Alesandro Gonçalves Barreto
Karina Kufa
Marcelo Mesquita Silva

CIBERCRIMES

E SEUS REFLEXOS NO DIREITO BRASILEIRO

3ª EDIÇÃO
Revista, ampliada
e atualizada

2022

EDITORA JusPODIVM
www.editorajuspodivm.com.br

CAPÍTULO 2

OS CIBERCRIMES

Os perigos da conectividade são extremamente subestimados. Mesmo sociedades tradicionalmente fechadas e caracterizadas pela desconfiança em relação a estranhos, como a norte-americana, onde as crianças são rotineiramente advertidas dos perigos de abrir portas ou falar com estranhos, não tomam as mesmas cautelas quando no ambiente cibernético. Como assevera Britz:

> No entanto, o advento da tecnologia reduziu as barreiras tradicionais e, em verdade, serviu como um convite informal a visitantes desconhecidos. Muitos perceberam tarde demais os perigos de sua desatenção e se tornaram vítimas de furto, da perda de dados privados e similares. Outros permanecem ignorantes de sua vulnerabilidade, prestes a sofrerem as consequências negativas de sua postura.[1]

1. Livre tradução. No original: "*However, the advent of technology has lowered traditional barriers and actually served as an informal invitation for unknown visitors. Many have recognized only too late the dangers of their inattentiveness – victims*

Este natural despreparo dos internautas em aspectos de Segurança da Informação - aliado a uma forte dependência da tecnologia no dia a dia e a uma falsa sensação de distanciamento de problemas - ao se utilizar um computador no conforto de casa, tem facilitado demasiadamente o cibercrime.

Abordaremos, no presente capítulo, os conceitos e categorias dos cibercrimes, suas principais características e o perfil do cibercriminoso. Apresentaremos a evolução do cibercrime e as dificuldades enfrentadas na sua repressão.

2.1 CONCEITO E CATEGORIAS DOS CIBERCRIMES

Questão tortuosa é tentar encontrar uma nomenclatura que albergue os delitos que podem ser cometidos através de redes de dados. Diversos termos são utilizados, indiscriminadamente, para se referir a um gênero de delitos ou misturar-se suas espécies. Exemplo dessa variedade encontra-se nos nomes das delegacias especializadas de Polícia Civil de diversos estados brasileiros, destinadas à investigação de tais infrações: Delegacia de Repressão aos Crimes Cibernéticos (DR-CCIBER)- AP; Delegacia Especializada em Repressão a Crimes Cibernéticos - AM; Grupo Especializado de Repressão aos Crimes por Meio Eletrônicos - BA; Delegacia de Repressão aos Crimes Cibernéticos - CE; Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC) - DF; Delegacia de Repressão a Crimes Eletrônicos (DRCE) - ES; Delegacia Estadual de Repressão a Crimes Cibernéticos (DERCC) - GO; Departamento

---

of theft, stolen privacy, and the like; while others, yet to suffer negative consequences, remain blissfully unaware of their own vulnerability." BRITZ, Marjie T. **Computer forensics and cybercrime:** an introduction. New Jersey: Prentice Hall, 2009, p. 4.

de Combate aos Crimes Tecnológicos (DCCT) - MA; Delegacia Especializada em Investigação de Crime Cibernético - MG; Gerência Especializada de Crime de Alta Tecnologia (GECAT) - MT; Divisão de Prevenção e Repressão a Crimes Tecnológicos (DRCT) - PA; Núcleo de Combate aos Cibercrimes (Nuciber) - PR; Delegacia de Polícia de Repressão aos Crimes Cibernéticos - PE; Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia (DERCAT) - PI; Delegacia de Repressão aos Crimes de Informática (DRCI) - RJ; Delegacia de Repressão aos Crimes Informáticos (DRCI) - RS; Divisão de Crimes Cibernéticos (DCCIBER) - SP; Delegacia de Repressão aos Crimes de Informática (DRCI) - SC; Delegacia de Repressão a Crimes Cibernéticos (DRCC) – SE e; Divisão de Repressão a Crimes Cibernéticos (DRCC) - TO.

Tal dificuldade não é experimentada apenas no Brasil. Os Estados Unidos da América, país mais à frente na repressão dessa nova modalidade delitiva, sofrem, também, o mesmo problema. Expressões como: *computer crime, computer-related crime, crime by computer*, ou, depois, com a maior disseminação da tecnologia, os termos: *high-tecnology crime, information-age crime*. Com o advento da internet surgiram: *cybercrime, virtual crime, internet crime, net crime*, além de outras variantes mais genéricas, como: *digital crime, electronic crime, e-crime, high-tech crime* ou *technology-enable crime*[2].

Conforme a doutrina de Clough, nenhum dos termos é perfeito, pois sofrem uma ou mais deficiências, não alcançando com perfeição todo o sentido desta nova categoria de crime que se quer conceituar. As expressões que contêm o vocábulo

2. CLOUGH, Jonathan. **Principles of Cybercrime**. New York: Cambridge University Press, 2010, p. 9.

"computador" podem não incorporar as infrações cometidas contra as redes de dados; o termo "cibercrime" pode ter como foco exclusivo a internet; "crimes de alta-tecnologia" podem ser entendidos como referências, tão somente, aos delitos envolvendo avançadas e recentes searas da tecnologia, como a nanotecnologia ou a bioengenharia[3].

Observe-se que não se trata, ao contrário do que possa parecer, de mero tecnicismo, de simples discussão acadêmica da melhor terminologia. Como bem asseveram estudiosos do tema, a ausência de uma padronização, de uma homogeneização no conceito e identificação de tais delitos impede um melhor levantamento estatístico, dificulta a implementação de ações preventivas e repressivas. Clough exemplifica que o crime de acesso não autorizado no *Misuse Act* do Reino Unido, que tipifica alguns cibercrimes, é referido como outras fraudes nas estatísticas sobre infrações penais do mesmo país[4]. No mesmo sentido, diz McQuade[5]:

> Na pesquisa, o conceito de termos padronizados refere-se à criação de definições precisas a fim de permitir a rotulagem consistente, a compreensão e mensuração dos fenômenos. Ao padronizar termos,

3. Ibidem.
4. Ibidem, p. 14.
5. Livre tradução. No original: *"In research, the concept of operationalizing terms refers to creating precise definitions in order to enable consistent labeling, understanding, and measurement of phenomena. By operationalizing terms, researchers (and practitioners and policy makers) can avoid inappropriately commingling meanings of different types of abuse, deviancy, crime, and security threats. Operationalizing terms helps to prevent confusing research findings that would be of little value for creating crime prevention and information security programs, enacting new crime legislation, or enforcing laws and regulations. Preventing such confusion does generally improve criminal justice and security practices and policies"*. MCQUADE III, Samuel C. **Understanding and managing cybercrime**. Boston: Pearson, 2006, p. 17-18.

> os pesquisadores (e também profissionais e agentes políticos) podem evitar a inadequada mistura entre os significados de diferentes tipos de ameaças, como: conduta abusiva, desvio de conduta, crime e incidentes de segurança. A padronização de termos ajuda a prevenir confusão nos resultados de investigações, evitando transtornos na criação de programas de prevenção de crime e estabelecimento de medidas de segurança da informação, além de facilitar a tipificação de novos crimes e o cumprimento da lei. Prevenir tal confusão, geralmente, aprimora a justiça criminal e as práticas e políticas de segurança.

Uma primeira tarefa, portanto, para alcançarmos uma terminologia satisfatória, é apresentar uma divisão das três principais categorias de crimes relacionados com o uso da Tecnologia da Informação, segundo a doutrina. Tal distinção, adotada pelo Departamento de Justiça Americano[6], vem sendo albergada por diversos estudiosos:

I. Crimes em que o computador ou rede de computador é o alvo da atividade criminosa. Por exemplo, *malware*, *hackers* e ataques DOS. 2. Infrações tradicionais onde o computador é uma ferramenta utilizada para cometer o crime. Por exemplo, pornografia infantil, ameaça, violação de direitos autorais e fraude. 3. Crimes em que o uso do computador é um aspecto

6. Livre tradução. No original: "*I. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DOS attacks. 2. Existing offences where the computer is a tool used to Commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud. 3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more a repository for evidence*". CLOUGH, Jonathan. **Principles of Cybercrime**. New York: Cambridge University Press, 2010, p. 10.

incidental no cometimento do crime, mas pode suprir provas na sua persecução. Por exemplo, endereços encontrados no computador de um suspeito de assassinato, ou registros telefônicos de conversas entre o agressor e a vítima antes de um homicídio. Nesses casos, o computador não está significativamente implicado na prática do delito, mas incrementa o repositório de provas.

Essa classificação tripartite de crimes é adotada, com algumas pequenas variações, e utilizada no ordenamento interno da Austrália, Canadá, Reino Unido e, em grande medida, internacionalmente[7].

Uma divisão em duas categorias, todavia, geralmente se referindo às duas primeiras daquelas três apresentadas, é a que mais vem sendo utilizada pelos doutrinadores e acolhida nesta obra. McQuade utiliza-se dos termos *computer crime* e *computer-related crime*[8]. De acordo com Fichtelberg, os criminologistas dividem os cibercrimes em duas categorias, uma na qual constam crimes convencionais que utilizam computadores como ferramenta e outra de delitos específicos que não existiam antes da invenção dos computadores e da internet[9].

Como fora dito anteriormente, não lograr-se-á uma terminologia perfeita e acabada, isenta de críticas. Por tal motivo, não se deve receber tais nomenclaturas de forma literal, mas como uma descrição ampla que enfatize o principal papel da tecnologia utilizada no delito[10]. No esteio de Clough,

7. Ibidem, p. 10.
8. MCQUADE III, Samuel C. **Understanding and managing cybercrime**. Boston: Pearson, 2006, p. 15-17.
9. FICHTELBERG, Aaron. **Crime without borders:** an introduction to international criminal justice. New Jersey: Pearson Prentice Hall, 2008, p. 265.
10. CLOUGH, op. cit. p. 9.

o presente trabalho adotará a terminologia "cibercrime", por ser aquela que melhor alberga os delitos aqui tratados, por ser a mais utilizada na doutrina internacional, por ressaltar a importância dos computadores conectados em rede e, especialmente, por ser o termo utilizado na Convenção de Budapeste, estudada adiante.

O termo *cybercrime* foi inicialmente cunhado por Sussman e Heuston em 1995, conforme aponta McQuade. Ele havia sido utilizado, em 1997, em relatório de comissão presidencial formada para estudar a proteção de infraestrutura crítica[11]. O autor define o conceito e também assevera ser a terminologia mais aceita[12]:

> O cibercrime é no momento o termo mais frequentemente usado para rotular as atividades em que os delinquentes usam computadores, ou outros dispositivos eletrônicos de TI, através de sistemas de informação, para facilitar comportamentos ilegais. Em essência, o cibercrime envolve o uso de aparelhos eletrônicos para acessar, controlar, manipular ou utilizar os dados para fins ilegais.

Segundo Fichtelberg[13], cibercrimes podem ser definidos como: "[...] atividades através do uso de computador que são ilegais, ou consideradas ilícitas por determinadas

11. MCQUADE III, Samuel C. **Understanding and managing cybercrime**. Boston: Pearson, 2006, p. 15.
12. Livre tradução. No original: "*Cybercrime is now the term most often used to label activities in which perpetrators use computers or other electronic IT devices via information systems to facilitate illegal behaviors. In essence, cybercrime involves using electronic gadgets to access, control, manipulate, or use data for illegal purposes.*" Ibidem, p. 16-17.
13. Livre tradução. No original: *"[...] computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks."* FICHTELBERG, Aaron. **Crime without borders:** an

partes, e que podem ser conduzidas através de redes globais de dados." Assim se extrai, portanto, que a grande maioria dos cibercrimes consiste em delitos tradicionais, agora com nova roupagem, alcance e potencial lesivo, além de cibercrimes propriamente ditos, que são novas infrações voltadas contra computadores[14] e redes de computadores, sem os quais não existiriam.

Este trabalho adota a terminologia "cibercrimes próprios" e "impróprios", a exemplo de outras categorias de crimes, como os militares, para diferenciar os que são propriamente praticados em face de bens jurídicos afeitos à tecnologia da informação, daqueles que eventualmente utilizam a tecnologia da informação como ferramenta para lesar bens jurídicos tradicionais, como honra, patrimônio, costumes, liberdade, entre outros.

A escolha de tais *nomen juris*, "próprios e impróprios", parece a mais acertada diante de seu largo uso pela doutrina, na seara penal, além do fato de já ter sido utilizada para os delitos em estudo[15], não sendo demais apontar a existência de outras nomenclaturas para a mesma divisão, como delitos informáticos puros e impuros, ou aquelas adotadas por Chacon: crimes informáticos comuns e específicos[16].

---

introduction to international criminal justice. New Jersey: Pearson Prentice Hall, 2008, p. 265.

14. Naturalmente que se refere aos cibercrimes que visam prejudicar a prestação de serviços, destruir dados, paralisar rotinas, ou mesmo, destruir equipamentos alterando a normalidade das configurações de máquinas controladas por computador. Assim, não se inclui, o furto de uma loja de eletro-eletrônicos.
15. SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003, p. 60.
16. ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006, p. 40.

2.2 CARACTERÍSTICAS DOS CIBERCRIMES E O PERFIL DO CIBERCRIMINOSO

Importante analisar as principais características do cibercrime, de maneira a compreender o mecanismo desta modalidade delitiva, identificando formas de prevenção e combate. Segundo Clough: "Foi dito que existem três fatores necessários para a prática de crime: a existência de criminosos motivados, disponibilidade de oportunidades adequadas e a ausência de vigilância eficaz"[17]. Tais elementos são facilmente encontrados no ciberespaço. Com cerca de 3,9 bilhões de internautas no mundo, o potencial número de criminosos e de vítimas é impressionante. Munida de um ponto de conexão e um computador ou outro dispositivo, qualquer pessoa pode, no conforto de sua casa ou de um lugar qualquer, cometer uma série de delitos. O fator que propicia essa ação é o anonimato, seja aquele real, alcançado por *experts* (dito *hackers*), seja a mera sensação de distanciamento do usuário mediano, ao utilizar falsas identidades *on-line* ou se valer de simples programas de mascaramento de IP[18].

Essa atividade foi bruscamente incrementada com a disseminação do *software* de código livre TOR (*The Onion Router*), que direciona o tráfego da internet com o fito de ocultar a localização e a identidade dos usuários[19], atra-

17. Livre tradução. No original: *"It has been said that there are three factors necessary for the commission of crime: a supply of motivated offenders, the availability of suitable opportunities and the absence of capable guardians."* CLOUGH, Jonathan. **Principles of Cybercrime**. New York: Cambridge University Press, 2010, p. 5.
18. Através desta técnica, utiliza-se um equipamento que intermedia a conexão, fazendo-se passar pelo computador do usuário, de modo que se forem rastreados os acessos feitos pelo criminoso será identificado o endereço de IP da máquina intermediária.
19. Disponível em: <https://www.torproject.org/>. Acesso em: 14/03/2021.

vés de uma rede livre, mundial, formada por mais de 7 mil voluntários que funcionam como servidores. A percepção dos delinquentes é a de que não serão identificados, além de terem a confiança, em regra infelizmente verdadeira, de que o poder público não tem aparato suficiente para produzir provas necessárias para lastrear uma condenação. A prova pericial é inafastável nesses casos e a volatilidade da informação, sem uma infraestrutura tecnológica e humana eficiente, pode restar corrompida, perdida ou não ser admitida em juízo. Segundo Érica Ferreira[20]:

> Estudos demonstram que os internautas possuem algumas características próprias: em geral são imparciais, liberais, tolerantes por natureza, politicamente incorretos, descrentes a respeito dos meios estabelecidos, sentem-se menos ameaçados pelo governo na medida em que o consideram antiquado e inoperante.

Um importante instrumento para a árdua tarefa de prevenir e combater os cibercrimes é a capacidade de avaliar o potencial delitivo de determinados indivíduos, traçando-se um adequado perfil. Embora banalizada por seriados norte-americanos de TV, esta atividade, que se arrima em elementos de criminologia, tem a crucial finalidade de estabelecer a conduta delitiva de cada pessoa. Isso é especialmente importante nos delitos perpetrados através da internet, já que os agentes estão amparados pela distância, o que dificulta a perfeita atribuição da participação de cada indivíduo.

---

20. MUÑOZ MACHADO, Santiago. **La regulación de la red:** Poder y Derecho en internet. Madrid: Taurus, 2000, p. 17, *apud* FERREIRA, Érica Lourenço de Lima. **Internet:** macrocriminalidade e jurisdição internacional. Curitiba: Juruá, 2007, p. 91.

Para tanto, foram criados métodos de investigação, entre eles o SKRAM, desenvolvido pelo consultor em Segurança da Informação, Donn Parker, conforme apresenta McQuade[21]:

> Donn Parker é creditado pelo desenvolvimento de um modelo de avaliação de criminosos que engloba o estudo de motivos, a oportunidade e os meios disponíveis para traçar o perfil de suspeitos em uma investigação. Conhecido como SKRAM (*skills, knowledge, resources, authority and motives*), seu modelo é adaptado para avaliar as habilidades, conhecimentos, recursos, autoridade técnica para acessar e manipular localizações e dados, sejam físicos ou virtuais, e avaliar a intensidade de motivos para cometer cibercrimes.

2.3 EVOLUÇÃO DO CIBERCRIME

O primeiro registro de delito com o uso de computador data de 1958, no qual um empregado do Banco de Minneapolis, nos Estados Unidos da América, havia alterado os programas de computador do banco, de modo a depositar para si as frações de centavos resultantes de milhões de movimentações financeiras. A primeira condenação por uma corte federal norte-americana deu-se em 1966, por alteração de dados bancários[22].

A variedade de crimes cometidos com o uso da internet é impressionante, e mesmo homicídios já foram cometidos

21. Livre tradução. No original: "*Donn Parker is credited with developing an attacker assessment model that subsumes the classic motive, opportunity, and means framework for establishing suspects in an investigation. Known as SKRAM, his model is adapted here to refer to the skills, knowledge, resources, and technical authority to access and manipulate physical and cyber locations and data, and intensity of motives for committing cybercrimes.*" MCQUADE III, Samuel C. **Understanding and managing cybercrime**. Boston: Pearson, 2006, p. 118.
22. Ibidem, p. 12.