora não legítimos, de atingir as metas. Assim, práticas como ataques

hackers, invasões de sistemas, uso de *ransomware*, fraudes, furtos, *phishing* e pirataria ocorrem com mais facilidade e, consequentemente, maior incidência.

A forma de adaptação do ritualista, por sua vez, também pode ser observada no espaço cibernético. Ela é identificada no comportamento de indivíduos que são *low profile*, isto é, que assumem uma atitude discreta no meio digital. Geralmente eles fazem parte das redes e utilizam as ferramentas digitais nas suas atividades rotineiras, mas não estão engajados nas metas culturais, seja por desapreço, medo de exposição ou insegurança. Pessoas com idade mais avançada, idosos, também podem exibir uma atitude ritualista virtualmente, muitas vezes por conta de uma inabilidade em entender e lidar com as novas tecnologias, bem como devido à falta de interesse ou por causa, até mesmo, de alguma deficiência. Nesse sentido, ao relacionar gerações com alguns perfis de usuário de tecnologia, Pinheiro (2021, p. 187) apontou para um tipo formado por indivíduos que possuem mais idade, afirmando que:

> ...este perfil tem fobia a tecnologia. Aprendeu tudo na era do papel, do mundo mais físico e presencial. É da era do “cata milho” e da máquina de escrever. Em geral, tem dificuldade em usar ferramentas tecnológicas, não gosta de ter senha, não confia nas máquinas. Por isso, costuma passar a senha para outra pessoa realizar a tarefa, seja secretária, filho, colega. É um alvo fácil para engenharia social.

Por esses razões, a pessoa idosa, de maneira frequente, tende a ser uma vítima mais fácil de criminosos cibernéticos. Este fato é notado pelo aumento do número de notícias sobre golpes que lesam a terceira idade, o que impulsionou a alteração de algumas legislações para melhor proteger os idosos. É o caso das já citadas, em capítulo anterior, modificações trazidas pela Lei n° 14.155/21 no art. 155, §4°-C, inciso II, e no art. 171, §4°, que aumentam a pena se a ação for cometida contra idosos nos crimes de furto mediante fraude e estelionato.

Por seu turno, a quarta forma de adaptação individual, o retraimento, do mesmo modo pode ser encontrada no mundo digital. O comportamento do indivíduo retraído e suas atividades não necessariamente constituem práticas criminosas (apesar de poderem fazer parte de algum outro problema que atinge a estrutura social) mas têm o potencial de assumir rumos ilícitos. Os retraídos dentro do meio virtual, devido às frustações, ao isolamento (ou à sensação de isolamento), e à uma busca por fuga, podem engajar em comportamentos destrutivos, como o vício em jogos eletrônicos ou jogos de azar *online*, o consumo e a produção de pornografia (inclusive

pornografia infantil), a proliferação de discursos de ódio e a participação em grupos extremistas. Condutas e opiniões racistas ou misóginas, feitas por grupos como os denominados *incels* e *red pills*, além do apoio ao nazismo e à atividades violentas são exemplos do que acontece virtualmente.

Recentemente os casos de ataques ocorridos contra escolas no Brasil, praticados em sua maioria por crianças e adolescestes que acessam plataformas digitais as quais permitem esse tipo de conteúdo, colocaram novamente em evidencia o PL 2630/2020 ou, como é mais conhecido, o PL das *fake news*. O projeto pretende, dentre outros assuntos, tratar da regulação das plataformas para promover a transparência e a responsabilização das mesmas em relação à moderação de conteúdo, além de prevenir a proliferação de conteúdo falso ou manipulado. O texto do projeto, porém, ainda está sendo discutido, especialmente no que concerne à um possível órgão regulador que será necessário para atender as previsões legais, e se encontra envolto em diferentes interesses políticos e interesses de grandes empresas como o Google, o Meta e o Telegram.

Por fim, a última forma de adaptação individual, a rebelião, pode ser identificada no âmbito virtual, por exemplo, através da ação de ativistas cibernéticos, que são indivíduos ou grupos que defendem uma causa social ou cultural. Essa atividade, o cibertivismo, pode ser compreendido como:

> ...um processo de comunicação realizado por meio de codificações sígnicas, com base em tecnologias digitais, visando representar os objetivos, as necessidades e principais metas de grupos sociais, com o objetivo de causar mudanças conscientes e coletivas em hábitos de pensamento, de ação e de sentimento (RODRIGUES; PIMENTA, 2015).

O ativismo cibernético, porém, tem o potencial de aderir a métodos radicais e ilegais, como ações terroristas, a fim de realizar ataques *hackers* à sites de empresas e órgãos governamentais. Uma amostra disso foram as notícias de invasão dos sistemas das empresas Friboi e JBS, em 2017, bem como os ataques realizados contra o banco de dados do Ministério da Defesa, em 2018, pelo grupo Anonymous, e as ações contra o Tribunal Superior Eleitoral, em 2020. Sobre o assunto, no Brasil, aponta-se para existência da Lei 13.260/2016 que, em seu art. 2°, §1°, inciso IV, considera como ato terrorista a sabotagem ou a apoderação, por meio de mecanismos cibernéticos, do controle de meios de comunicação ou transporte, de instituições de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações militares ou relacionadas à energia, petróleo

e gás, além de instituições bancárias e sua rede de atendimento (BRASIL, 2016). Para além disso, as condutas *online* de grupos de extremistas políticos e religiosos também podem ser considerados como uma adaptação rebelde.

Finalmente, diante de tudo o que foi exposto, contudo, é importante esclarecer que a teoria da anomia, tanto de Durkheim quanto de Merton, não explica todas as formas de comportamento criminoso informático, e o recorte que propõe ignora relevantes aspectos individuais, psicológicos e sociais, focando, portanto, em uma utilização teórica. Para um entendimento mais completo dos crimes digitais é necessário uma análise conjunta com outras áreas do conhecimento, bem como é preciso considerar outras teorias criminológicas. A despeito disso, a utilização da teoria e de sua abordagem macrossociológica e funcionalista colabora para a melhor compreensão do contexto da criminalidade cibernética no Brasil, através de uma visão abrangente, que coloca seu ponto de partida na sociedade e em suas estruturas.

6 CONCLUSÃO

Ao final desta pesquisa, conclui-se que, sob a perspectiva das teorias de Émile Durkheim e Robert Merton, o contexto dos crimes cibernéticos no Brasil é anômico.

O estudo da anomia por Durkheim foi realizado através de dois pontos de vistas abordados em suas obras. O primeiro deles é explicado nas formulações sobre a sociedade moderna e a divisão do trabalho. A coesão ocorrida por meio da solidariedade orgânica, que é relacionada às sociedades mais atuais, tem por fundamento a divisão do trabalho, vez que quanto mais o trabalho vai se especializando, mais o indivíduo e os órgãos sociais dependem do grupo, e o grupo deles. Existe, portanto, uma interdependência que gera a integração social. A divisão do trabalho, além de útil, tem o papel de produzir um efeito moral.

Porém, quando os órgãos sociais não têm um bom contato, ou esse contato não ocorreu por tempo suficiente, pode acontecer de produzir uma situação em que os regulamentos enfraqueçam, pois não estão em consonância com a divisão do trabalho, ou nem existam. Esta é a anomia. A divisão do trabalho anômica pode ser provocada por mudanças repentinas e bruscas, que afetam os órgãos e as relações sociais, que tocam no fenômeno da densidade moral.

A segunda explicação de Durkheim para a anomia é dada nos seus estudos sobre o suicídio. Nesta situação, o indivíduo que comete o suicídio anômico é aquele que tira a própria vida porque encontra-se sem disciplina, porque vive em um momento em que faltam regras, ou que elas não têm força suficiente. Aqui, diante das desproporções entre suas necessidades e os caminhos para as satisfazer, a pessoa sofre com a falta de um freio moral. Sob essa perspectiva, novamente Durkheim aponta que a causa para a anomia pode ser uma grande perturbação na ordem coletiva. E independe se esta perturbação é maléfica ou benéfica, o fato é que interferiu na proporção entre necessidades e seus meios.

Tendo sido realizada interligações entre esses pensamentos e o contexto dos crimes digitais no Brasil, foi verificado que o surgimento repentino e intenso das tecnologias da informação e da comunicação a partir da terceira revolução industrial foi e continua sendo uma grande mudança social positiva, mas que levou à anomia. A conclusão a que se chegou é aparentemente contraditória: tecnologias que acentuam as relações sociais afetam a integração social e a moral. O que foi

entendido, porém, é que, em virtude das características específicas do ambiente cibernético, e das ferramentas e dos meios que elas proporcionaram para as pessoas, cresceu o potencial de deturpação dos comportamentos. O indivíduo pode ser anônimo ou não, pode ser mais de uma pessoa, pode acessar informações extremamente específicas, pode ultrapassar distâncias físicas, pode ser membro nativo de realidades culturais que coexistem e se sobrepõem, sem mencionar uma infinidade de outras possibilidades.

Um dos sintomas dessa anomia é o aumento excessivo do índice de criminalidade, como foi apontado também na pesquisa, tendo em vista as informações do crescente número de delitos virtuais. Para Durkheim a existência da criminalidade em uma sociedade é algo normal e até funcional, há crimes em todas os grupos sociais. O problema, para ele, reside no aumento excessivo do índice de crime, quando este atinge determinado nível se torna anormal. E, por certo, essa anormalidade, forma patológica do crime, pode ser causada por fortes perturbações sociais.

Na análise de Merton, por sua vez, diferente do que propôs Durkheim, foi central a ideia das ênfases culturais exageradas. Durkheim indicou a desproporção entre necessidades e meios, enquanto Merton apontou para a desproporção entre metas culturais e meios institucionalizados. O problema residia nas pressões que eram geradas pela grande exaltação dos objetivos culturalmente definidos, o que permitia o aparecimento de modos de adaptações individuais para lidar com essas tensões. O comportamento conformista, inovador, ritualista, retraído e rebelde surgem disso.

Associada essa perspectiva com a realidade do ambiente digital, ficou demonstrado que as ênfases culturais desse meio, dentro de uma estrutural social desigual como é a brasileira, produzem tensões suficientes para também induzir modos de adaptação no ciberespaço, o que resultou em explicações para a prática de alguns tipos de crimes e o melhor entendimento de dinâmicas sociais *online*.

Por fim, apesar de ter sido reconhecida, sob a visão de Durkheim e Merton, a anomia quanto aos crimes informáticos no Brasil, não se pode dizer o mesmo quanto à situação recente do ordenamento jurídico brasileiro sobre o tema. A legislação já prevê alguns delitos informáticos próprios e impróprios, bem como, com a adesão à Convenção de Budapeste, é reforçada, vez que o tratado possibilita o começo de uma

melhor delimitação e interpretação de conceito e termos, além de uma orientação para a tipificação de novas condutas e uma cooperação internacional facilitada.

Em suma, esta monografia explorou as interligações entre a teoria da anomia de Durkheim e Merton e os crimes cibernéticos no Brasil. Ao longo da pesquisa, foi destacada a complexidade desse tipo de criminalidade, que envolve ampla gama de atividades ilícitas, as quais podem ter parte de sua origem explicada através do entendimento da estrutura social, da cultura digital e da nova realidade que se impõe pelo avanço das tecnologias da informação e da comunicação.

REFERÊNCIAS

ARNAUDO, Daniel. **O Brasil e o Marco Civil da Internet**: O Estado da Governança Digital Brasileira. Instituto Igarapé, [*s. l.*], Artigo Estratégico 25, abr. 2017. Disponível em: https://igarape.org.br/marcocivil/assets/downloads/igarape_o-brasil-e-o-marco-civil-da-internet.pdf. Acesso em: 15 nov. 2022.

ARON, Raymond. **As etapas do pensamento sociológico**. Tradução de: Sérgio Bath. 6. ed. São Paulo: Martins Fontes, 2003.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte especial (arts. 155 a 212) crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos. 18. ed. rev. e atual. São Paulo: SaraivaJur, 2022, v. 3. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786553622074/. Acesso em: 17 nov. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Casa Civil, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 nov. 2022.

BRASIL. **Decreto-Lei n° 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro: Casa Civil, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 24 set. 2022.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília: Casa Civil, 2012a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 15 nov. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Casa Civil, 2012b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 nov. 2022.

BRASIL. **Lei nº 13.260, de 16 de março de 2016**. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Brasília, Casa Civil, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 1 jun. 2023

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília: Casa Civil, 2021b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 15 nov. 2022.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Brasília: Casa Civil, 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 15 nov. 2022.

BRASIL. **Lei nº 9.296, de 4 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília: Casa Civil, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 16 nov. 2022.

BRASIL. **Lei nº 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Brasília: Casa Civil, 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 27 set. 2022.

BROOKSHEAR, J. Glenn. **Ciência da computação**: uma visão abrangente. Tradução de: Cheng Mei Lee. 7. ed. Porto Alegre: Bookman, 2008.

CASTELLS, Manuel. **A sociedade em rede**: A era da informação: economia, sociedade e cultura. Tradução de: Roneide Venancio Majer. 6. ed. São Paulo: Paz e Terra, 1999. v. 1.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes Notificados ao CERT.br**: Incidentes notificados voluntariamente ao CERT.br por CSIRTs, administradores de redes e usuários finais. Brasil, 2023. Disponível em: https://stats.cert.br/. Acesso em: 7 jul. 2023.

COUNCIL OF EUROPE. **Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems**. Strasbourg, 2003. (European Treaty Series - No. 189). Disponível em: https://rm.coe.int/168008160f. Acesso em: 30 set. 2022.

COUNCIL OF EUROPE. **Computer-related crime**: recommendation n. r (89) 9 on computer-related crime and final report of the european committee on crime problems. Strasbourg, 1990.

COUNCIL OF EUROPE. **Convention on cybercrime**. Budapest, 2001a. (European Treaty Series - No. 185). Disponível em: https://rm.coe.int/1680081561. Acesso em: 3 set. 2022.

COUNCIL OF EUROPE. **Explanatory report to the convention on cybercrime**. Budapest, 2001b. (European Treaty Series - No. 185). Disponível em: https://rm.coe.int/16800cce5b. Acesso em: 25 out. 2022.

COUNCIL OF EUROPE. **Recommendation No. R (81) 12 of the committee of ministers to member states on economic crime**. [Strasbourg], 1981. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804cae97. Acesso em: 25 out. 2022.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.
DÍAZ, Omar Huertas. Anomia, normalidad y función del crimen desde la perspectiva de Robert Merton y su incidencia en la criminología. **Revista Criminalidad**, Bogotá, v. 52, n. 1, p. 365-376, 2010. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082010000100010. Acesso em: 28 jun. 2023.

DURKHEIM, Émile. **As regras do método sociológico**. Tradução de: Paulo Neves. 3. ed. São Paulo: Martins Fontes, 2007.

DURKHEIM, Émile. **Da divisão do trabalho social**. Tradução de: Eduardo Brandão. 2. ed. São Paulo: Martins Fontes, 1999.

DURKHEIM, Émile. **O suicídio**: estudo de sociologia. Tradução de: Monica Stahel. São Paulo: Martins Fontes, 2000.

EILBERG, Daniela Dora *et al*. **Os cuidados com a Convenção de Budapeste**: Objetivo da norma é a criação de vias para cooperação internacional em matéria penal e de procedimentos para combate aos cibercrimes. Jota, [*s. l.*], 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021. Acesso em: 31 out. 2022.

FORTINET. **Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina**: Fortinet registrou 31,5 bilhões de tentativas de invasão no país no primeiro semestre do ano, quase o dobro reportado no mesmo período de 2021. Ataques de ransomware dobram na região, chegando a 52 mil detecções no período. São Paulo, 18 ago. 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em: 7 jul. 2023.

GORDON, Sarah; FORD, Richard. On the definition and classification of cybercrime. **Journal of Computer Virology**, [*s. l.*], v. 2, p. 13-20, 2006. Disponível em: https://link.springer.com/article/10.1007/s11416-006-0015-z. Acesso em: 21 set. 2022.

GRECO, Rogério. **Curso de direito penal**: artigos 213 a 361 do código penal. 19. ed. rev. e atual. Barueri: Atlas, 2022, v. 3.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KAY, Jay; SMITH, Toby. Virtual insanity. Intérprete: Jay Kay. In: TRAVELLING without moving. Intérprete: Jamiroquai. [London]: Sony Soho Square, 1996. Disponível em: http://jamiroquai.com/music;Travelling_Without_Moving. Acesso em: 15 nov. 2022.

MAÍLLO, Alfonso Serrano; PRADO, Luiz Regis. **Curso de criminologia**. 2. ed. reform., atual e ampl. São Paulo: Editora Revista dos Tribunais, 2013.

MARTÍN, Ricardo M. Mata y. **Delincuencia informática y derecho penal**. Managua: Hispamer, 2003.

MERTON, Robert King. **Sociologia**: Teoria e estrutura. Tradução de: Miguel Maillet. São Paulo: Mestre Jou, 1970.

MOURA, Grégore Moreira de. **Curso de direito penal informático**. Belo Horizonte, São Paulo: D'Plácido, 2021.

NUCCI, Guilherme de Souza. **Curso de direito penal**: parte especial arts. 121 a 212 do código penal. 5. ed. rev. e atual. Rio de Janeiro: Editora Forense, 2021a, v. 2. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559640157/. Acesso em: 14 nov. 2022.

NUCCI, Guilherme de Souza. **Curso de direito penal**: parte especial arts. 213 a 361 do código penal. 5. ed. rev. e atual. Rio de Janeiro: Editora Forense, 2021b, v. 3. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559640188/. Acesso em: 16 nov. 2022.

OHANIAN, Christian. **The UN Cybercrime Treaty Has a Cybersecurity Problem In It**. Just security, [*s. l.*], 17 out. 2022. Disponível em: https://www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it/. Acesso em: 9 nov. 2022.

PAGE, Mercedes. **The hypocrisy of Russia's push for a new global cybercrime treaty**: The same Russia in the middle of invading a neighbour is preaching respect for state sovereignty online. The interpreter, [*s. l.*], 7 mar. 2022. Disponível em: https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty. Acesso em: 9 nov. 2022.

PHILLIPS, Kirsty *et al*. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. **Forensic Sciences**, [*s. l.*], v. 2, p. 379-398, 2022. Disponível em: https://www.mdpi.com/2673-6756/2/2/28. Acesso em: 28 set. 2022.

PIGATTO, Jaqueline Trevisan; ZANATTA, Rafael. **A Convenção de Crimes Cibernéticos da ONU e a guerra entre Rússia e Ucrânia**: Início das atividades do Comitê de Convenção de Cibercrimes da ONU é marcado pelo clima diplomático instável. Data Privacy Brasil Research, [*s. l.*], 11 mar. 2022. Disponível em: https://www.dataprivacybr.org/a-convencao-de-crimes-ciberneticos-da-onu-e-a-guerra-entre-russia-e-ucrania/. Acesso em: 9 nov. 2022.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Editora Saraiva, 2021. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 01 jul. 2023.

RODRIGUES, Gustavo**. A Convenção de Budapeste sobre o Cibercrime e as controvérsias sobre a adesão brasileira**. Instituto de Referência em internet e Sociedade. [*S. l.*], 2021. Disponível em: https://irisbh.com.br/a-convencao-de-budapeste-sobre-o-cibercrime-e-as-controversias-sobre-a-adesao-brasileira/. Acesso em: 30 out. 2022.

RODRIGUES, Luciana Ribeiro; PIMENTA, Francisco José Paoliello. Discussões sobre o conceito de ciberativismo e suas práticas atuais através de uma abordagem pragmaticista. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 38., 2015, Rio de Janeiro. **Anais** [...]. Rio de Janeiro, 2015. p.1-11. Disponível em: https://www.portalintercom.org.br/anais/nacional2015/resumos/R10-3234-1.pdf. Acesso em: 1 jul. 2023.

SABADELL, Ana Lucia. **Manual de sociologia jurídica**: introdução a uma leitura externa do direito. 6. ed. rev. atual. e aum. São Paulo: Editora Revista dos Tribunais, 2013.

SANTOS, Bruna Martins dos. **Convenção de Budapeste Sobre o Cibercrime na América Latina**: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México. [*S. l.*]: Derechos Digitales, 2022. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/PT-Ciberdelincuencia-2022.pdf. Acesso em: 28 out. 2022.

SARRE, Rick; LAU, Laurie Yiu-Chung; CHANG, Lennon Y.C.. Responding to cybercrime: current trends. **Police Practice And Research**: An International Journal, [*s. l.*], v. 19, n. 6, p. 515-518, 2018. Disponível em: https://www.tandfonline.com/doi/full/10.1080/15614263.2018.1507888. Acesso em: 3 out. 2022.

SELL, Carlos Eduardo. **Sociologia clássica**: Marx, Durkheim e Weber. Petrópolis: Vozes, 2017.

SHANGHAI COOPERATION ORGANIZATION. **Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization**. [Yekaterinburg], 2009. Disponível em: http://eng.sectsco.org/documents/. Acesso em: 13 set. 2022.

SHECAIRA, Sérgio Salomão. **Criminologia**. 6. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2014.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2015. *E-book*. Disponível em: https://bibliotecadigital.saraivaeducacao.com.br/books/580813. Acesso em: 4 jun. 2022.

UNITED KINGDOM. Home Office. **Cybercrime, a review of the evidence**: summary of key findings and implications. London, 2013. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. Acesso em: 20 set. 2022.

UNITED NATIONS. A/RES/74/247. **Resolution adopted by the General Assembly on 27 December 2019**: Countering the use of information and communications technologies for criminal purposes. 27 dec. 2019. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement. Acesso em: 9 nov. 2022.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

VIEIRA, Eduardo. **Os bastidores da internet**: A história de quem criou os primeiros negócios digitais do Brasil. [*S. l.: s. n.*], 2018. *E-book*.

WEBINAR: Convenção sobre Cibercrime, com Pedro Borges Mourão [Promotor de Justiça - RJ]. Gravação de Wesley Rodrigo. [S.l.: s.n.], 2022. 1 vídeo (93 min.) Publicado pelo canal Academia de Forense Digital. Disponível em: https://www.youtube.com/watch?v=dIvXpJezJ7Q. Acesso em: 28 out. 2022.