UNIVERSIDADE FEDERAL DE MINAS GERAIS

Faculdade de Filosofia e Ciências Humanas

Departamento de Sociologia

Especialização em Estudos da Criminalidade e Segurança Pública

Camila Fernandes Bicalho

Crimes patrimoniais na era digital: contribuições da Teoria das Atividades Rotineiras

Belo Horizonte

2024

Camila Fernandes Bicalho

Crimes patrimoniais na era digital: contribuições da Teoria das Atividades Rotineiras

Monografia de especialização apresentada à Faculdade de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Especialista em Estudos da Criminalidade e Segurança Pública.

Orientador: Prof. Dr. Frederico Couto Marinho

Belo Horizonte

2024

301
B583c
2024

Bicalho, Camila Fernandes.

Crimes patrimoniais na era digital [recurso eletrônico] : contribuições da teoria das atividades rotineiras / Camila Fernandes Bicalho. - 2024.

1 recurso online (75 f. : il.) : pdf

Orientador: Frederico Couto Marinho.

Monografia apresentada ao curso de Especialização em Estudos da Criminalidade e Segurança Pública - Universidade Federal de Minas Gerais, Faculdade de Filosofia e Ciências Humanas.

Inclui bibliografia.

1.Crime contra o patrimônio. 2. Crime por computador. 3.Ciberespaço . I. Marinho, Frederico Couto.II. Universidade Federal de Minas Gerais. Faculdade de Filosofia e Ciências Humanas. III. Título.

Ficha catalográfica elaborada por Vilma Carvalho de Souza - Bibliotecária - CRB-6/1390

UNIVERSIDADE FEDERAL DE MINAS GERAIS

ATA

UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE SOCIOLOGIA
ESPECIALIZAÇÃO EM ESTUDOS DE CRIMINALIDADE E SEGURANÇA PÚBLICA

ATA DE DEFESA DE MONOGRAFIA DE

2023692401 CAMILA FERNANDES BICALHO

Aos dezessete dias do mês de dezembro de dois mil e vinte e quatro, reuniu-se a banca examinadora de defesa de monografia do Curso de Especialização em Estudos de Criminalidade e Segurança Pública, composta por: Prof. Drº Frederico Couto Marinho (orientador), Profª . Drª Ludmila Mendonça Lopes Ribeiro, e Prof. Me. Lucas Caetano Pereira de Oliveira para examinar a monografia intitulada "**Crimes patrimoniais na era digital: contribuições da Teoria das Atividades Rotineiras**" – discente **CAMILA FERNANDES BICALHO**. Procedeu-se a arguição, finda a qual os membros da banca examinadora reuniram-se para deliberar, decidindo por unanimidade pela aprovação da monografia, com nota 85,0 (oitenta e cinco). Para constar, foi lavrada a presente ata que vai datada e assinada.

Belo Horizonte, 17 de dezembro de 2024

Profa Dra. Ludmila Mendonça Lopes Ribeiro

Me Lucas Caetano Pereira de Oliveira

Prof. Dr. Frederico Couto Marinho (Orientador)

Documento assinado eletronicamente por **Frederico Couto Marinho**, **Coordenador(a) de curso**, em 06/01/2025, às 15:35, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Lucas Caetano Pereira de Oliveira**, **Usuário Externo**, em 06/01/2025, às 16:06, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ludmila Mendonca Lopes Ribeiro**, **Professor(a)**, em 07/01/2025, às 05:10, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3862265** e o código CRC **9982AD26**.

Referência: Processo nº 23072.253465/2024-07 SEI nº 3862265

RESUMO

O presente trabalho analisou o fenômeno dos crimes contra o patrimônio praticados pelo meio virtual e teve como objetivo compreender as mudanças nos padrões de crimes patrimoniais no Brasil por meio da Teoria das Atividades Rotineiras (TAR). O problema que guiou a pesquisa foi: Quais as contribuições da Teoria das Atividades Rotineiras na explicação das mudanças nos padrões de crimes patrimoniais? A hipótese levantada foi a de que a crescente utilização dos meios digitais, desacompanhada de medidas efetivas de proteção e conscientização sobre segurança cibernética, contribui para a vulnerabilidade dos usuários e a facilidade de acesso por parte de potenciais criminosos. O método científico utilizado foi o hipotético-dedutivo, já que o trabalho busca explorar argumentos que comprovem, ou não, a hipótese estabelecida. Houve coleta de dados públicos nacionais do Fórum Brasileiro de Segurança Pública sobre o aumento de crimes informáticos patrimoniais, sobretudo antes, durante e depois da pandemia por Covid-19. Ao final, verificou-se que o crescimento expressivo do uso de TICs durante a pandemia contribuiu significativamente para o aumento dos crimes patrimoniais virtuais e que a Teoria das Atividades Rotineiras é uma ferramenta útil para entender as novas dinâmicas de vulnerabilidade e oportunidades de crime na era digital.

Palavras-chave: Crimes patrimoniais; cibercrimes; ciberespaço; Teoria das Atividades Rotineiras.

ABSTRACT

This study aimed to investigate the phenomenon of property crimes committed through virtual means and sought to understand the changes in patterns of property crimes in Brazil using the Routine Activity Theory (RAT) by Cohen and Felson (1979). To this end, the main research question guiding the scientific inquiry is summarized as follows: What are the contributions of Routine Activity Theory in explaining the changes in patterns of property crimes? The hypothesis proposed is that the increasing use of digital media, without accompanying effective protection measures and awareness of cybersecurity, contributes to user vulnerability and facilitates access for potential criminals. The scientific method applied was hypothetical-deductive, as the study seeks to explore arguments that may confirm or refute the established hypothesis. National public data from the Brazilian Public Security Forum on the rise in property-related cybercrimes was collected, focusing especially on the periods before, during, and after the Covid-19 pandemic. In the end, it was found that the significant increase in the use of ICTs during the pandemic contributed substantially to the rise in virtual property crimes, and that Routine Activity Theory is a valuable tool for understanding the new dynamics of vulnerability and crime opportunities in the digital age.

Keywords: Property crimes; cybercrimes; cyberspace; Routine Activity Theory.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Estamos na era da conexão[1] e da informação[2]. A partir do desenvolvimento da computação móvel (laptops, notebooks), das tecnologias nômades (smartphones, smartwatch e tablets) e da internet (especialmente, o Wi-Fi e as redes móveis), que marcam a emergência das comunicações sem fio, vivenciamos diversas modificações no espaço urbano[3].

A tecnologia, em sentido amplo, está presente em todos os espaços cotidianos, sendo praticamente impossível pensar em uma realidade sem ela. Desde as atividades mais simples às mais complexas, a tecnologia "*existe para servir ao homem*"[4], facilitando o acesso à informação, conectando pessoas ao redor do mundo e otimizando processos, tornando o dia a dia mais eficiente e dinâmico.

Especificamente, as Tecnologias de Informação e Comunicação (TICs) tornaram-se "*os vetores principais desse fluxo generalizado e dessa circulação virótica de informação, dinheiro, pessoas, produtos e processos - o que é uma radicalização do processo de globalização que se inicia com as grandes navegações do século XVI*"[5]. Definidas como sendo "*aparatos técnicos inventados pelo homem que se destinam a colaborar para propagação e preservação cultural por meio de comunicação oral e/ou escrita*"[6], as TICs têm um papel fundamental na integração das sociedades atuais, promovendo trocas culturais e de informação em nível global.

Por outro lado, especialmente após o período da pandemia de Covid-19, o uso das TICs e do ambiente virtual passou a ser um cenário frequente para a realização de diversas atividades, incluindo práticas consideradas criminosas, uma vez que essas tecnologias se incorporaram profundamente ao cotidiano social. Atividades como transações financeiras, comunicação e comércio criaram oportunidades para novas formas de crime, fraudes e estelionatos aplicados via redes sociais e aplicativos de mensagens. Assim, o espaço digital se tornou não apenas uma extensão das interações humanas, mas também um ambiente onde criminosos exploram

---

[1] LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**, [S. l.], v. 22, n. 1_100, p. 107–133, 2018. Disponível em: https://www.revistarazonypalabra.org/index.php/ryp/article/view/1145. Acesso em: 17 set. 2024.
[2] CASTELLS, Manuel. **A sociedade em rede**. Tradução de Roneide Venâncio Majer. 6 ed. São Paulo: Paz e Terra, 2002.
[3] LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**...
[4] PINOCHET, Luis Hernan Contreras. **Tecnologia da informação e comunicação** - 1. ed. - Rio de Janeiro: Elsevier, 2014. p. 03.
[5] LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**...
[6] CAPOBIANCO, Ligia. A Revolução em Curso: Internet, Sociedade da Informação e Cibercultura. **Estudos em Comunicação** nº7 - Volume 2, 175-193, 2010, p. 185.

vulnerabilidades tecnológicas e a falta de familiaridade de muitos usuários com práticas seguras.

Com o intuito de estudar esse fenômeno, o presente trabalho se propõe a investigar as transformações sociais e culturais decorrentes do avanço das TICs e sua relação com o aumento dos crimes cibernéticos. A partir dessa análise, busca-se compreender como o ambiente digital impacta o cotidiano das pessoas, introduz novas dinâmicas criminais e exige adaptações nas políticas de segurança pública. Para isso, o trabalho utiliza a Teoria das Atividades Rotineiras, de Cohen e Felson (1979), como uma base para examinar os fatores que contribuem para a ocorrência de crimes patrimoniais virtuais no Brasil, considerando o perfil dos usuários, o aumento da conectividade e as vulnerabilidades que emergem com a digitalização de atividades diárias.

Nesse sentido, no capítulo 1 o trabalho realizou uma breve análise sobre a cibercultura e o uso das TICs no Brasil. Observou-se que a transformação cultural e no espaço urbano promovida ao longo dos anos pela disseminação das TICs e da internet impactou significativamente o país. Atualmente, o Brasil ocupa o terceiro lugar mundial em consumo de redes sociais, embora apresente um índice considerável de pessoas sem habilidades digitais básicas.

No capítulo 2, a pesquisa apresentou conceitos importantes acerca do ciberespaço, frisando o modo como a nova configuração social, marcada pela crescente utilização das TICs e da internet contribuiu para a incidência dos cibercrimes. Além disso, demonstrou de que forma as atuais leis penais tratam dos crimes cibernéticos no país e, ainda, como a criminologia – e, mais específico, a Teoria das Atividades Rotineiras – podem auxiliar no entendimento desses crimes.

No capítulo 3, o trabalho analisou os dados disponíveis no Anuário Brasileiro de Segurança Pública, no período de 2019 a 2024, e publicados pelo Fórum Brasileiro de Segurança Pública para identificar possíveis diferenças entre os índices de crimes patrimoniais cometidos em âmbitos urbanos (físicos) e no ciberespaço ao longo dos anos, considerando um período pré e pós pandemia por Covid-19.

No capítulo 4, foi possível compreender melhor a aplicação da Teoria das Atividades Rotineiras no contexto brasileiro, levando em consideração os dados apresentados no trabalho e aqueles disponibilizadas pelo Anuário Brasileiro.

Ao final, foram apontadas considerações acerca dos dados analisados e as contribuições da Teoria das Atividades Rotineiras, sobretudo para possíveis (re)formulações de políticas públicas voltadas a esse tipo de criminalidade, que assola o país – e o mundo. Pode-se concluir

que a crescente utilização dos meios digitais, desacompanhada de medidas efetivas de proteção e conscientização sobre segurança cibernética, contribui para a vulnerabilidade dos usuários e a facilidade de acesso por parte de potenciais criminosos. Assumindo as premissas e o modelo causal da Teoria das Atividades Rotineiras, pode-se afirmar que a expansão acelerada numa escala global do uso das TIC´s leva a mudanças nos padrões dos crimes contra o patrimônio.

1. UMA BREVE ANÁLISE SOBRE A CIBERCULTURA E O ACESSO ÀS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NO BRASIL

A revolução tecnológica, iniciada no século XX, promoveu transformações significativas na sociedade e na sua forma de relacionar[7]. Desde a criação dos computadores, que inicialmente eram máquinas de grande porte operadas apenas por especialistas[8], o desenvolvimento de novos equipamentos tecnológicos alavancou, passando a fazer parte intrínseca do cotidiano das pessoas[9].

De acordo com André Lemos (2018), a informatização da sociedade se iniciou na década de 70, "*com a convergência tecnológica e o estabelecimento do personal computer (PC)*". Em seguida, já nos anos 80-90, houve a popularização da internet e a transformação do computador pessoal (PC) em computador coletivo (CC), conectado ao espaço virtual (**ciberespaço**). Atualmente, estamos na era dos computadores coletivos móveis (CCm). Nas palavras do autor[10]:

> Estamos na era da conexão. Ela não é apenas a era da expansão dos contatos sobre forma de relação telemática. Isso caracterizou a primeira fase da internet, a dos "computadores coletivos" (CC). Agora temos os "computadores coletivos móveis (CCm)".
> Podemos esboçar uma pequena cronologia.
> Na primeira fase da micro-informática, nos anos 70-80, surgem os PC. Na segunda fase, com a decolagem da internet, surgem os CC, nos anos 80 e 90. Aqui a idéia é que os computadores sem conexão são instrumentos sub-aproveitados e que, na verdade, o verdadeiro computador é a grande rede. Agora, com o desenvolvimento das tecnologias móveis, o CCm estabelece-se com a computação ubíqua sem fio. Trata-se da ampliação de formas de conexão entre homens e homens, máquinas e homens, e máquinas e máquinas motivadas pelo nomadismo tecnológico da cultura contemporânea e pelo desenvolvimento da computação ubíqua (3G, Wi-Fi), da computação senciente (RFID5, bluetooth) e da computação pervasiva, além da continuação natural de processos de emissão generalizada e de trabalho cooperativos da primeira fase dos CC (blogs, fóruns, chats, softwares livres, peer to peer, etc). Na era da conexão, do CCm, a rede transforma-se em um "ambiente" generalizado de conexão, envolvendo o usuário em plena mobilidade.

A **internet**, assim como a computação, é uma invenção norte-americana, surgida durante a Guerra Fria por volta de 1969, sob o nome de Arpanet. Inicialmente, era um sistema utilizado pelo Departamento de Defesa dos Estados Unidos, que posteriormente se expandiu para universidades e centros de pesquisa, até que seu uso se tornou irrestrito. A internet, no

---

[7] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito Processual) - Universidade Federal de São Paulo, São Paulo, 2012. Acesso em: 29 mai. 2024.
[8] MACHADO, Luís Antônio Licks Missel; SILVA, Jardel Luís da. Crimes digitais: o aumento da complexidade das relações sociais e os novos espaços de intervenção estatal. **Revista Eletrônica de Ciências Contábeis**, 2013, n. 3, p. 64-73. Acesso em: 29 mai. 2024.
[9] VAZ, Denise Provasi. **Provas digitais no processo penal**...
[10] LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**...

formato que conhecemos hoje, com os sistemas HTTP, WWW e a linguagem HTML, foi criada em 1991 pelo cientista Tim Berners-Lee[11].

É nesse cenário que, para Lemos (2018), surgiu a **cibercultura**. A partir da microinformática dos anos 70, a cibercultura "*solta as amarras e desenvolve-se de forma onipresente, fazendo com que não seja mais o usuário que se desloca até a rede, mas a rede que passa a envolver os usuários e os objetos numa conexão generalizada*"[12]. Para Pierre Lévy (1999, p. 17), cibercultura seria o "*conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço*"[13].

Muito mais do que informações disponíveis em rede, a cibercultura trata-se, de acordo com Patrícia Cella (2005, p. 18), de uma "*variedade de informações, vindas de inúmeros países, pessoas de crenças, cores, ideologias e vidas completamente diferentes, e cada navegante dessa rede pode acessar estas informações e conhecer, sob o ponto de vista de cada um, o que se passa no mundo*"[14]. De acordo com a autora:

> A cibercultura mundializa visões díspares e modos de organização social contrastantes, sem favorecer pensamentos únicos. Congrega forças, ímpetos e desejos contraditórios, com a peculiaridade fundamental – apontada por Pierre Lévy – de universalizar sem totalizar. Na direção aqui proposta, a totalidade tem a ver com a descontextualização dos discursos, que possibilita o domínio dos significados, o anseio pelo todo, a tentativa de instaurar em cada lugar unidades de sentido idênticas. A noção de totalidade busca bloquear a pluralidade de contextos e a multiplicidade de segmentos que neles deveriam intervir[15].

O termo cibercultura surge da ampliação do conceito de cultura, sendo que a cultura digital representa uma evolução natural da cultura desenvolvida pelas sociedades. Sua principal distinção está no fato de que os dados estão concentrados em um espaço desterritorializado, acessível à maior parte das pessoas, oferecendo novas oportunidades de socialização e comunicação. Isso ocorre por meio de diversas ferramentas tecnológicas, como e-mails, chats, fóruns, entre outros[16].

Para Ligia Capobianco (2010, p. 187), a revolução tecnológica que atravessa grande parte dos setores sociais estabelece os alicerces da cibercultura, que, por sua vez, demanda a

---

[11] SIMÕES, Isabella de Araújo Garcia. A Sociedade em Rede e a Cibercultura: dialogando com o pensamento de Manuel Castells e de Pierre Lévy na era das novas tecnologias de comunicação. **Revista eletrônica Temática**. Ano V, n. 05 – Maio/2009.
[12] LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**...
[13] LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu Costa – São Paulo: Ed. 34, 1999, p. 17.
[14] CELLA, Patrícia de Oliveira Gasieri. Cibercultura: Uma realidade no Mundo Virtual. **Revista CESUMAR – Ciências Humanas e Sociais Aplicadas**, v. 10 n. 1 (2005): jan./jun. p. 18.
[15] *Ibidem*, p. 20.
[16] CAPOBIANCO, Ligia. A Revolução em Curso: Internet, Sociedade da Informação e Cibercultura... p. 187.

criação de novas estruturas, especialmente no que diz respeito à organização do trabalho, do lazer e da comunicação entre as pessoas. Os limites da cibercultura tornam-se mais claros à medida que seu uso se expande, assim como o acesso e a eficiência das tecnologias de informação e comunicação. No entanto, ainda faltam definições mais abrangentes, já que um dos aspectos mais relevantes da cultura digital é justamente sua diversidade[17].

Desde a década de 70, a cibercultura é caracterizada pela formação de uma sociedade estruturada por uma conectividade telemática ampla, que expande o potencial de comunicação, possibilita a troca de informações nas mais diversas formas e incentiva novas formas de agregação social[18]. A partir dos anos 90, a geração já passa a se familiarizar com tecnologias como multimídia, realidade virtual e redes telemáticas.

Aliás, em 2003 o número de telefones celulares ativos superou o total de linhas fixas em escala global. Nos anos seguintes, houve uma rápida expansão das redes de alta velocidade (àquela época, a rede 3G) e o surgimento de dispositivos móveis com capacidade computacional avançada: os *smartphones*[19]. De acordo com Ivan Satuf (2016, p. 210), a partir daquele ano, à medida que as redes digitais começaram a acompanhar a mobilidade dos corpos, o computador deixou de ser a única interface de conexão[20]. E o autor complementa:

> A melhoria constante das infraestruturas de telecomunicação alterou gradualmente a percepção de tempo e espaço que até então caracterizava a conexão digital. Dispositivos móveis como smartphones e tablets, ao contrário dos computadores, são tecnologias "always-on" (BARON, 2008; TURKLE, 2011) que recebem e enviam dados mesmo quando não estão em uso direto pelo usuário. Alertas noticiosos chegam a qualquer momento, sensores de geolocalização indicam a posição exata do usuário e aplicativos de mensagem instantânea criam conexões a partir das demandas interativas. Basta pressionar a pequena tela táctil para imediatamente se conectar à rede (...)[21].

Nesse cenário, a cibercultura emerge com os pós-mídia (*postmedia*) incluindo redes informáticas, interação multimídia e ambientes virtuais. Esse novo contexto não significa apenas a cibernetização da sociedade, mas uma verdadeira reconfiguração das relações humanas e técnicas, onde a tecnologia se torna um espaço de socialização. A simulação,

---

[17] *Ibidem*, p. 187.
[18] LEMOS, André, **Cibercultura, tecnologia e vida social na cultura contemporânea**, Porto Alegre, Sulina, 2004. p. 87.
[19] SATUF, Ivan. Onde está o ciberespaço? A metáfora da "nuvem" aplicada aos estudos da cibercultura. **AÇÃO MIDIÁTICA**, n.11. Jan/jun. 2016. Curitiba. PPGCOM-UFPR. ISSN 2238-0701. p. 210.
[20] *Idem.*
[21] *Idem.*

característica central da cibercultura, surge como uma forma de apropriação do real, transformando a maneira como vivemos, interagimos e entendemos o mundo ao nosso redor[22].

E toda essa transformação cultural e no espaço urbano promovida ao longo dos anos também ecoou, por óbvio, no Brasil. No país, os primeiros computadores destinados a atividades científicas surgiram a partir da década de 60, sendo que somente com o advento dos computadores pessoais (microcomputador/PC) que seu uso começou a se espalhar, embora de maneira ainda bastante lenta, pela sociedade[23]. Atualmente, porém, com o avanço dos equipamentos digitais e da praticidade para o seu manuseio, a proporção de domicílios com PCs recuou e o uso do *tablet* subiu ligeiramente.

De acordo com os dados divulgados pelo Módulo de Tecnologia de Informação e Comunicação (TIC) da Pesquisa Nacional por Amostra de Domicílios (PNAD) Contínua[24], de 2021 a 2022 a porcentagem de domicílios com microcomputador (PC) diminuiu de 40,7% para 40,2%, enquanto que a proporção de domicílios com *tablet* aumentou de 9,9% em 2021 para 10,7% em 2022[25].

Segundo os dados divulgados, de 2021 a 2022 o acesso da rede de internet nos domicílios do país aumentou de 90% para 91,5%[26]. De acordo com a pesquisa, em 2022, 161,6 milhões de brasileiros com 10 (dez) anos ou mais fizeram uso da internet durante o período de referência da PNAD, correspondendo a 87,2% da população nessa faixa etária[27]. Para tanto, o telefone móvel celular era o principal dispositivo de acesso à internet em casa, sendo utilizado

---

[22] LEMOS, André. Ciber-socialidade: tecnologia e vida social na cultura contemporânea. **Logos**, [S. l.], v. 4, n. 1, p. 15–19, 2015. Disponível em: https://www.e-publicacoes.uerj.br/logos/article/view/14575. Acesso em: 3 out. 2024.

[23] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011. p. 16.

[24] A PNAD Contínua "*Visa acompanhar as flutuações trimestrais e a evolução, no curto, médio e longo prazos, da força de trabalho, e outras informações necessárias para o estudo do desenvolvimento socioeconômico do País. Para atender a tais objetivos, a pesquisa foi planejada para produzir indicadores trimestrais sobre a força de trabalho e indicadores anuais sobre temas suplementares permanentes (como trabalho e outras formas de trabalho, cuidados de pessoas e afazeres domésticos, tecnologia da informação e da comunicação etc.), investigados em um trimestre específico ou aplicados em uma parte da amostra a cada trimestre e acumulados para gerar resultados anuais, sendo produzidos, também, com periodicidade variável, indicadores sobre outros temas suplementares. Tem como unidade de investigação o domicílio*." Fonte: PNAD Contínua - Pesquisa Nacional por Amostra de Domicílios Contínua. **IBGE.** Disponível em: <https://www.ibge.gov.br/estatisticas/sociais/populacao/9171-pesquisa-nacional-por-amostra-de-domicilios-continua-mensal.html?=&t=o-que-e>. Acesso em: 03 jun. 2024.

[25] EM 2022, Internet estava presente em 91,5% dos domicílios do país. **Agência Gov, 2023**. Disponível em: <https://agenciagov.ebc.com.br/noticias/202311/em-2022-streaming-estava-presente-em-43-4-dos-domicilios-com-tv>. Acesso em: 03 jun. 2024.

[26] IBGE: Internet está em 91,5% dos domicílios. **ABRANET, 2023**. Disponível em: <https://www.abranet.org.br/Noticias/IBGE%3A-Internet-esta-em-91%2C5%25-dos-domicilios-4623.html>. Acesso em: 04 jun. 2024.

[27] INTERNET chega a 87,2% dos brasileiros com mais de 10 anos em 2022, revela IBGE. **Ministério das Comunicações (Governo brasileiro), 2023**. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2023/novembro/internet-chega-a-87-2-dos-brasileiros-com-mais-de-10-anos-em-2022-revela-ibge>. Acesso em: 04 jun. 2024.

em 98,9% dos domicílios com acesso à rede, seguido pela televisão (47,5%), microcomputador (35,5%) e *tablet* (7,6%)[28]. Aqui, vale destacar um recorte contextual importante: a ocorrência da pandemia por Covid-19, em 2020, que intensificou a utilização de tecnologias no Brasil[29].

De toda forma, essa realidade reflete aquilo que Lemos (2018, p. 114) já havia sinalizado. Segundo o autor, diversos estudos destacam as características do uso do telefone celular em diferentes países e, embora as especificidades culturais influenciem as formas de utilização, há um consenso sobre a crescente expansão tanto no número de usuários quanto nas maneiras de uso (como chamadas de voz, SMS, compras e contatos)[30].

Atualmente, o celular é uma espécie de controle remoto, ou melhor, de "teletudo", já que se tornou "*um equipamento que é ao mesmo tempo telefone, máquina fotográfica, televisão, cinema, receptor de informações jornalísticas, difusor de e-mails e SMS5, WAP6, atualizador de sites (moblogs), localizador por GPS, tocador de música (MP3 e outros formatos), carteira eletrônica...*"[31]. Nas palavras do pesquisador:

> Podemos agora falar, ver TV, pagar contas, interagir com outras pessoas por SMS, tirar fotos, ouvir música, pagar o estacionamento, comprar tickets para o cinema, entrar em uma festa e até organizar mobilizações políticas e/ou hedonistas (caso das smart e flash mobs). O celular expressa a radicalização da convergência digital, transformando-se em um "teletudo" para a gestão móvel e informacional do quotidiano. De média de contato inter-pessoal, o celular está se transformando em um media massivo[32].

Outro dado relevante apontado pela PNAD Contínua é que o percentual de utilização da internet pelas pessoas com 60 (sessenta) anos ou mais aumentou de 57,5% em 2021[33] para 62,1% em 2022[34]. Proporcionalmente, o referido grupo etário é o que menos acessa a rede, ficando atrás dos demais grupos, formados pelo público de 10 (dez) a 59 (cinquenta e nove) anos de idade.

---

[28] 161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022. **Agência IBGE Notícias, 2023**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022#:~:text=O%20equipamento%20mais%20utilizado%20para,35%2C5%25%20de%202022>. Acesso em: 04 jun. 2024.

[29] ESTUDO mostra que pandemia intensificou uso das tecnologias digitais. **Agência Brasil, 2021**. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais>. Acesso em: 10 nov. 2024.

[30] LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**... p. 115.

[31] *Ibidem*, p. 114.

[32] *Idem.*

[33] CELULAR segue como aparelho mais utilizado para acesso à internet no Brasil. **Ministério das Comunicações (Governo brasileiro), 2022**. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2022/setembro/celular-segue-como-aparelho-mais-utilizado-para-acesso-a-internet-no-brasil>. Acesso em: 20 mar. 2024.

[34] 161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022. **Agência IBGE Notícias, 2023**...

A crescente utilização da internet pelos brasileiros fez com que o Brasil se tornasse, ainda em 2021, o 5º (quinto) país com mais usuários da rede no mundo. Conforme divulgado no site da revista Forbes Brasil, um estudo realizado pela plataforma de desconto Cupom Válido, com dados da Statista (empresa alemã especializada em marketing, dados de mercado e consumidores), revelou que o país possui cerca de 165 milhões de usuários, liderando o *ranking* dos países da América Latina[35]. Atualmente, esse número ultrapassa 181 milhões[36].

De fato, é perceptível que nos dias atuais os brasileiros estão cada vez mais conectados. As TICs de acesso à internet são utilizadas por esses cidadãos não apenas como método de estudo e trabalho, mas também como forma de interação entre nichos sociais. Nesse sentido, as próprias redes sociais, utilizadas por meio de aparelhos tecnológicos, têm se tornado um dos principais canais de comunicação e obtenção de informação, o que fez com que o Brasil ocupasse o lugar de terceiro maior consumidor de redes sociais no mundo[37].

Essa utilização contínua da internet fez dela ferramenta necessária e essencial, que se encontra mais presente nos lares brasileiros do que serviços de saneamento básico. Conforme levantamento divulgado em 2023 pelo *Global Overview Report*, da organização Kepios, dentre as pessoas que possuem acesso à internet, cerca de 18 milhões não têm acesso à saneamento básico. A pesquisa ainda revela que, dentre os brasileiros conectados, mais de 9 milhões recebem salário inferior a R$ 550,00 (quinhentos e cinquenta reais) por mês[38].

Acontece que, apesar do avanço no acesso à tecnologia e às redes, seu uso é constantemente desacompanhado de habilidades digitais básicas para navegar no ambiente digital. De acordo com o levantamento realizado pela Agência Nacional de Telecomunicações (ANATEL) e apresentado no evento "Huawei 25 anos", apenas 24% dos brasileiros têm entendimentos digitais básicos, que seriam habilidades de anexar documentos em e-mails e baixar aplicativos, e cerca de 76% dos brasileiros são analfabetos digitais[39].

---

[35] BRASIL já é o 5º país com mais usuários de internet no mundo. **Forbes, 2022**. Disponível em: <https://forbes.com.br/forbes-tech/2022/10/brasil-ja-e-o-5o-pais-com-mais-usuarios-de-internet-no-mundo/>. Acesso em: 20 mar. 2024

[36] QUANTIDADE de brasileiros com internet, mas sem saneamento básico, equivale à população do Equador. **Revista Piauí, 2023**. Disponível em: <https://piaui.folha.uol.com.br/quantidade-de-brasileiros-com-internet-mas-sem-saneamento-basico-equivale-populacao-do-equador/#:~:text=Em%20janeiro%20deste%20ano,a%20servi%C3%A7os%20de%20saneamento%20b%C3%A1sico.>. Acesso em: 13 jun. 2024.

[37] BRASIL é o terceiro maior consumidor de redes sociais em todo o mundo. **Forbes, 2023**. Disponível em <https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>. Acesso em: 11 jun. 2024.

[38] QUANTIDADE de brasileiros com internet, mas sem saneamento básico, equivale à população do Equador. **Revista Piauí, 2023...**

[39] ANALFABETISMO digital: 76% dos brasileiros não têm habilidades digitais básicas. **Diário do Grande ABC, 2023**. Disponível em: <https://www.dgabc.com.br/Noticia/4063023/analfabetismo-digital-76-dos-brasileiros-nao-tem-habilidades-digitais-basicas>. Acesso em: 17 jun. 2024.

O analfabetismo digital se trata da ausência de conhecimento e familiaridade na utilização de ferramentas digitais comuns e seus aplicativos. Essa vertente do analfabetismo abarca não só os indivíduos que não possuem contato com tecnologias digitais, como também "*compreende aquelas pessoas que manuseiam o computador, mas não sabem utilizar as ferramentas de forma correta*"[40].

Por óbvio, o fenômeno não se restringe à falta de conhecimento sobre o uso de computadores pessoais, abrangendo também celulares, televisão com acesso à internet e *tablet*, e "*traz como consequência a existência de receptores passivos dos meios de comunicação, em lugar de pessoas que interagem, buscam e colaboram entre si, organizando a informação*"[41].

A ausência de senso crítico na análise das informações veiculadas na internet também acomete os analfabetos funcionais, que são pessoas que "*apresentam limitações para fazer uso da leitura, da escrita e da matemática em atividades cotidianas. Isso inclui, por exemplo, reconhecer informações em um cartaz ou fazer operações aritméticas simples*"[42]. Segundo dados divulgados em 2018 pelo Indicador de Alfabetismo Funcional (Inaf), 58% dos analfabetos funcionais brasileiros utilizam o celular e se conectam à internet[43] e, por não terem capacidade analítica, são mais suscetíveis a assimilar e compartilhar desinformações e informações falsas nas redes sociais[44].

Devido ao nível de preparo e educação digital baixos, o avanço da internet no Brasil ainda é lento se comparado com outros países como Chile e Suécia – que se destacam na América Latina e na Europa, respectivamente, por terem índices de qualidade, preparo e educação digital maiores[45]. Mesmo assim, tendo em vista que ela tem se tornado ferramenta

---

[40] FONSECA, Mayara de Sousa Guimarães. CIBERESPAÇO E SUAS CONTRADIÇÕES: a questão do analfabetismo digital. **Revista Igapó**, [S. l.], v. 5, n. 1, 2022. Disponível em: https://igapo.ifam.edu.br/index.php/igapo/article/view/61. Acesso em: 17 jun. 2024.

[41] MALHEIRO, Emerson Penha. DIREITOS HUMANOS NA SOCIEDADE DA INFORMAÇÃO. **Revista Paradigma**, [S. l.], v. 25, n. 1, 2017. Disponível em: https://revistas.unaerp.br/paradigma/article/view/218-230. Acesso em: 17 jun. 2024.

[42] TRÊS em cada 10 brasileiros são analfabetos funcionais**. Revista Educação, 2018**. Disponível em: <https://revistaeducacao.com.br/2018/08/08/tres-em-cada-10-brasileiros-sao-analfabetos-funcionais-1/>. Acesso em: 27 jun. 2024.

[43] USO educacional do celular com internet ajudaria a reduzir analfabetismo funcional. **Inaf, 2020**. Disponível em: <https://alfabetismofuncional.org.br/uso-educacional-do-celular-com-internet-poderia-ajudar-a-reduzir-o-analfabetismo-funcional-no-brasil/>. Acesso em: 27 jun. 2024.

[44]Sobretudo no campo das eleições, ver SPINELLI, Egle Müller; RAMOS, Daniela Osvald. Desordem informacional no ecossistema digital das eleições brasileiras de 2018. **As fake news e a nova ordem (des)informativa na era da pós-verdade.** FIGUEIRA, João; SANTOS, Sílvio (Orgs.). Imprensa da Universidade de Coimbra, 2019. Disponível em: <https://books.uc.pt/chapter?chapter=67856>. Acesso em: 27 jun. 2024.

[45] Os dados são do Relatório Anual "The Inclusive Internet Index 2019", elaborado pela revista britânica *The Economist* e patrocinado pelo Facebook. Fonte: ANALFABETISMO digital segura avanço do acesso à internet no Brasil. **Exame, 2019**. Disponível em: <https://exame.com/tecnologia/alfabetizacao-digital-segura-avanco-do-acesso-a-internet-no-brasil/>. Acesso em: 25 jun. 2024.

inerente nos lares brasileiros por meio da tecnologia, não se pode mais desconsiderar o uso da internet e seu impacto no Brasil e no mundo atual.

Conforme aponta Ligia Capobianco (2010, p. 191), embora as tecnologias de comunicação e informação tenham desempenhado um papel significativo na criação de uma comunidade global, elas ainda não foram suficientes para eliminar as desigualdades econômicas e sociais. Citando diretamente Webb e Schiratto (2007, p. 255-261), Capobianco destaca que a ideia dos autores de que "*tecnologia é igual a conhecimento que é igual progresso*" constitui uma narrativa ideológica, capaz de encobrir ou excluir os interesses políticos por trás de sua criação e disseminação[46].

A exclusão digital não se resume à falta de acesso ao uso de dispositivos como o computador ou o telefone celular, mas está relacionada à incapacidade de pensar e de criar, bem como de organizar novas e justas dinâmicas de produção e distribuição de riqueza, tanto simbólica quanto material, conforme explica Gilson Schwartz (SCHWARTZ, 2000 *apud* PORTO; FADANELLI, 2020, p. 41)[47].

Nessa perspectiva, Ana Paula Porto e Eberson Fadanelli (2020, p. 41) refletem sobre as relações de poder subjacentes. De acordo com os autores, devido ao avanço das redes e das TICs, é essencial considerar como esses conhecimentos e informações são aplicados na criação de novos saberes e dispositivos para o processamento e comunicação de dados. No entanto, esse processo não ocorre de maneira uniforme. Aqueles que têm maior acesso à rede, recursos para adquirir as ferramentas e preparo para utilizá-las conseguem aproveitar muito mais os benefícios que a cibercultura oferece[48].

Nesse contexto, apontam os autores que aqueles que mais dependem do direito à informação e ao conhecimento são justamente os que são excluídos dele. As pessoas economicamente vulneráveis continuam à margem do acesso a novos conhecimentos, debates científicos, informações atualizadas e possibilidades de interação global, além de serem privadas da construção de novos saberes por meio de ferramentas digitais. Dessa forma, as condições sociais desfavorecidas reforçam a exclusão digital, que, por sua vez, perpetua o modelo social tradicional, marcado por divisões de classe e relações de poder hierarquizadas. A exclusão digital, assim, torna-se mais um fator que amplia a exclusão social[49].

---

[46] CAPOBIANCO, Ligia. A Revolução em Curso: Internet, Sociedade da Informação e Cibercultura... p. 191.
[47] PORTO, Ana Paula Teixeira; FADANELLI, Eberson Luiz. CIBERCULTURA, TECNOLOGIAS E EXCLUSÃO DIGITAL. **Revista Literatura em Debate**, [S. l.], v. 14, n. 26, p. 33–44, 2020. Disponível em: https://revistas.fw.uri.br/literaturaemdebate/article/view/2407. Acesso em: 7 out. 2024.
[48] *Idem.*
[49] *Idem.*

Ana Paula Porto e Eberson Fadanelli (2020, p. 42) ressaltam que, além dessa realidade, aqueles com mais oportunidades de acesso, produção e disseminação de informações na rede tendem a ocupar posições mais altas na hierarquia de poder, pois controlam o que será produzido, publicado e o público ao qual será direcionado. Com o avanço da inteligência artificial, surgem mecanismos de controle dessa disseminação, amplamente utilizados por instituições e empresas para promover projetos, ideologias, crenças e produtos. Isso resulta em uma disseminação massiva que busca conquistar novos seguidores para os ideais, valores e comportamentos "vendidos" na rede[50].

Assim, no contexto da cibercultura e da ascensão das novas TICs, a dominação cultural, social e econômica também se manifesta, acentuando não apenas a exclusão digital, mas também social e cultural. Isso ocorre especialmente devido aos diferentes níveis de acesso aos benefícios que a rede oferece. Muitos cidadãos permanecem à margem, fora dos espaços de debate ou sem a capacidade de compreender as intenções por trás das publicações, o que amplia ainda mais as desigualdades no cenário digital[51].

Patrícia Cella (2005, p. 27) afirma que, embora a cibercultura, no contexto da rede mundial de computadores, tenha o potencial de promover maior igualdade entre as pessoas, a globalização, que beneficia principalmente os mais privilegiados, impede que essa igualdade se concretize de forma justa no ciberespaço. Isso é particularmente evidente nas áreas onde ela é mais necessária, como entre as populações em extrema pobreza, que acabam ainda mais marginalizadas nesta nova sociedade digital e intelectual[52].

Na realidade brasileira, como visto anteriormente, a população em situação de maior vulnerabilidade, embora não tenha acesso a saneamento básico, dispõe de acesso a celular e internet. Esse acesso, de certa forma, exerce um impacto em diversos aspectos, como a busca por oportunidades de trabalho, capacitação profissional, obtenção de informações relevantes, acesso a serviços públicos e manutenção de vínculos familiares e sociais por meio das redes sociais, entre outros.

No entanto, esse acesso ao celular e à internet pela população de maior vulnerabilidade não é suficiente para garantir um acesso equitativo às mesmas oportunidades e condições vivenciadas por aqueles que dispõem de maior conforto em seus lares. A ausência de infraestrutura adequada, como saneamento básico e espaços propícios ao estudo ou trabalho

[50] *Ibidem*, p. 42.
[51] *Ibidem*, p. 43.
[52] CELLA, Patrícia de Oliveira Gasieri. Cibercultura: Uma realidade no Mundo Virtual. Revista CESUMAR – Ciências Humanas e Sociais Aplicadas...p. 27.

remoto, limita significativamente o pleno aproveitamento desses recursos tecnológicos, perpetuando desigualdades sociais.

O raciocínio é o mesmo daquele exposto por Lévy (1999, p. 240 *apud* WALDMAN; ZAMBRANO; RONHA, 2023, p. 7). Embora adote uma visão otimista ao tratar da cibercultura, o pesquisador reconhece que ela pode também intensificar desigualdades e exclusão. Ao refletir sobre o surgimento da cibercultura em meio a tantas injustiças e desigualdades sociais, Lévy manifesta uma preocupação relevante e contemporânea no contexto da sociedade da informação. Ele destaca a necessidade de resolver questões práticas e objetivas, como as disparidades no acesso à internet, especialmente no que se refere à qualidade da conexão. Contudo, ele enfatiza que isso, por si só, não basta. É fundamental superar barreiras "humanas", que não se referem à capacidade técnica de enfrentar os desafios da cibercultura, mas sim às atitudes e emoções que acabam agravando as desigualdades[53].

Cumpre-nos, portanto, buscar entender de que forma as vulnerabilidades e desigualdades sociais sentidas no âmbito digital podem impactar na incidência de crimes cometidos no espaço digital. À medida que o acesso à internet e a dispositivos móveis se expandiu globalmente – inclusive, aqui no Brasil –, a falta de habilidades básicas e as desigualdades sociais ainda persistem.

Essas disparidades não estão apenas ligadas à infraestrutura técnica, mas também às "barreiras humanas" – atitudes e comportamentos que podem intensificar desigualdades. Nesse contexto, é necessário questionar se indivíduos que enfrentam limitações no acesso à internet de qualidade ou à informação digital estão mais suscetíveis (ou não) a crimes cibernéticos (especialmente, os patrimoniais), enquanto outros, com maior domínio da tecnologia, podem tirar proveito dessas fragilidades, agravando ainda mais o cenário de exclusão digital e facilitando a ocorrência de crimes no ambiente virtual.

Para tanto, torna-se necessário adentrar nos conceitos de ciberespaço e cibercrime e, posteriormente, analisar os dados públicos acerca dos crimes patrimoniais (foco desta pesquisa), antes de desbravar a Teoria das Atividades Rotineiras, a que se utiliza para o desenvolvimento das ideias defendidas neste trabalho.

---

[53] WALDMAN, Ricardo; ZAMBRANO, Virginia; RONHA, Amanda Nunes. Erosão do ciberespaço e da cibercultura na privacidade a luz das teorias de Pierre Levy e Manuel Castells. **Revista Direito Mackenzie**, v. 17 n. 1 (2023), p. 7.

2. A NOVA CONFIGURAÇÃO SOCIAL, O CIBERESPAÇO, O CIBERCRIME E A TEORIA DAS ATIVIDADES ROTINEIRAS

2.1. O ciberespaço

As ferramentas tecnológicas de acesso à internet, sobretudo as TICs, reconfiguraram o modo de ser da sociedade. Com a difusão desses mecanismos e a modernização tecnológica, estabeleceu-se um novo espaço para relações sociais e compartilhamento e obtenção de informações: o ciberespaço (espaço digital).

O termo "ciberespaço" surgiu inicialmente em 1984, no romance de ficção científica *Neuromancer* (ou *Neuromante*), escrito pelo norte-americano William Gibson. Na obra, a expressão inventada pelo autor fazia referência ao espaço de dados e universo das redes digitais, que seriam campos de disputa entre multinacionais e palco de outros conflitos em uma sociedade pós-moderna. Posteriormente, o termo foi adotado pelos usuários e criadores de redes digitais[54].

Para Lévy (1999, p. 92), ciberespaço é definido como "*o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores*" e tem como uma de suas principais funções o "*acesso a distância aos diversos recursos de um computador*"[55]. Trata-se do "*universo das redes digitais como lugar de encontros e de aventuras, terreno de conflitos mundiais, nova fronteira econômica e cultural*"[56]. Nas palavras do autor:

> O ciberespaço (que também chamarei de "rede") é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo[57].

[54] LÉVY, Pierre. **Cibercultura**...
[55] *Idem.*
[56] LÉVY, Pierre. **A inteligência coletiva por uma antropologia do ciberespaço**. Tradução: Luiz Paulo Rouanet. São Paulo: Editora Loyola,1998, p. 104.
[57] LÉVY, Pierre. **Cibercultura**..., p. 17.

Ultrapassando limites físicos, o ciberespaço é verdadeiramente desterritorializante e, ao mesmo tempo, cria nova territorialização[58]. De acordo com Lemos (2006), no universo das redes não se encontram fronteiras delimitadas quanto à cultura, economia ou política, sendo possível processos nômades de troca, vinculação e acesso de informação. De acordo com o pesquisador:

> Definimos território através da ideia de controle sobre fronteiras, podendo essas serem físicas, sociais, simbólicas, culturais, subjetivas. Criar um território é controlar processos que se dão no interior dessas fronteiras. Desterritorializar é, por sua vez, se movimentar nessas fronteiras, criar linhas de fuga, re-significar o inscrito e o instituído.

É nesse sentido que, inclusive, o autor se refere à internet como uma "*máquina desterritorializante*". Segundo afirma, a internet des-territorializa "*sob os aspectos político (acesso e ação além de fronteiras), econômico (circulação financeira mundial), cultural (consumo de bens simbólicos mundiais) e subjetivo (influência global na formação do sujeito)*"[59].

No entanto, Lemos (2006) destaca que "*não existe desterritorialização sem reterritorialização e não há formação de território que não deixe aberto processos desterritorializantes*". Para o autor, o ciberespaço "*nasce como espaço estriado, território controlado pelo poder militar e industrial e vai sendo, pouco a pouco, des-re-territorializado por novos agenciamentos da sociedade (tensões de controle e acesso informacionais)*". No mesmo sentido, são as tecnologias de comunicação móveis[60]:

> As tecnologias de comunicação móveis são tidas como desterritorializantes, instituintes de processos nômades, justamente por criar deslocamentos de corpos e informação. (...) As tecnologias móveis permitem exercer um maior controle sobre o espaço e o tempo, agindo também como ferramentas de territorialização. Por instituir formas de controle, através de uma justaposição do espaço eletrônico e físico, tecnologias móveis criam territorializações e controles informacionais, podendo ou não criar procedimentos nômades.

Ou seja, tanto o ciberespaço quanto as tecnologias utilizadas para navegação nesse universo são desterritorializantes na medida em que permitem a mobilidade, especialmente das informações; e, também, são territorializantes, porque permitem que as pessoas tenham maior controle sobre o espaço e o tempo[61]. Nessa perspectiva, com o "*uso dessas tecnologias móveis*

---

[58] LEMOS, André. Ciberespaço e tecnologias móveis: processos de territorialização e desterritorialização na cibercultura. In: **Comunicación local: da pesquisa á producción...**

[59] *Idem.*

[60] *Idem.*

[61] FONTES, Gabriela Scroczynski; LIMA E GOMES, Icléia Rodrigues de. Cibercidades: as tecnologias de comunicação e a reconfiguração de práticas sociais. **Informação & Informação**, [S. l.], v. 18, n. 2, p. 60–76,

de comunicação as pessoas conseguem quebrar a barreira espaço/tempo e agilizar/acelerar o processo de comunicação, independentemente do local físico onde estão e passam a controlar informações"[62].

Entre diversas (des)territorializações, o universo virtual proporcionou novas formas de relacionamento entre as pessoas. Com a criação de *blogs*, redes sociais, correios eletrônicos, plataformas digitais, SMS e outros tantos aplicativos virtuais, passaram a existir diversos espaços de interação e de diferentes nichos sociais, onde pessoas se conectam, conversam e realizam diversas atividades no ciberespaço. Nas palavras de Marcos Cesar Weiss (2019)[63], ao discorrer sobre a transformação digital no corpo social:

> A vida humana tem sido marcada pelas novidades, pelas mudanças, decorrentes de sua inegável inventividade. Hoje nos encontramos e nos relacionamos no mundo virtual. Já não nos reunimos em torno da fogueira ou ao pé do rádio, como faziam nossos antepassados. Nossas fogueiras e rádios agora se chamam redes sociais e tudo sugere que não poderemos delas nos desvencilhar sem danos.

Há, portanto, novas concepções quanto a noção de espaço público e privado. A internet sem fio, os dispositivos inteligentes e os celulares avançados trazem novos desafios, como a apropriação do espaço público (quando nos conectamos à internet em uma praça ou usamos o celular em meio à multidão), a questão da privacidade (à medida que deixamos rastros de nossas atividades diárias) e as novas formas de interação social em grupo, como as *smart mobs*[64].

De acordo com Lemos (2018), os conceitos de espaço de lugar e de espaços de fluxos estão sendo reformulados diante das novas tecnologias de comunicação sem fio. Para o autor, nas cidades contemporâneas, os espaços de lugar tradicionais, como ruas, praças, avenidas e monumentos, estão gradualmente se convertendo em espaços de fluxos, que são flexíveis e comunicacionais, conhecidos como "lugares digitais"[65].

As cidades contemporâneas são, portanto, o produto das transformações que ocorreram após a revolução industrial, ou seja, são resultado das mudanças nas cidades industriais no início do novo milênio[66]. Com as novas TICs e com a atual cibercultura, a cidade contemporânea é

2013. DOI: 10.5433/1981-8920.2013v18n2p60. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/16161. Acesso em: 30 jul. 2024.

[62] *Idem.*

[63] WEISS, Marcos Cesar. Sociedade sensoriada: a sociedade da transformação digital. **Estudos Avançados**, v. 33, n. 95, p. 203–214, jan. 2019. Disponível em: <https://doi.org/10.1590/s0103-4014.2019.3395.0013>. Acesso em: 03 jul. 2024.

[64] De acordo com Lemos, *smart mobs* é um termo cunhado por H. Rheingold (2002) para definir as novas formas de agrupamento que utilizam tecnologias móveis, como celulares com voz e SMS, internet sem fio, blogs, entre outros. Os propósitos dessas mobilizações são variados. LEMOS, André. Cibercultura y movilidad: una era de conexión**. Razón y Palabra**...

[65] *Idem.*

[66] SANTOS, Gláucia Regina Silva; BARROS, Glhevysson Santos. Um olhar sobre as cidades contemporâneas: dinâmica de organização e funcionamento. **Revista Eletrônica do Instituto de Humanidades**, [S. l.], v. 24, n.

"*preenchida e complementada por novas redes telemáticas - e as tecnologias daí derivadas (internet fixa, wireless, celular, satélites, etc) - que se somam às redes de transporte, de energia, de saneamento, de iluminação e de comunicação*"[67].

Também chamada de cidade-ciborgue, a cidade contemporânea, devido à sua estreita conexão com as redes telemáticas, é formada pelo espaço de fluxo, assim definido por Castells (1996: 412 *apud* LEMOS, 2004) como

> a organização material de tempo-compartilhado de práticas sociais que funcionam por fluxos. Por fluxo eu entendo sucessões propositadas, repetitivas, programáveis de troca e interação entre posições fisicamente deslocadas, organizadas por atores sociais nas estruturas econômicas, políticas e simbólicas de sociedade.

Lemos (2018) ainda destaca que a cidade sempre foi um artefato, mas a particularidade atual está em sua estreita conexão com as redes telemáticas. Para ele, as tecnologias digitais e as novas formas de conexão sem fio permitem usos mais flexíveis do espaço urbano: acesso nômade à internet, conectividade contínua por meio de celulares, objetos inteligentes que transmitem informações para diversos dispositivos, etiquetas de rádio frequência (RFID) que possibilitam o rastreamento de objetos, equipamentos com *bluetooth* que criam redes locais, entre outros. Esses impactos tornam-se cada vez mais evidentes. A cidade contemporânea está se transformando em uma cidade da mobilidade, onde as tecnologias móveis integram-se às suas paisagens[68].

O ciberespaço está profundamente integrado à cidade contemporânea, funcionando como uma extensão do ambiente urbano físico. Ele não apenas amplia as interações sociais, mas também redefine os fluxos de comunicação e informação, conectando indivíduos e comunidades em tempo real, independentemente da localização geográfica. Nesse sentido, o ciberespaço se torna uma parte essencial das dinâmicas urbanas modernas, complementando os espaços de fluxo das cidades e contribuindo para a formação de uma rede global de trocas e interações. A cidade contemporânea, portanto, não é apenas um espaço físico, mas um ambiente híbrido, onde o digital e o material coexistem e se entrelaçam.

50, p. 26–36, 2020. Disponível em: https://publicacoes.unigranrio.edu.br/reihm/article/view/6333. Acesso em: 1 out. 2024.

[67] LEMOS, André. Cidade-ciborgue: a cidade na cibercultura. **Galáxia**, n. 8, p. 129-148, 2004.

[68] LEMOS, André. Cibercultura y movilidad: una era de conexión**. Razón y Palabra**...

Nesse sentido, destaca Lemos (2004), mais uma vez:

> O espaço de fluxo da cidade-ciborgue não se opõe ao espaço de lugar. Diversos estudos apontam para essa afirmação (Graham e Marvin, 1996; Horan, 2000; Wheeler, Aoyama, Warf, 2000; Mitchell, 2000). A cidade-ciborgue, ao contrário, agudiza a relação entre esses dois espaços. Os espaços de lugar, como ruas, monumentos e praças passam a ser interfaceados pelo espaço de fluxo através dos diversos dispositivos de conexão às informações digitais. As diversas práticas sociais da cibercultura mostram bem essa inter-relação (Lemos 2002, Mccaughrey e Ayers, 2003). Podemos rapidamente exemplificar através de projetos como as diversas experiências com as chamadas cidades virtuais (cidades digitais, cibercidades, etc), a expansão das redes sem fio (wireless), as diversas comunidades e ativistas que usam a rede para agir sobre o local, os fenômenos atuais das Flash Mobs e do Bookcrossing, entre outros mostram a intensa relação entre os dois espaços. O ciberespaço, como afirma Benedikt, aumenta e complexifica a realidade das cidades contemporâneas (Benedikt, 1992)[69].

E as novas relações experienciadas no ciberespaço também são analisadas no campo da psicologia. Em uma análise da nova realidade, as psicólogas Taziane Silva, Talita Teixeira e Sylvia Freitas (2015) destacam que a comunicação online "*promove um espaço para as pessoas se expressarem sem restrições, emitirem as suas opiniões, contudo essa exposição de opinião, muitas vezes sem o senso de alteridade que requer o cuidado com o outro, resulta, com a mesma agilidade e facilidade, no rompimento das relações*"[70]. De acordo com as autoras:

> Nessa nova plataforma da realidade, o homem experimenta e conhece outras formas de ser, logo também realiza novos projetos de existência. Na relação com o outro, a internet agencia novos modos de relacionamento, o que nos leva a indagar se as relações no ciberespaço tornam as pessoas mais próximas ou distantes. A atitude solitária diante dos aparatos que nos conectam em rede é um cenário contraditório.
> (...)
> Ao pensar nos laços afetivos no ciberespaço, Castells (2006) pontua que a rede é um espaço apropriado para a diversidade de sua produção, sendo esses laços muitas vezes frágeis, úteis na divulgação de informações e levantamento de possibilidades. Uma vantagem da rede é a criação desses laços com pessoas até então desconhecidas, de um modo igualitário de interação, na qual os aspectos sociais têm menor influência. Percebe-se que, diferentemente da Era Industrial, na Era do Conhecimento, o homem tem uma ampla possibilidade de relações sociais que não se restringem mais aos limites de seu contexto físico, mas essa mesma amplitude limita o envolvimento necessário para apurar os critérios de julgamento.

[69] LEMOS, André. Cidade-ciborgue: a cidade na cibercultura. **Galáxia**...

[70] SILVA, Taziane Mara da; TEIXEIRA, Talita de Oliveira; FREITAS, Sylvia Mara Pires de. Ciberespaço: uma nova configuração do ser no mundo. **Psicol. rev. (Belo Horizonte)**, Belo Horizonte, v. 21, n. 1, p. 176-196, jan. 2015. Disponível em <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-11682015000100012&lng=pt&nrm=iso>. Acesso em 01 ago. 2024.

Nesse sentido, o ciberespaço seria um "*campo gerador de infinitas possibilidades interativas, um novo espaço de comunicação, de sociabilidade, de reconfiguração de identidades, para além de sua dimensão mais visível e pragmática, que é organização e transação da informação e do conhecimento*"[71].

Para Cynthia Gontijo, Ivone Silva, Adalci Viggiano, Edmilson Paixão e Antônio Tomasi (2007), há três mudanças que concretizam o ciberespaço "*como um universo aglutinador de todas essas possibilidades*", que são: 1) mudança na tecnologia informática, tendo em vista que a tela do computador passa a também ser ambiente de manipulação, possibilitando múltiplas conexões; 2) mudança na esfera social, já que há a emergência de um novo espectador, menos passivo, que aprende com o mouse; e 3) mudança no cenário comunicacional, considerando a transição da lógica da comunicação (interatividade) entre usuários, que deixou de ser o mero "emissor-mensagem-receptor"[72].

E como consequência do surgimento desse novo universo, as diversas mudanças significativas existentes acabaram por criar uma nova configuração social, isto é, um novo meio de relacionamento entre as pessoas. Conforme destaca Spencer Toth Sydow (2023, p. 31), as pessoas estão mais tempo sozinhas, interagindo e se comunicando virtualmente. A presença física foi substituída pela "presença virtual", com a mediação de computadores controlados por seus usuários. As barreiras geográficas foram praticamente superadas, impactando significativamente o comércio[73].

Por consequência disso, e por ser mais prático e ágil, Sydow (2023, p. 31) destaca que o ambiente digital foi cada vez mais adotado, atraindo mais investimentos, maior confiança e se consolidando como padrão. Como resultado, tornou-se também um espaço com grande potencial para gerar lucros e benefícios, "*tornando-se alvo da delinquência por conta da sua potencialidade, suas vulnerabilidades, erros de programação, falhas de segurança, técnicas de sobrepujamento, engenhosidade social e até mesmo por mero lazer*"[74].

É nesse cenário que emerge o **cibercrime**. Em que pese as inúmeras vantagens e oportunidades proporcionadas pelo ciberespaço, como a facilidade de comunicação, acesso à informação e desenvolvimento econômico, há também aqueles que o utilizam para fins ilícitos,

---

[71] GONTIJO, Cynthia Rúbia Braga; SILVA, Ivone Maria Mendes; VIGGIANO, Adalci Righi; PAIXÃO, Edmilson Leite; TOMASI, Antônio de Pádua Nunes. Ciberespaço: que território é esse?. **Educ. Tecnol.**, Belo Horizonte, v. 12, n. 3, p. 34-38, set./dez. 2007.
[72] *Idem.*
[73] SYDOW, Spencer Toth. **Curso de Direito Penal Informático** – Partes Geral e Especial – 4. ed. rev. e atual. – São Paulo: Editora Juspodivm, 2023. p. 31.
[74] SYDOW, Spencer Toth. **Curso de Direito Penal Informático...** p. 31.

aproveitando-se de suas vulnerabilidades para cometer crimes e explorar suas brechas de segurança.

2.2. O cibercrime

Cibercrime, ou crime cibernético, trata-se dos "*delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral)*"[75]. Pode ser entendido como uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou *hackers* com fins lucrativos; ocasionalmente, o crime cibernético visa danificar computadores ou redes por outros motivos (pessoais ou, até mesmo políticos) que não o lucro[76].

Não há consenso na doutrina (e, muito menos, na legislação ou jurisprudência) quanto a nomenclatura correta para referenciar os delitos cometidos nessa modalidade. Para além do termo crime cibernético ou cibercrime, há ainda quem utiliza a nomenclatura de crime digital, crime virtual, crime informático, entre outras. Todas elas trazem, em certa medida, limitações e contribuições.

O termo "crime digital" surge a partir da relação com o dígito binário (*binarydigit*), sistema que consiste apenas nos valores 0 (desligado) e 1 (ligado) para realizar operações computacionais[77]. Por sua vez, a nomenclatura "crime virtual" surge com o objetivo de diferenciar o mundo real do mundo virtual, de forma que os crimes cometidos no mundo criado pelos sistemas computacionais herdariam esse termo[78].

Por outro lado, há quem adote o termo "crime informático", por considerá-lo mais adequado e específico, como fazem Túlio Vianna e Felipe Machado[79], e Grégore Moura[80]. Para os autores, a referida nomenclatura estaria mais adequada aos propósitos legislativos e ao sistema penal, sobretudo quando se fala sobre inviolabilidade das informações automatizadas (dados), tendo em vista que a ciência que tem como objeto de estudo os dados automatizados seria a Informática.

---

[75] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação – 2. ed. – Rio de Janeiro: Brasport, 2013. p. 18.
[76] O QUE são crimes cibernéticos e como se proteger deles?. **Kaspersky, 2024**. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acesso em: 15 out. 2024.
[77] MOURA, Grégore Moreira de. **Curso de direito penal informático** – 1. ed. – Belo Horizonte, São Paulo: D'Plácido, 2021, p. 29.
[78] *Ibidem*, p. 30.
[79] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2003. p. 22.
[80] MOURA, Grégore Moreira de. **Curso de direito penal informático...** p. 32.

Inobstante as justificativas empregadas em cada um desses termos, o presente estudo adota a nomenclatura de cibercrime (e crime cibernético), em razão da popularidade da palavra, por ser mais utilizada pela doutrina internacional e por se referir especificamente ao ciberespaço. Ainda, considera-se que as delegacias e promotorias especializadas em crimes desta espécie comumente fazem referência ao termo "crimes cibernéticos", como a Delegacia Especializada em Investigação de Crimes Cibernéticos, localizada em Belo Horizonte/MG; e o Grupo de Atuação Especial de Combate aos Crimes Cibernéticos (GAECIBER), do Ministério Público de Minas Gerais (MPMG).

Além disso, o termo "crime cibernético" é utilizado na Convenção de Budapeste de 2001, que foi promulgada no Brasil em 2023 pelo Decreto nº 11.491/2023. Também chamada de Convenção sobre o Crime Cibernético, ela foi resultado de uma preocupação advinda da Conselho da Europa na década de 1980 quanto aos crimes envolvendo computadores e tecnologia da informação[81].

O texto da convenção é composto por três capítulos, sendo que o primeiro estabelece conceitos fundamentais para garantir a mútua compreensão e o desenvolvimento dos trabalhos; o segundo aborda as medidas a serem implementadas nas jurisdições nacionais, dividindo-se nas seções de Direito Penal, de Direito Processual e de Jurisdição; e o terceiro trata da cooperação internacional, destacando princípios e mecanismos de assistência jurídica entre os países[82]. Aberta para assinatura em 2001, em Budapeste, a Convenção foi ratificada por 68 (sessenta e oito) Estados, membros e não membros do Conselho da Europa. O Brasil, em específico, ratificou a Convenção em 2022 e a promulgou internamente em 2023[83].

Por essas razões é que se adota a nomenclatura **cibercrime** no presente trabalho. Conforme orientam Ana Maria Murata e Paula Ritzmann Torres (2023, p. 13), os termos "cibercrime" ou "criminalidade cibernética" não são terminologias legais, definidas por lei, mas termos casuais[84]. As autoras também afirmam que "*Para ser cyber não basta estar relacionado a um computador, mas sim conectado à rede*"[85] e, por esse motivo

> [N]os Estados Unidos, Reino Unido, Canadá e Austrália, utiliza-se a classificação de delitos *cyber*-capacitados e *cyber*-dependentes; o primeiro grupo contemplando aqueles cometidos por meio da tecnologia da informação e comunicação (TIC) e que a tem como alvo (hacking, malware, pirataria digital etc.), e o segundo que pode ser

[81] LUMI KAMIMURA MURATA, Ana Maria; RITZMANN TORRES, Paula. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [S. l.], v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 15 out. 2024.
[82] *Idem.*
[83] *Idem.*
[84] *Idem.*
[85] *Idem.*

> cometido sem o uso de TIC, mas que, quando a utiliza, há uma mudança significativa de escala e alcance (fraudes por pirâmide, cyber-pornografia, apostas online)[86].

De acordo com Emerson Wendt e Higor Jorge (2013, p. 18), os crimes cibernéticos podem ser divididos em *(i)* crimes cibernéticos abertos e *(ii)* crimes exclusivamente cibernéticos. Os crimes cibernéticos abertos "*são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele*"[87], de forma que bem jurídico tutelado é variável (pode ser a honra, o patrimônio, a liberdade sexual, entre outros)[88].

A exemplo, cita-se os crimes contra a honra (calúnia, difamação e injúria, previstos respectivamente nos arts. 138, 139 e 140 do Código Penal brasileiro), em que é possível a sua prática independentemente do uso de computadores ou da internet. No entanto, se o crime for cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, há a incidência da causa de aumento de pena (majorante) prevista no art. 141, §2º, do Código Penal, aplicando-se em triplo a pena.

Por sua vez, os crimes exclusivamente cibernéticos seriam aqueles que "*somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem acesso à internet*"[89]. Seriam, portanto, aqueles crimes em que o tipo penal exige o necessário uso do computador ou da rede mundial de computadores, ou a invasão desses dispositivos, para a sua consumação; e cujo bem jurídico tutelado é a inviolabilidade da informação automatizada[90]. Como exemplo, há o crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, bem como os crimes de inserção de dados falsos em sistema de informações (art. 313-A, Código Penal) e de modificação ou alteração não autorizada de sistema de informações (art. 313-B, Código Penal).

No Brasil, o legislador encontra-se atento às práticas criminosas realizadas no âmbito virtual. Nos últimos anos, foram criados, por meio de leis, diversos tipos penais, agravantes e causas de aumento que buscam criminalizar e punir, de forma mais rígida, atos ilícitos praticados por meio de redes sociais e meios eletrônicos, no geral.

Em 2012, foi sancionada a Lei nº 12.737/12, também conhecida como Lei Carolina Dieckmann, que alterou o Código Penal e acrescentou o art. 156-A, tipificando a conduta de

---

[86] *Idem.*
[87] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos...** p. 18.
[88] Também classificados como crime informáticos impróprios. MOURA, Grégore Moreira de. **Curso de direito penal informático...** p. 33.
[89] *Idem.*
[90] Também classificados como crime informáticos próprios. MOURA, Grégore Moreira de. **Curso de direito penal informático...** p. 33.

invasão de dispositivo informático (conforme mencionado), e incluiu o §1º ao art. 266 ("interrupção ou perturbação de serviço telegráfico ou telefônico"), "*por meio do qual se ampliou o âmbito de proteção da norma penal aos serviços informáticos, telemáticos ou de informação de utilidade pública*"[91]. A referida lei surgiu após terem sido divulgadas fotos íntimas da atriz brasileira Carolina Dieckmann, acessadas por meio de invasão de seu computador particular, e foi a pioneira no país a tratar de crimes envolvendo dispositivos informáticos.

Em 2019, a Lei nº 13.968/19 alterou a redação do crime de induzimento, instigação ou auxílio a suicídio ou a automutilação, previsto no art. 122 do Código Penal, e, dentre outras mudanças, passou a prever que a pena deve ser aumentada até o dobro se a conduta é realizada por meio da rede de computadores, de rede social ou transmitida em tempo real (art. 122, §4º); e deve ser aumentada em metade se o agente é líder ou coordenador de grupo ou de rede virtual (art. 122, §5º). À época, o projeto de lei visava combater e punir práticas nocivas que estavam se disseminando pelas redes sociais, como o jogo da Baleia Azul, que desafiava jovens a cumprirem uma série de tarefas perigosas, culminando com a automutilação ou até mesmo o suicídio[92].

Anos depois, com a prática recorrente de golpes virtuais que visavam obtenção de vantagem ilícita, foi sancionada a Lei nº 14.155 em 2021, que aprimorou a redação do art. 156-A e aumentou significativamente suas penas. Além disso, introduziu no Código Penal dois novos crimes específicos: o de furto mediante fraude eletrônica (art. 155, §4º-B do CP) e o de fraude eletrônica (art. 171, §2º-A do CP). Ao apresentar o projeto de lei que originou à referida alteração legislativa, o Senador responsável apontou que o Brasil ocupava o terceiro lugar no *ranking* mundial em registros de fraudes eletrônicas e que as punições para esse tipo de prática, até então, eram brandas[93].

Em 2024, a Lei nº 14.811/24, respaldada na Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente, alterou o Código Penal e a Lei nº 8.072/90 (Lei dos Crimes Hediondos) para introduzir os crimes de intimidação sistemática

---

[91] WOJCIECHOWSKI, Paola Bianchi. A fábrica midiática de inimigos e o risco à democracia. Uma análise do papel dos grandes meios de comunicação na elaboração e adoção de leis penais casuísticas no Brasil. **Sistema Penal & Violência**, Porto Alegre, v. 7, n. 1, p. 49-65, jan.-jun. 2015. p. 59.

[92] BARBOSA, R. da S.; CURY, L. V. M.; BOTELHO, G. S. Induzimento, instigação e auxílio ao suicídio no ambiente virtual a partir da Lei 13.968/2019. **STUDIES IN SOCIAL SCIENCES REVIEW**, [S. l.], v. 5, n. 1, p. 39–57, 2024. DOI: 10.54018/sssrv5n1-003. Disponível em: https://ojs.studiespublicacoes.com.br/ojs/index.php/sssr/article/view/4468. Acesso em: 24 oct. 2024.

[93] LEI com penas mais duras contra crimes cibernéticos é sancionada. **Agência Senado, 2021**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada>. Acesso em: 24 out. 2024.

(*bullying*) e intimidação sistemática virtual (*cyberbullying*), por meio do art. 146-A e parágrafo único, do Código Penal; e tornar hediondo o crime do art. 122, *caput* e §4º, do Código Penal (induzimento, instigação ou auxílio a suicídio ou a automutilação realizados por meio da rede de computadores, de rede social ou transmitidos em tempo real).

Além disso, também foi alterada a Lei nº 8.069/90 (Estatuto da Criança e do Adolescente) para punir quem "*exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de cena de sexo explícito ou pornográfica com a participação de criança ou adolescente*" (art. 240, §1º, II, ECA).

No entanto, as diversas alterações nas leis penais por vezes surgem como resultado do clamor social, midiático e do populismo penal, razão pela qual recebe diversas críticas de parte da doutrina – que se manifesta contra a expansão do Código Penal e do direito penal para atender demandas populares que, em maioria, são desacompanhadas de estudos e medidas eficazes que visam de fato mitigar a prática criminosa. O exemplo mais recente é a criminalização do *cyberbullyng*, em que, apesar da boa intenção do legislador (de punir o *bullying* praticado no âmbito virtual), o tipo penal possui redação repetitiva e, a depender da situação, "*o crime já nasce em desuso*", já que a sua redação pode gerar confusão ao se sobrepor a crimes já previstos no ordenamento jurídico, como injúria, difamação ou ameaça, que também podem ser aplicados em casos de condutas virtuais[94].

Inobstante as ponderadas (e necessárias) críticas de parte da doutrina, fato é que o legislador brasileiro vem buscando adequar a legislação nacional à nova realidade de crimes cibernéticos, em resposta ao avanço tecnológico e ao crescimento expressivo de delitos praticados no ambiente digital. Em certa medida, a criação de novos tipos penais, focados especialmente na prática de delitos envolvendo dispositivos eletrônicos, redes sociais e a rede mundial de computadores, surgem como forma de buscar aplicar, de fato, a lei penal àqueles que supostamente praticam a conduta criminosa – e, consequentemente, puni-los sob a forma da lei.

O Judiciário, de certa forma, também tenta fazer isso. Na rotina dos tribunais, tem sido cada vez mais comum a utilização dos termos "estupro virtual", "extorsão cibernética" ou

[94] ZANI MORGADO, H. Criminalização do bullying e do cyberbulliyng: o Estado penal ataca novamente. **Boletim IBCCRIM**, [S. l.], v. 32, n. 376, p. 27–30, 2024. DOI: 10.5281/zenodo.10685205. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/982. Acesso em: 24 out. 2024.

"sextorsão"[95]. Trata-se de casos em que há a discussão acerca da prática (ou não) dos crimes de estupro e extorsão por meio virtual. Nessas situações, há a profunda e complexa análise dos casos concretos, juntamente com a análise do tipo penal, para que se decida se houve ou não a consumação ou tentativa dos crimes.

Isso porque, conforme destaca Mauro da Fonseca Ellovitch (2023), antigamente as chantagens eram realizadas pessoalmente ou, no máximo, por meio de cartas e telefonemas. O suposto chantagista precisava estabelecer algum contato direto com a vítima e, para forçar alguém a realizar algo contra sua vontade, com uma finalidade financeira, como descrito no art. 158 do Código Penal, também precisava possuir uma informação confidencial e valiosa sobre a vítima[96].

Além disso, buscava-se encontrar uma forma de comunicação com ela para apresentar a chantagem e definir o método de pagamento do benefício ilícito. Com frequência, exigia-se que a vítima pagasse em dinheiro em um local específico, evitando assim a identificação das contas dos infratores. Esses fatores tornavam a chantagem um crime mais "pessoal", o que limitava o alcance dos delitos e facilitava a identificação do suposto chantagista[97]. Da mesma forma, para a ocorrência do crime de estupro, era indispensável a presença do suposto autor e a conjunção carnal ou o ato libidinoso com a vítima para a consumação do crime.

Com a era digital, destaca o autor que "*O chantagista não precisa mais conhecer antecipadamente nada sobre seu alvo para chantageá-lo. Basta usar malwares, engenharia social e/ou avatares*"[98]. Nesse sentido, por meio de técnicas de invasão usando programas maliciosos e ataques a vulnerabilidades de dispositivos, os supostos *cybercriminosos* acessam remotamente bancos de dados, fotos, vídeos e conversas sensíveis de alvos, usando essas informações para golpes ou extorsões.

Agora, "*a chantagem é enviada por meio de contas de aplicativos de mensagens ou de e-mails, criados facilmente com dados cadastrais falsos*" e "*a obtenção do proveito econômico ilícito nesse novo cenário também pode acontecer de modo a dificultar ainda mais a investigação, com o uso de criptomoedas ou de transferências digitais (especialmente por PIX) para contas criadas em nome de 'laranjas' em bancos digitais*", não sendo necessário haver

[95] ELLOVITCH, Mauro da Fonseca. Extorsão cibernética, estupro virtual e sextorsão: a chantagem na era digital. **Consultor Jurídico, 2023**. Disponível em: <https://www.conjur.com.br/2023-dez-16/extorsao-cibernetica-estupro-virtual-e-sextorsao-a-chantagem-na-era-digital/>. Acesso em: 05 nov. 2024.
[96] *Idem.*
[97] *Idem.*
[98] *Idem.*

um local físico para a obtenção da vantagem ilícita[99]. No caso do "estupro virtual", o Promotor destaca que:

> Quando, ao invés de visar o auferimento de vantagem econômica, a grave ameaça é voltada à obtenção da prática de atos libidinosos através da internet; temos não a extorsão, mas sim o chamado "estupro virtual". Utilizando-se dos supramencionados artifícios de malwares, engenharia social e/ou avatares, o chantagista consegue obter dados pessoais tão valiosos a ponto de conseguir coagir a vítima à humilhação de praticar atos de natureza sexual em meio cibernético. Apesar da semelhança com a extorsão no modus operandi, no "estupro virtual" o agente visa a satisfação da concupiscência própria ou de terceiros e a objetividade jurídica é a liberdade/dignidade sexual da vítima.
> Mesmo a consumação do estupro em meio cibernético agora independe do encontro presencial entre o estuprador e o violado, podendo ser realizado o ato libidinoso completamente on-line. As vítimas são constrangidas a praticarem atos de natureza sexual, como se masturbarem, em frente a webcams e até mesmo a praticarem atos de sadomasoquismo transmitidos pela internet para a satisfação da libido do chantagista. Quanto mais o alvo cede à grave ameaça, mais o predador sexual obtém material para alavancar as chantagens e aumentar a gravidade do que passa a exigir da vítima.

Fato é que, mesmo com as tentativas do legislador e do Judiciário nos processos de criação e aplicação das leis penais, a dificuldade de punição para esse tipo de criminalidade é manifesta. Há não apenas as questões relacionadas às exigências do tipo penal (isto é, para que uma conduta seja considerada criminosa, é necessário que ela se adeque ao tipo penal e preencha os elementos objetivos e subjetivos contidos na norma, sob pena de ser atípica e, por isso, não punida), mas, antes disso, a dificuldade de identificação e localização dos possíveis infratores.

Essa situação ocorre porque, em geral, os supostos criminosos utilizam redes de internet disponíveis em locais públicos, como shoppings, praças e *lan houses*, entre outros[100]. Nesses casos, a transmissão de dados fica desprotegida, o que facilita a interceptação da atividade criminosa, mas dificulta a identificação dos responsáveis[101]. Conforme afirma Ludimila de Freitas Souza e André de Paula Viana[102]:

> Uma das questões mais complexas que envolvem os crimes virtuais e digitais é a identificação do usuário, devido aos hackers nem sempre é fácil rastrear o IP (Internet Protocol ou em português Protocolo de internet), o qual identifica o usuário, o qual atualmente só é fornecido mediante solicitação judicial, a proposta é de que as forças policiais e o MP, possuam acesso de forma livre sem a necessidade de requisitar, até mesmo como forma de agilizar essa identificação e cessar o crime, pois esse dado deve oferece, nome, filiação e o endereço domiciliar do indivíduo, cabe aqui ressaltar que muitos criminosos aproveita-se de lan house para o cometimento do crime, o que

---

[99] *Idem.*
[100] ZACARIAS, Fabiana; FREIRE, Lucas Zacharias. Crimes virtuais: análise das dificuldades e limitações ao combate. **REVISTA JurES** - v.16, n.29, p. 29-61, jun. 2023. p. 55.
[101] *Idem.*
[102] SOUZA, Ludimila de Freitas; VIANA, André de Paula. Marco civil da internet e os crimes virtuais. **Conteúdo Jurídico, 2021**. Disponível em:https://conteudojuridico.com.br/consulta/Artigos/51965/marco-civil-da-internet-e-os-crimes-virtuais. Acesso em: 05 nov. 2024.

> dificulta e muito a identificação, sem contar ainda que softwares atuais conseguem mascarar o IP, ou os provedores se mostram carentes de dados essenciais do usuário.

No mesmo sentido, afirma Grégore Moura (2021, p. 37, nota de rodapé)[103]:

> O desafio no combate aos crimes informáticos é hercúleo, já que o "mundo virtual" se caracteriza pela imediatidade (tudo opera com rapidez e em tempo real), desterritorialidade (os crimes "atravessam" diversos países, o que dificulta a definição da jurisdição e da competência para julgamento, refletindo na apuração dos fatos), imaterialidade (as informações são líquidas) e interatividade (maior interação, mais possibilidade de ocorrência de crimes).

Ou seja, as dificuldades na identificação, localização e punição dos possíveis cibercriminosos permeiam tanto a cibercultura quanto o ciberespaço. Com base no que foi descrito em tópico anterior, observa-se que a cibercultura influencia, a todo momento, a conectividade ampla dos cidadãos ao ambiente virtual. Com isso, conectados ao ciberespaço, que conforme visto neste tópico é amplamente vasto e desterritorializante, observa-se um ambiente atrativo para os cibercriminosos e, ao mesmo tempo, a existência de diversas barreiras tecnológicas e de jurisdição que restringem a possibilidade de rastreamento e punição desses possíveis infratores.

Nesse sentido, com a facilidade de acesso a redes públicas e o anonimato proporcionado pelo ciberespaço, os cibercriminosos encontram um ambiente, de certa forma, favorável para agir, sem grandes receios de serem inicialmente identificados e/ou localizados. A crescente sofisticação dos métodos de ataque e a complexidade de rastreamento dificultam ainda mais o trabalho dos legisladores, das autoridades e do Judiciário, que se veem desafiados a acompanhar a evolução rápida das práticas ilícitas digitais.

Dessa forma, o cenário atual aponta para a necessidade urgente de estratégias mais avançadas de segurança e monitoramento para conter o avanço dessas atividades criminosas. Essas estratégias, no entanto, perpassam pela análise crucial de todo esse cenário da vida real: a cultura da era digital; a intrínseca utilização das TICs, da internet e das redes sociais e de interação do ciberespaço; as dificuldades e a ausência de barreira dos usuários; a criação de leis eficazes e a sua devida aplicação; e as possibilidades para inibição dos cibercriminosos.

E tal análise perpassa não apenas pela leitura dogmática penal e processual penal, mas à interdisciplinaridade entre as áreas do Direito, da Sociologia, da Antropologia, Psicologia e de tantas outras. Para se pensar no crime cibernético (e, sobretudo, nas suas formas de prevenção e punição) é necessário também a analisar o cenário real diante da **criminologia**, dentro das **ciências sociais**.

---

[103] MOURA, Grégore Moreira de. **Curso de direito penal informático...** p. 37.

2.3. A Teoria das Atividades Rotineiras

O comportamento criminoso pode ser analisado por diversas áreas do conhecimento, como Antropologia, Psicologia, Sociologia, Direito e Ciências Sociais. Embora a violência exista desde os primeiros tempos da humanidade, foi somente na segunda metade do século XX que pesquisadores começaram a direcionar sua atenção da figura do criminoso para a vítima[104]. A partir da década de 70, estudiosos americanos começaram a coletar e analisar dados sobre as vítimas de violência. A partir disso, surgiram várias **teorias sobre vitimização**, entre as quais se destacam: a Teoria da Exposição por Estilo de Vida, a Teoria da Anomia, Teoria da Desorganização Social e a Teoria das Atividades Rotineiras[105].

Na expectativa de compreender o fenômeno do crime, cada teoria apresenta recortes de análise distintos, focando em diferentes aspectos do comportamento criminoso, das motivações dos indivíduos e das condições sociais em que o crime ocorre. Enquanto algumas teorias se concentram nas características do criminoso, outras abordam as condições externas, como a estrutura social, as influências culturais e os fatores econômicos.

Em que pese as características de cada teoria da vitimização, a Teoria das Atividades Rotineiras foi a escolhida para o presente estudo, por destacar a influência do ambiente urbano na ocorrência de delitos[106] e, além disso, ser recorrentemente utilizada para analisar crimes contra o patrimônio, como furtos e roubos (que, de certa forma, também são foco do presente trabalho). A Teoria parte do grupo de teorias ecológicas de oportunidade, que preocupam com "*aspectos de natureza ecológica e ambiental na determinação de fenômenos sociais tais como o da criminalidade*"[107] e, por isso, que procura entender a variação nas taxas de crime não pelas características dos infratores, mas pelas condições em que os crimes acontecem[108].

Inicialmente desenvolvida por Lawrence E. Cohen e Marcus Felson em 1979, nos Estados Unidos, a Teoria das Atividades Rotineiras, também conhecida como Triângulo do Crime, busca explicar a ocorrência de crimes com base em **três** elementos principais, que devem convergir, simultaneamente, no tempo e no espaço: *(i)* um potencial ofensor motivado, disposto a cometer um possível crime; *(ii)* um alvo disponível, ou seja, uma pessoa ou objeto a

---

[104] SILVA, Cristiane. Determinantes da vitimização no Brasil. **Revista Cadernos de Economia**, Chapecó, v. 19, n. 35, p. 30-46, jan./jun. 2015, p. 32.
[105] *Idem.*
[106] FARIAS, P. J. L. Respeito às Funções Urbanísticas e a Prevenção da Criminalidade Urbana: Uma Visão Integrada à Luz da Escola de Chicago. **Direito Público**, [S. l.], v. 4, n. 15, 2010. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/1416. Acesso em: 8 nov. 2024. p. 51.
[107] BEATO F, Cláudio; PEIXOTO, Betânia Totino; ANDRADE, Mônica Viegas. Crime, oportunidade e vitimização. **Revista brasileira de ciências sociais**, 2004, 19: 73-89.
[108] *Idem.*

ser atacado; e *(iii)* a ausência de um guardião capaz de proteger o alvo[109]. A relação desses três fatores se daria, portanto, da seguinte forma:

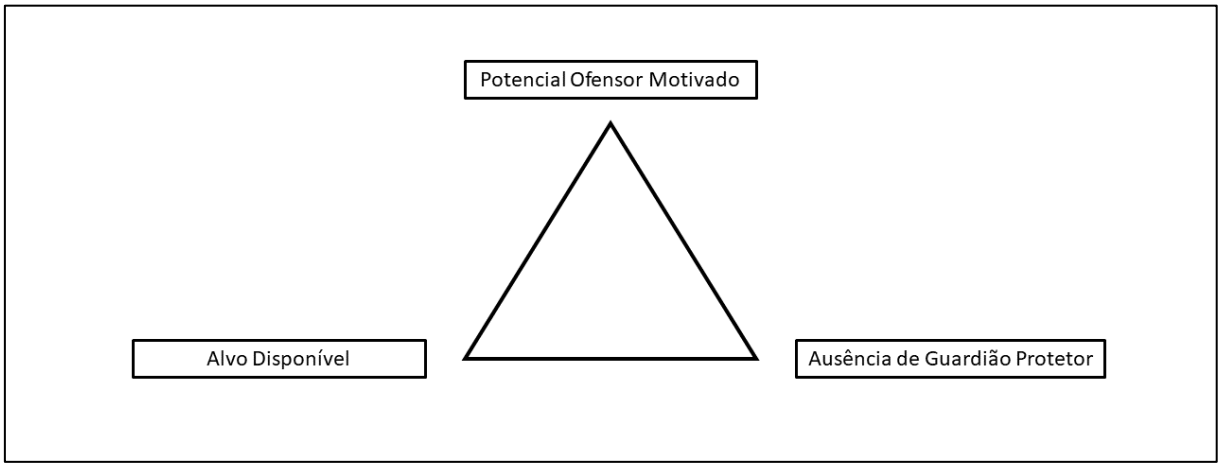

Figura 1 - Cohen e Felson (1979)

De acordo com Cláudio Beato, Betânia Peixoto e Mônica Andrade (2004, p. 74 e 75), em que pese ser um modelo econômico em seus elementos e se tratar de uma abordagem focada nas características ambientais onde ocorrem crimes predatórios, ela ainda mantém alguns pontos em comum com a criminologia mais tradicional, ao enfatizar a motivação dos ofensores como um elemento central[110].

Nessa teoria, a ação predatória é direcionada a "alvos", ou seja, pessoas ou objetos situados em um determinado tempo e espaço, o que acaba por remover o aspecto moral que o termo "vítima" carrega, já que o alvo é definido por seu valor e por certas características que o tornam adequado para a ação predatória[111]. Além disso, os guardiões não se limitam às instituições do sistema de justiça criminal, como é comumente entendido pela criminologia tradicional, de modo que mecanismos de controle social informais também desempenham um papel crucial na ocorrência de delitos, tais como vizinhos, amigos, familiares, transeuntes ou o proprietário do objeto visado[112].

Cohen e Felson demonstram como fatores como o local de residência dos ofensores e das vítimas, o relacionamento entre eles, o local de seus encontros, a idade das vítimas, o

[109] COHEN, Lawrence E.; FELSON, Marcus. Social Change and Crime Rate Trends: A Routine Activity Approach. **American Sociological Review**, vol. 44, no. 4, 1979, pp. 588–608. JSTOR, https://doi.org/10.2307/2094589. Acesso em: 08 nov. 2024.
[110] BEATO F, Cláudio; PEIXOTO, Betânia Totino; ANDRADE, Mônica Viegas. Crime, oportunidade e vitimização. **Revista brasileira de ciências sociais**...
[111] *Idem*.
[112] *Idem.*

número de adultos em uma casa e o horário dos eventos, entre outros, estão associados à frequência de crimes[113]. Dessa forma, no caso de crimes patrimoniais ocorridos em rua, a teoria evidenciou que o aumento de arrombamentos residenciais nos Estados Unidos é relacionado a mudanças na estrutura de emprego na sociedade norte-americana, com um número crescente de pessoas (incluindo mulheres) saindo de casa para trabalhar, deixando as residências mais vulneráveis a atividades predatórias[114]. Trata-se da demonstração de como o "*estilo de vida do indivíduo e as oportunidades geradas por ele influenciam a probabilidade de vitimização*"[115].

Conforme afirmam Cláudio Beato, Betânia Peixoto e Mônica Andrade (2004, p. 76), os principais fatores que aumentam o risco de vitimização dos indivíduos incluem: exposição, proximidade com o agressor, capacidade de proteção, atratividade das vítimas e a natureza dos crimes. A exposição refere-se ao tempo que os indivíduos passam em locais públicos, onde estabelecem contatos e interações sociais. O estilo de vida de cada pessoa influencia a intensidade com que esses fatores se manifestam em sua vida, determinando o grau de exposição em espaços públicos, sua capacidade de proteção, seu nível de atratividade para agressores e a proximidade com eles[116].

A proximidade entre vítima e agressor refere-se à frequência de contatos sociais entre ambos, o que é influenciado pelo local de residência, pelas características socioeconômicas e pelos atributos de idade e sexo, assim como pela afinidade em interesses culturais. Indivíduos da mesma faixa etária tendem a frequentar os mesmos lugares em atividades de lazer[117].

A capacidade de proteção está ligada ao estilo de vida das vítimas. Aqueles que têm maior capacidade de se proteger, evitando contato com possíveis agressores, apresentam menor chance de vitimização. A exemplo, os autores citam que pessoas que usam carro em vez de transporte público têm uma proteção maior, pois reduzem a possibilidade de contato com agressores; da mesma forma, contratar segurança privada diminui as chances de se tornarem vítimas de crime[118].

Em que pese a Teoria das Atividades Rotineiras ter premissas similares à Teoria de Estilo de Vida e Exposição, sua principal diferença é ter sido desenvolvida para entender as variações nas taxas de crime ao longo do tempo; enquanto a Teoria de Estilo de Vida e

---

[113] *Idem.*
[114] *Idem.*
[115] *Idem.*
[116] *Ibidem*, p. 76.
[117] *Idem.*
[118] *Idem.*

Exposição foi elaborada para explicar as diferenças no risco de vitimização entre certos grupos sociais.

Segundo Cohen e Felson (1979), mudanças estruturais nos padrões de atividades rotineiras influenciam diretamente as taxas de criminalidade, pois afetam a convergência no tempo e no espaço dos três elementos essenciais para a ocorrência de crimes. A teoria das atividades rotineiras, portanto, parte do princípio de que diversas transformações sociais na sociedade podem ampliar as oportunidades para a prática de crimes.

Logo, como esses três elementos são essenciais e necessários, a ausência de qualquer um deles é suficiente para impedir a ocorrência de um crime. Além disso, Cohen e Felson observaram que o aumento nas taxas de criminalidade pode ocorrer sem que haja um aumento nas condições estruturais que normalmente motivam os agressores a cometerem crimes, como o desemprego, a segregação racial e a desigualdade econômica[119].

Na perspectiva proposta por Cohen e Felson (1979), as atividades rotineiras são aquelas que ocorrem de maneira recorrente ou constante, como resultado das necessidades básicas da população ou dos indivíduos. Semelhante ao conceito de estilo de vida, essas atividades incluem o trabalho, o lazer e os meios pelos quais as pessoas satisfazem suas necessidades básicas, como alimentação, moradia e outros desejos. Eles argumentam que os indivíduos estão distribuídos em nichos ecológicos com um determinado tempo, local e ritmo, onde a criminalidade pode ser uma forma de alcançar a satisfação dessas necessidades ou desejos às custas de outros[120].

Nesse contexto, as potenciais vítimas, nesses ambientes, constantemente ajustam seus hábitos e ações diárias de maneira que possam atrair ou evitar a atenção de agressores, tornando-se alvos em potencial. As atividades rotineiras das vítimas influenciam, portanto, as condições que aumentam ou restringem as oportunidades para a prática de crimes[121].

Em que pese a teoria ter sido desenvolvida para analisar crimes patrimoniais em ambientes urbanos (físicos), a escolha dessa abordagem teórica para analisar crimes cibernéticos se dá porque a dinâmica subjacente aos delitos no meio virtual frequentemente reflete os mesmos princípios fundamentais que a Teoria das Atividades Rotineiras busca explicar. No ciberespaço, assim como nos ambientes físicos, existem *(i)* indivíduos motivados a cometer crimes, *(ii)* alvos disponíveis para serem atacados e *(iii)* uma ausência de guardiões capazes de proteger esses alvos. Portanto, aplicar essa teoria ao estudo dos cibercrimes oferece

---

[119] *Ibidem*, p. 29.
[120] *Idem.*
[121] *Idem.*

uma estrutura analítica útil para compreender os fatores que influenciam a ocorrência desses crimes e identificar estratégias de prevenção e repressão.

A aplicação da teoria para analisar crimes cometidos no meio digital já foi utilizada em outras oportunidades. No artigo "*Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory*" (em português, "Atividades de rotina on-line e combate à fraude na Internet: ampliando a generalidade da Teoria das Atividades Rotineiras), publicado em 2010, os pesquisadores Travis C. Pratt, Kristy Holtfreter e Michael D. Reisig, da Universidade Estadual do Arizona, nos Estados Unidos, baseiam-se na Teoria das Atividades Rotineiras e na investigação do comportamento do consumidor para compreender como as características pessoais e as rotinas online aumentam a exposição das pessoas a infratores motivados na prática do crime de fraude da internet[122].

A referida pesquisa ampliou a literatura sobre vitimização criminal para o estudo do direcionamento de fraudes na internet – assim como este trabalho busca fazer. De acordo com os pesquisadores, a Teoria das Atividades Rotineiras prevê que mudanças nas estruturas de oportunidades legítimas (por exemplo, a utilização da tecnologia) podem aumentar a convergência de infratores motivados e alvos adequados na ausência de uma tutela capaz. Nesse sentido, consideram que a internet mudou fundamentalmente as práticas de consumo e simultaneamente expandiu as oportunidades para os *cyberfraudadores* atingirem os consumidores online[123].

Citando Newman e Clarke (2003), os autores destacam que as mudanças na sociedade e as mudanças subsequentes nos padrões de criminalidade podem ser atribuídas aos avanços tecnológicos[124]. Segundo os pesquisadores, ao aplicarem a teoria no ciberespaço, Newman e Clarke (2003), perceberam que o principal alvo do crime na internet é a informação e que, em um contexto de fraude na internet, a Teoria das Atividades Rotineiras e a prevenção situacional do crime possuem implicações importantes para a política de controle do crime, na medida em que os potenciais alvos podem ser educados sobre como alterar as suas rotinas online para reduzir as hipóteses de serem alvo de fraude[125].

Comparativamente, no contexto de crimes de rua, os autores destacam que pesquisas de Stewart e Schreck revelaram que estilos de vida desviantes, envolvendo comportamentos

---

[122] PRATT, Travis C.; HOLTFRETER, Kristy; REISIG, Michael D.. Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. **Journal of Research in Crime and Delinquency, 2010...**

[123] *Ibidem*, p. 267.

[124] *Ibidem*, p. 269.

[125] *Ibidem*, p. 270.

ilegais diversos (como prostituição e uso de drogas), aumentam a exposição a ofensores motivados, elevando assim as chances de vitimização violenta. No entanto, a aplicabilidade dos indicadores tradicionais de atividades rotineiras (como estilos de vida desviantes) foi questionada no contexto de fraudes contra consumidores, já que os indivíduos geralmente são alvo de golpistas durante comportamentos rotineiros e escolhas de estilo de vida cotidianas, não desviantes. Ou seja, os tipos de comportamentos rotineiros que poderiam ser considerados arriscados mudam quando se trata de fraudes direcionadas (ou seja, de comportamentos desviantes para não desviantes), e tais comportamentos podem ser específicos para o contexto do ciberespaço[126].

Os pesquisadores destacam que Cohen e Felson (1979) observaram há muito tempo que avanços tecnológicos projetados para fins legítimos podem influenciar a natureza da vitimização criminosa e que, dentre essas mudanças potenciais, as mudanças nas vendas de bens de consumo seria um fator contribuidor para o aumento das oportunidades criminais[127]. Ao final, informam que os resultados da pesquisa parecem ser diferentes daqueles tipicamente associados à vitimização por crimes de rua.

De acordo com os pesquisadores, enquanto a vitimização por crimes violentos de rua geralmente está associada a jovens de minorias masculinas, as vítimas de fraudes na internet tendem a ser mais jovens e mais bem educadas. No entanto, essas diferenças ocultam uma descoberta mais importante: tanto os crimes violentos quanto as fraudes na internet compartilham o mesmo mecanismo causal subjacente, relacionado às atividades rotineiras de potenciais alvos de crimes[128].

Seguindo a mesma linha, o artigo "*Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level*" (em português, "Guardiões nas Alturas: Uma Aplicação da Teoria das Atividades Rotineiras ao Roubo de Identidade Online na Europa nos Níveis Nacional e Individual"), publicado em 2016, destaca que, já que a Teoria das Atividades Rotineiras tem como foco o evento criminoso em vez do criminoso, isso é particularmente saliente para o estudo do cibercrime, pois raramente temos acesso a criminosos cibernéticos para estudar suas motivações (devido aos baixos níveis

[126] *Ibidem*, p. 273.
[127] *Ibidem*, p. 274.
[128] *Ibidem*, p. 285.

de apreensão) e os eventos cibercriminosos são abundantes e deixam para trás assinaturas digitais para análise[129].

De acordo com Matthew L. Williams (2016, p. 23), Newman e Clarke (2003) estavam entre os primeiros a avançar a aplicabilidade da teoria ao crime cibernético e argumentaram que a acessibilidade do alvo na internet (aumentada pela ausência de tutela capaz) e a visibilidade (aumentada pela variedade e frequência de atividades rotineiras online, por exemplo, compras e serviços bancários) são características discriminatórias entre vítimas e não vítimas do crime cibernético[130].

O autor destaca que Yar (2005) descobriu que, com relação aos conceitos centrais da Teoria das Atividades Rotineiras, "infratores motivados" e "tutela capaz" poderiam ser tratados como amplamente semelhantes entre cenários cibernéticos e terrestres. No entanto, a aplicação de "alvos adequados" era problemática, dado que a teoria sustenta que a organização do tempo e do espaço é central para a explicação criminológica[131].

Ainda assim, o ciberespaço é espaço-temporalmente desorganizado (ou seja, a vítima e o infrator raramente estão copresentes). Com isso, Matthew L. Williams rememora que Eck e Clarke (2003) abordam essa questão sugerindo que a teoria pode ser expandida para explicar crimes em que o perpetrador e a vítima não ocupam o mesmo espaço físico. Logo, ao modificar o requisito de espaço físico compartilhado da teoria para incluir uma "rede compartilhada", como a internet, permanece a ideia de que o perpetrador pode alcançar um alvo por meio dessa rede[132].

Sob a mesma perspectiva, mais recentemente Matthew L. Williams e outros pesquisadores publicaram o artigo "*Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory*" (em português, "Medo do Cibercrime Econômico na Europa: Uma Aplicação Multinível da Teoria das Atividades Rotineiras"), em 2023, em que apresenta a aplicação da teoria em crimes econômicos praticados por meio virtual na União Europeia e no Reino Unido. De acordo com a pesquisa, dados europeus sobre crimes e pesquisas criminológicas mostram que, sobretudo após a pandemia por Covid-19, criminosos

[129] WILLIAMS, Matthew L. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level, **The British Journal of Criminology**, Volume 56, Issue 1, January 2016, Pages 21–48, DOI: https://doi.org/10.1093/bjc/azv011.
[130] *Idem*.
[131] *Idem.*
[132] *Idem.*

estão explorando a dependência crescente de tecnologias digitais, e que as taxas de crimes online têm aumentado nos últimos anos, muito mais do que os crimes offline[133].

De todo modo, tanto as pesquisas desenvolvidas por Travis C. Pratt, Kristy Holtfreter e Michael D. Reisig, em 2010, e por Matthew L. Williams, em 2015, nos auxiliam a entender melhor a forma como a Teoria das Atividades Rotineiras contribuem na análise do evento criminoso ocorrido no meio virtual. Com os resultados de estudo publicados pelos pesquisadores, é possível analisar o cibercrime utilizando dos elementos estabelecidos pela teoria sob outra perspectiva.

Enquanto nos ambientes urbanos (físicos) o ofensor motivado geralmente é uma pessoa que se encontra presente fisicamente no local onde se encontra o alvo, no ambiente virtual ele é uma pessoa fisicamente distante, podendo estar em qualquer lugar do mundo, dada a ausência de fronteiras e a desterritorialização do ciberespaço, que contribuem para a dificuldade de localização e identificação do ofensor. No mesmo sentido, condições sociais e econômicas, como desemprego, falta de acesso a recursos e desigualdades, também podem contribuir para a motivação dos ofensores no crime de rua; enquanto que nos crimes virtuais, em que pese a difícil identificação dos autores (que normalmente utilizam rede pública de internet ou bloqueio de IP), pressupõe-se que eles, ao menos *a priori*, possuem certo nível de conhecimento quanto a utilização da internet e das ferramentas digitais e acesso a esses itens (como celular e/ou computador conectados à internet).

O alvo disponível também é lido sob outra perspectiva. Nos crimes patrimoniais cometidos em ambientes urbanos, observa-se que o alvo disponível pode ser, a exemplo, uma casa ou um veículo localizados em áreas de pouca iluminação e vigilância ou com trânsito reduzido de pessoas; ou mesmo uma pessoa localizada em um ponto de ônibus numa rua deserta; ou, ainda, uma pessoa que, transitando em um local aleatório e de pouca observação, deixa sua bolsa aberta ou com pertences à mostra. Diferentemente, nos crimes patrimoniais cometidos no ambiente virtual observa-se que o alvo disponível geralmente é a pessoa que rotineiramente utiliza redes sociais, sites de compras ou sistemas de banco digital.

Por fim, quanto a ausência de um guardião, sabe-se que nos crimes urbanos a presença física de agentes de segurança pública ou de câmeras de vigilância contribuem para a mitigação de crimes. Já no meio virtual, a amplitude do ciberespaço e o anonimato tornam o desafio ainda maior para a prevenção desses crimes, devido as técnicas avançadas utilizadas pelos possíveis

[133] COOK, Steven; GIOMMOLI, Luca; PAREJA, Nicolas Trajtenberg; LEVI, Michael; WILLIAMS, Matthew L. Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory. **The British Journal of Criminology**, 2023, 63, 384–406. DOI: https://doi.org/10.1093/bjc/azac021.

cibercriminosos. Nesses casos, o acompanhamento de atividades suspeitas ou a utilização de sistemas de segurança, como softwares, criptografias, senhas fortes ou sistemas de dupla validação podem ser interpretados como "guardiões" do ambiente virtual.

Nesse sentido, conforme afirmam Solbey Morillo Puente e Iván Neftalí Ríos Hernández, em pesquisa desenvolvida na Universidade de Medellín, na Colômbia, a Teoria das Atividades Rotineiras, aplicada ao ciberespaço, enfatiza três variáveis: *um alvo online adequado*, descrito como comportamentos de uso da internet de uma coisa ou pessoa que é um alvo adequado para o crime; *exposição a um ofensor motivado online*, definida como atividades que expõem indivíduos a um cibercriminoso quando estão conectados à internet; e, por fim, o *guardião capaz*, que inclui pessoas, táticas individuais e ferramentas tecnológicas que podem prevenir potenciais cibercrimes[134].

Inevitavelmente, com a ocorrência da pandemia por Covid-19 e as medidas de restrição que visavam a sua contenção, pessoas de todo o mundo passaram a continuar com as atividades de rotina por meio virtual, como trabalhar, estudar, comunicar, comprar e realizar transações de maneira remota, o que ampliou o uso de plataformas e sistema digitais e, como visto, expôs novos alvos ao cibercrime. Esse cenário aumentou a vulnerabilidade dos usuários a crimes virtuais e, no caso brasileiro, não foi diferente, como visto em tópico anterior.

No entanto, observa-se que a situação do país é ainda mais específica. Conforme observado no início do presente trabalho, a transformação cultural e no espaço urbano promovida ao longo dos anos por conta das TICs e da rede mundial de computadores impactou o país, que hoje ocupa o lugar de terceiro maior consumidor de redes sociais no mundo, mas que possui considerável índice de pessoas que não possuem habilidades básicas digitais, o que pode contribuir para a vitimização dessas pessoas, já que não possuem conhecimento e familiaridade na utilização de ferramentas digitais comuns e seus aplicativos.

Entender tais questões é crucial para se pensar sobre possíveis políticas públicas de enfrentamento a esse tipo de criminalidade no Brasil. Conforme afirma Grégore Moura (2021, p. 59), "*a maior forma de prevenção deste tipo de crime é a educação digital, o que talvez seja um dos grandes desafios da Sociedade 5.0, já que melhorar o bem-estar das pessoas pela tecnologia é criar formas de diminuir a criminalidade informática*"[135].

Para Sydow (2023, p. 808), "*O vitimizador informático não escolhe seu alvo ao acaso*" e a virtualidade "*é um ambiente propício para a execução de delitos, especialmente porque sua*

[134] MORILLO PUENTE, Solbey; RÍOS HERNÁNDEZ, Iván Neftalí. Cibervictimización en el marco de la Teoría de Actividades Rutinarias en la era digital. **Revista de Psicología** (PUCP), 2022, 40.1: 265-291.
[135] MOURA, Grégore Moreira de. **Curso de direito penal informático**... p. 59.

estrutura propicia oportunidade, no sentido de que a contemporaneidade por si só traz a vítima para o ambiente e a vulnerabiliza"[136]. Com isso, o autor afirma que tal fator, somado ao tipo de crime planejado e, também, à "*contribuição do usuário que age negligente ou imprudentemente, faz com que crimes determinados mostrem-se mais fáceis de serem cometidos*"[137].

A esse respeito, Sydow (2023, p. 809) aponta a relevância de se estabelecer uma política criminal voltada aos usuários, já que nos casos do cibercrime "*as ações da vítima têm imensa relevância para o aperfeiçoamento de um delito*"[138] e que é possível dizer que "*boa parte das consequências do ciberespaço seja gerada por ações da própria vítima*"[139]. Nas palavras do autor:

> Diferentemente dos delitos comuns em que cada indivíduo pode eleger formas de se proteger e resguardar (por exemplo indo para a escola acompanhado, contratando um segurança ou até mesmo trancando as portas – elemento guardião ou *guardian*), no delito informático não há mecanismo perfeito de proteção. E é a postura do usuário na virtualidade o principal fator de fragilidade.

Pensamento semelhante é o de Raymond Cox III, Terrance A. Johnson e George E. Richards (*apud* SYDOW, 2023, p. 809)[140]:

> O problema central em policiar a Internet está no fato de que não é possível trazer outros humanos conosco. Não importa o quão sofisticados e complexos os 'policiamentos' para os usuários da Internet são, ainda assim serão todos dispositivos mecânicos. E não são reativos. São elaborados para prevenir ações que já foram identificadas. Não conseguem responder a novas intrusões e atividade criminal.

A proteção dos usuários também é dever do Estado. Seja pela educação, seja pela adoção de medidas de segurança que promovam a conscientização e a prevenção de riscos no ambiente virtual, cabe ao Estado atuar para a proteção de dados, segurança cibernética e prevenção de fraudes digitais. Medidas como a recentemente adotada pelo Banco Central do Brasil (BC) para reduzir a possibilidade de fraudadores utilizarem dispositivos distintos daqueles empregados pelo cliente para gerenciar chaves e realizar transações Pix são cada vez mais necessárias para garantir a segurança dos usuários[141].

---

[136] SYDOW, Spencer Toth. **Curso de Direito Penal Informático**... p. 808.
[137] *Idem.*
[138] *Ibidem*, p. 809.
[139] *Ibidem*, p. 810.
[140] COX III, Raymond W. et al. Routine Activity Theory and Internet Crime. In **Crimes of the Internet**. Pearson Prentice Hall, New Jersey, 2008, p. 313 *apud* SYDOW, Spencer Toth. Curso de Direito Penal Informático... p. 809.
[141] BC aperfeiçoa os mecanismos de segurança do Pix e estabelece 16 de junho de 2025 como nova data de lançamento do Pix Automático. **Banco Central do Brasil, 2024**. Disponível em: < https://www.bcb.gov.br/detalhenoticia/20227/nota>. Acesso em: 09 nov. 2024.

3. O CENÁRIO DOS CRIMES PATRIMONIAIS NO BRASIL: UM "ANTES E DEPOIS" DA PANDEMIA POR COVID-19

Com a imersão da sociedade na era digital, na cibercultura e no ciberespaço, o Brasil passou a ter diversos casos de crimes cibernéticos. De acordo com um estudo realizado pelo *FortiGuard Labs* e publicado pela CNN, apenas no primeiro semestre de 2022, o Brasil registrou cerca de 31,5 bilhões de tentativas de ataques cibernéticos, o que representa um aumento de 94% em comparação com os 16,2 bilhões registrados no ano anterior[142]. Tais dados colocam o Brasil na segunda posição na América Latina em termos de ataques virtuais, ficando atrás apenas do México, que registrou 85 bilhões de tentativas de fraudes digitais, segundo o estudo[143].

Não se pode negar que, devido ao avanço da tecnologia e a crescente digitalização de processos e atividades, o meio virtual tornou-se um ambiente onde ocorrem uma multiplicidade de crimes[144], especialmente os patrimoniais. O uso generalizado da internet e a proliferação de dispositivos digitais proporcionaram aos criminosos novas oportunidades para perpetrar fraudes, roubo de identidade, extorsões e outros delitos financeiros online.

Mesmo diante dos dados, esse fato é de saber notório. Todos os dias, brasileiros e brasileiras se deparam com notícias em jornais ou em mídias sociais acerca da existência de novos golpes virtuais, invasão de contas em redes sociais ou de tentativas diversas de fraudes eletrônicas e bancárias.

Com o intuito de analisar especificamente o cenário dos crimes patrimoniais no país, o presente trabalho examinou dados desse tipo de criminalidade disponíveis no Anuário Brasileiro de Segurança Pública, no período de 2019 a 2024, e publicados pelo Fórum Brasileiro de Segurança Pública[145]. Tratam-se de dados públicos, que podem ser acessados e analisados por qualquer pessoa que ingressar no referido endereço eletrônico.

A escolha da análise do Anuário Brasileiro de Segurança Pública fundamenta-se na confiabilidade e abrangência dos dados fornecidos por essa publicação. O anuário é uma das

---

[142] BRASIL vive aumento no número de crimes cibernéticos. **Valor Econômico, 2023**...

[143] *Idem.*

[144] São diversos os dados tratam sobre o aumento dos crimes de ódio, crimes contra crianças e adolescentes, crimes sexuais e outros. Veja-se, a exemplo: <https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os-avancos-da-inteligencia-artificial/>; <https://agenciagov.ebc.com.br/noticias/202401/incitacao-a-violencia-contra-a-vida-na-internet-lidera-violacoes-de-direitos-humanos-com-mais-de-76-mil-casos-em-cinco-anos-aponta-observadh#:~:text=Os%20crimes%20de%20%C3%B3dio%20na,Crimes%20Cibern%C3%A9ticos%2C%20da%20organiza%C3%A7%C3%A3o%20Safernet.>.

[145] BRASIL. Fórum Brasileiro de Segurança Pública. Disponível em <https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/>. Acesso em: 18 nov. 2024.

principais fontes de informação sobre segurança pública no país, já que é elaborado com base em dados fornecidos pelas secretarias estaduais de segurança pública, pelas polícias civis, militares e federal, além de outras fontes oficiais da área de Segurança Pública. Com isso, pode-se inferir que o anuário oferece dados consistentes e atualizados anualmente, o que permite um panorama claro e detalhado sobre a evolução dos crimes patrimoniais no país.

Além disso, a escolha do período de 2019 a 2024 permite observar as variações antes, durante e após a pandemia de Covid-19, possibilitando compreender dinâmicas e mudanças nesse tipo de criminalidade em um período recente e significativo de transformações sociais e digitais.

Antes de proceder à análise, é importante definir e delimitar alguns pontos, quais sejam: apresentar a definição de crimes patrimoniais e definir, dentre esses, quais serão os crimes analisados no presente estudo.

Os crimes contra o patrimônio encontram-se previstos no Título II do Código Penal brasileiro (Decreto-lei nº 2.848/1940) a partir do artigo 155 (furto) até o artigo 183-A (que trata de uma das disposições gerais aplicadas a esse tipo de criminalidade). Tratam-se de delitos cujo bem jurídico protegido é, justamente, o patrimônio. São diversos os crimes patrimoniais: furto, roubo (incluindo o latrocínio), extorsão, usurpação, dano, apropriação indébita, estelionato, fraude e receptação. No entanto, considerando os dados apresentados no referido Anuário e com o intuito de comparar a diferença entre crimes cometidos em ambientes urbanos (físicos) e crimes virtuais, a análise do presente estudo focará nos crimes de roubo, furto, estelionato e fraude, deixando os demais em segundo plano.

Roubo trata-se da subtração da "*coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência*", e está previsto no artigo 157 do Código Penal. Por sua vez, o furto encontra-se previsto no artigo 155 e se trata da subtração de coisa alheia móvel sem o emprego de violência ou grave ameaça.

Conforme já narrado em linhas pretéritas, desde 2021 existe a previsão no Código Penal para a figura do furto qualificado, quando o furto mediante fraude é "*cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo*", conforme prevê o artigo 155, §4-B, do Código Penal.

O crime de estelionato, conforme definido no artigo 171 do Código Penal, envolve "*obter, para si ou para outra pessoa, vantagem ilícita em detrimento de terceiros, induzindo ou mantendo alguém em erro, por meio de artifício, ardil ou qualquer outra forma de fraude*"

(Art. 171 do Código Penal). Em 2021, foi incluída a tipificação de fraude eletrônica, adicionando o §2º-A ao artigo 171, abrangendo situações em que o estelionato, popularmente conhecido como golpe, ocorre por meio de informações obtidas da vítima ou de terceiros induzidos ao erro por redes sociais, chamadas telefônicas, e-mails fraudulentos, ou outros métodos semelhantes (art. 171, §2º-A do Código Penal).

Destacar o contexto vivido no Brasil e no mundo pela pandemia por Covid-19 também é necessário. Nesse sentido, Liliana Patrícia Peralta Pinto (2021, p. 03) relembra acerca do período pandêmico[146]:

> O novo coronavírus, chamado de Síndrome Respiratória Aguda Grave – Coronavírus - 2 (SARS-CoV-2), foi identificado na China, em dezembro de 2019, associado a grupos de pacientes com pneumonia que foram epidemiologicamente ligados a um mercado de frutos do mar e animais vivos na cidade de Wuhan, Província de Hubei (Zhu et al., 2020). Devido ao seu elevado potencial de contágio resultou num aumento exponencial de casos de infetados. A sua transmissão generalizada foi reconhecida pela Organização Mundial da Saúde como uma Pandemia, a 11 de março de 2020 (WHO, 2020). Como esperado, o alcance geográfico do vírus, o número de infetados e a taxa de mortalidade, causaram na população sentimentos de medo e de insegurança, impuseram medidas de contenção raramente observadas na história da humanidade e, em consequência, diminuíram a mobilidade e a interação direta, aumentaram o afastamento e o isolamento social e afetaram, globalmente, a saúde mental das populações (Ornell et al., 2020).

De modo geral, a pandemia teve um impacto significativo em todos os segmentos da população, gerando transformações nas rotinas e nos estilos de vida de quase todos os cidadãos. O período forçou as pessoas a reduzir o contato social, resultando em um aumento do tempo passado em casa (com medidas governamentais de confinamento, quarentenas, teletrabalho quando viável, restrições à circulação em espaços públicos, entre outras), além de haver intensificação e maior uso da internet, tornando-se parte central da rotina diária[147].

A declaração oficial do fim da pandemia ocorreu em 2023, pela Organização Mundial da Saúde (OMS)[148]. No entanto, desde o final de 2021 e início de 2022, ao menos no Brasil, já havia diminuição do isolamento social e o retorno gradual das atividades presenciais, como trabalho, esporte, lazer e estudos, ante o avanço da vacinação contra a doença.

De toda forma, o período pandêmico proporcionou uma intensificação do uso das tecnologias. De acordo com a pesquisa desenvolvida pela TIC de Domicílios em 2020, o

---

[146] PINTO, Liliana Patrícia Peralta. **Impacto da pandemia de Covid-19 no uso da Internet e nos comportamentos de interação sexual online**. Dissertação (Mestrado em Psicologia) – Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto. Porto/Portugal, 2021, p. 03.

[147] *Idem.*

[148] OMS declara fim da Emergência de Saúde Pública de Importância Internacional referente à COVID-19. **OPAS, 2023**. Disponível em: <https://www.paho.org/pt/noticias/5-5-2023-oms-declara-fim-da-emergencia-saude-publica-importancia-internacional-referente>. Acesso em: 10 nov. 2024.

período pandêmico aumentou significativamente o uso de tecnologias digitais no Brasil, elevando o número de domicílios com acesso à internet de 71% em 2019 para 83% em 2020, representando cerca de 61,8 milhões de residências conectadas à rede àquela época[149].

Desde então, conforme narrado em linhas pretéritas, a crescente utilização da internet pelos brasileiros fez com que o país se tornasse o 5º (quinto) país com mais usuários da rede no mundo em 2021. E, mesmo com o anúncio do fim da pandemia, alguns hábitos adotados naquela época ainda permaneceram, dentre eles o contínuo acesso às plataformas digitais[150], redes sociais ou plataformas bancárias[151], ocasionando uma nova configuração social.

Realizados os referidos destaques, passa-se à análise dos dados ofertados pelo Anuário Brasileiro de Segurança Pública, que, em maioria, apresenta dados analisados até o ano anterior a sua publicação.

O Anuário Brasileiro de Segurança Pública publicado em **2019** (ano anterior à pandemia) apresenta dados estatísticos de até 2018 acerca de diversos crimes cometidos no país. Conforme se analisa, não há menção a nenhum tipo de crimes cibernéticos no documento. Especificamente no caso de delitos contra o patrimônio, as estatísticas são referentes aos crimes de roubo e furto em ambientes urbanos, sobretudo de veículos e de carga. De acordo com o documento, o número de roubos registrados no Brasil em 2018 caiu 14% em relação ao ano anterior e, em relação aos roubos de carga, houve uma queda de 20% se comparado com os dados de 2017[152].

Ressalta-se que, à época, já estavam vigentes no Brasil as leis nº 12.737/12 (Lei Carolina Dieckmann) e nº 13.968/19 (que alterou a redação do crime de induzimento, instigação ou auxílio a suicídio ou a automutilação, previsto no art. 122 do Código Penal, passando a prever aumento de pena nos casos envolvendo ambientes virtuais).

De maneira lúdica, o documento apresenta os principais dados referentes a roubos e furtos em ambientes urbanos da seguinte forma:

---

[149] ESTUDO mostra que pandemia intensificou uso das tecnologias digitais. **Agência Brasil, 2021...**

[150] Em uma matéria divulgada em 2022 pela Fundação Getúlio Vargas (FGV), há o destaque do "boom" das plataformas de delivery no Brasil desde a pandemia. Veja-se: <https://portal.fgv.br/artigos/boom-plataformas-delivery-brasil-e-suas-consequencias-peculiares>.

[151] Veja matéria do G1 sobre "PIX cresce em 2022 e se torna principal instrumento do mercado, com 29% das transações, diz BC", em: <https://g1.globo.com/economia/noticia/2023/05/31/pix-cresce-em-2022-e-representa-29percent-de-todas-as-transacoes-se-tornando-o-principal-instrumento-do-mercado-diz-banco-central.ghtml>.

[152] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2019. São Paulo: Fórum Brasileiro de Segurança Pública, ano 13, 2019. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/62>. Acesso em: 10 nov. 2024.

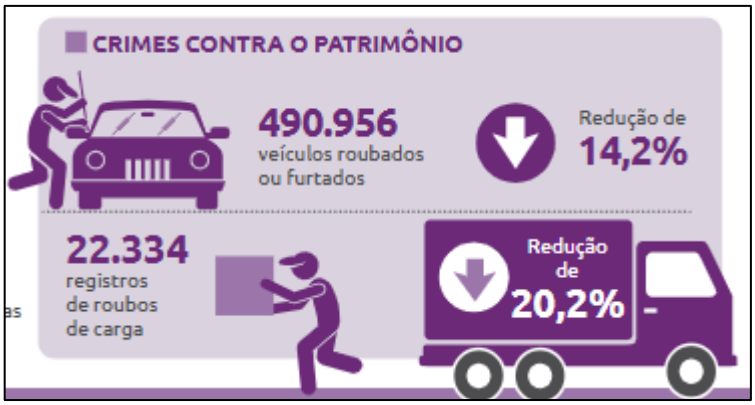

Figura 2 - Anuário Brasileiro de Segurança Pública (2019, p. 07)

No ano seguinte, o Anuário Brasileiro de Segurança Pública de **2020** (ano da pandemia por Covid-19) fez um balanço amplo acerca dos impactos da pandemia no crime e na violência no Brasil. No mesmo sentido do ano anterior, o Anuário de 2020 também não menciona nenhum dado estatístico referente a cibercrimes. Contudo, traz uma análise interessante quanto a crimes de roubo no primeiro semestre de 2020: de acordo com os dados analisados, houve diminuição em 33% de roubos a transeuntes; em 21,5% de roubos de veículos; 25,2% de roubos de carga; 18,9% de roubos a comércios; e de 16,9% de roubos a residências[153]. Essas quedas foram didaticamente demonstradas da seguinte forma:

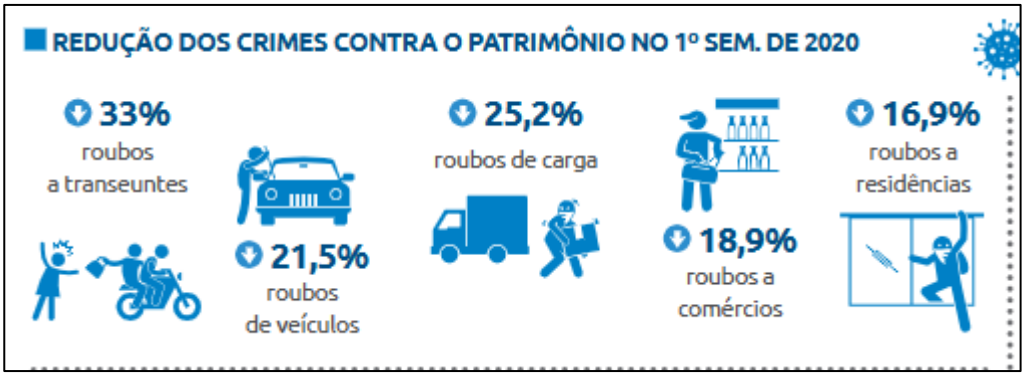

Figura 3 - Anuário Brasileiro de Segurança Pública (2020, p. 12)

Em 2021, ano seguinte após a declaração da pandemia no mundo, o Anuário de Brasileiro de Segurança Pública publicado também não apresentou dados estatísticos relacionados a crimes cibernéticos. No entanto, o documento apresentou dados referentes à

[153] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2020. São Paulo: Fórum Brasileiro de Segurança Pública, ano 14, 2020. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/61>. Acesso em: 10 nov. 2024.

queda de roubos no país, tendo apontado a redução de 26,9% de roubos de veículos; 27,1% de roubos a estabelecimentos comerciais; 16,6% a residências; 36,2% a transeuntes; e 25,4% a roubos de carga[154]. As estatísticas são ilustradas da seguinte forma:

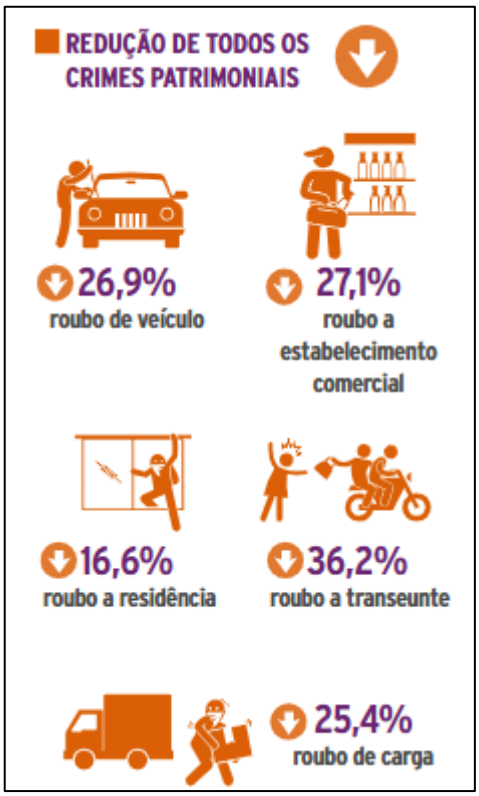

Figura 4 - Anuário Brasileiro de Segurança Pública (2021, p. 14)

Posteriormente, o Anuário Brasileiro de Segurança Pública de **2022** trouxe novas mudanças na análise dos crimes patrimoniais no país, passando a mencionar, de forma inédita, dados estatísticos dos crimes de roubo e furto de celulares e, também, dos crimes de estelionato e estelionato por meio eletrônico.

Em artigo publicado no referido documento, David Marques e Amanda Lagreca, pesquisadores do Fórum Nacional de Segurança Pública mencionam a "*mudança de cenário no que se refere aos efeitos das medidas sanitárias na dinâmica da criminalidade*", considerando os dados apresentados pela pesquisa nacional. De acordo com os pesquisadores[155]:

---

[154] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2021. São Paulo: Fórum Brasileiro de Segurança Pública, ano 15, 2021. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/60>. Acesso em: 10 nov. 2024.

[155] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2022. São Paulo: Fórum Brasileiro de Segurança Pública, ano 16, 2022. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/58>. Acesso em: 10 nov. 2024.

> É possível verificar uma tendência nos registros de crimes patrimoniais no Brasil? Essa questão tem permeado as reflexões sobre os dados nas últimas edições deste Anuário. Na edição de 2019, Guaracy Mingardi analisava a queda no número total de roubos em 2018 questionando "ladrões de férias?". Em 2020, quando da análise dos dados do primeiro semestre daquele ano, já impactado pelas medidas de distanciamento social impostas no contexto da pandemia de Covid-19, verificamos a intensificação da redução nos indicadores de roubo entre 2019 e 2020. Agora, ao analisar os dados de 2021, a identificação de tendência de redução nos crimes patrimoniais, sobretudo nos roubos, torna-se ainda mais difícil, tendo em vista a mudança de cenário no que se refere aos efeitos das medidas sanitárias na dinâmica da criminalidade.

De acordo com os autores, a preocupação pública com crimes patrimoniais cibernéticos cresceu, especialmente com a expansão dos serviços e do comércio digital durante a pandemia, criando um ambiente favorável para novas modalidades criminais. O lançamento do PIX, que facilita transferências bancárias, impulsionou o aumento de fraudes envolvendo roubos e furtos de celulares, onde vítimas são induzidas a fazer transferências ou têm suas contas acessadas após o roubo do dispositivo. Nesse contexto, entre 2018 e 2021, 3,7 milhões de celulares foram roubados ou furtados, com uma redução de 22,8% na taxa desses crimes. Porém, entre 2020 e 2021, a taxa aumentou 1,8%, ainda abaixo dos níveis pré-pandêmicos, refletindo o efeito moderado das restrições de circulação em 2021[156].

Para os pesquisadores, as restrições de mobilidade durante a pandemia de Covid-19 não impediram o aumento dos registros de estelionato e parecem até ter incentivado sua prevalência. Os dados indicam uma transição dos crimes patrimoniais para o ambiente digital. A queda de roubos a transeuntes (-7,5%) e o aumento de roubos e furtos de celulares (1,8%) provavelmente refletem essa mudança, sugerindo que os índices de roubos e furtos de celulares representam melhor os crimes em áreas públicas e a percepção de segurança urbana[157].

O Anuário de 2022 demonstra que entre 2018 e 2021 registraram-se 3,1 milhões de casos de estelionato, com 1,2 milhão em 2021, um aumento significativo de 179,9% em relação a 2018 (e 36,3% entre 2020 e 2021). À época, já estava vigente o crime de estelionato eletrônico, tipificado pela Lei nº 14.155/2021, e já havia sido mensurado em alguns estados, com 60.590 casos de fraude eletrônica registrados em 2021. De acordo com os pesquisadores, a análise confirma que o crescimento dos registros de estelionato está ligado ao ambiente digital e, com a tipificação, poderá ser mais monitorado e orientado por políticas públicas para conter esse problema crescente no Brasil[158].

---

[156] *Ibidem*, p. 118.
[157] *Ibidem*, p. 119.
[158] *Idem*.

De acordo com David Marques e Amanda Lagreca (2022, p. 121)[159]:

> Os dados acima demonstram que, muito embora tenhamos verificado queda nos crimes patrimoniais no período entre 2019 e 2020, com o início da pandemia de Covid-19, essa tendência não se manteve no período mais recente. O ano de 2021 foi marcado pela retomada das atividades, principalmente a partir do avanço da vacinação, e o que as estatísticas nos indicam é que também houve retomada de parte considerável das ocorrências de crimes contra o patrimônio – como falado anteriormente, tivemos leve crescimento de roubo a estabelecimentos comerciais, a residências, roubo a instituições financeiras (com destaque para os casos de maior repercussão, como no "novo cangaço") e roubo de carga. As taxas, contudo, ainda não se igualam aos patamares anteriores à pandemia de Covid-19. Os crescimentos mais significativos ocorreram no crime de estelionato, com taxas muito acima daquelas vistas em 2018 e 2019, e de estelionato no contexto virtual. Entre 2020 e 2021, houve, praticamente, estabilidade no roubo e furto de veículos e roubo e furto de celulares. Tivemos, ademais, queda de roubo a transeunte e queda no total de roubos.

Todos esses dados foram apresentados da seguinte forma:

Figura 5 - Anuário Brasileiro de Segurança Pública (2022, p. 15)

Já em **2023**, o levantamento divulgado pelo Anuário Brasileiro de Segurança Pública destaca que, a partir da pandemia, houve reconfiguração de alguns crimes, sobretudo os crimes patrimoniais, passando a existir uma migração dos crimes de roubo e furto para estelionatos e

[159] *Ibidem*, p. 121.

fraudes praticadas por meio eletrônico. Em artigo publicado no Anuário, os pesquisadores Renato Sérgio de Lima e Samira Bueno (2023, p. 90) destacam que[160]:

> [H]á movimentos preocupantes e tendências que começam a ganhar corpo e merecem maior atenção dos profissionais da segurança pública, dos tomadores de decisão política e de pesquisadores. **E esse é o caso dos crimes patrimoniais, cujos movimentos sinalizam para uma forte reconfiguração de como tais crimes são cometidos, sobretudo a partir da pandemia de Covid-19, incluindo a migração dos roubos para modalidades como furtos, estelionatos e golpes virtuais**.
> (...)
> No Brasil (...), com queda generalizada dos indicadores de crimes patrimoniais nos anos de 2020 e 2021. A partir de 2022, no entanto, algumas modalidades criminais retomam tendências pré-pandemia, com crescimento dos roubos e furtos de celular e de veículos que serão descritos na sequência. **Outros, no entanto, seguem em queda, como é o caso de roubos a instituições financeiras (-21,9%), de carga (-4,4%), a estabelecimentos comerciais (-15,6%) e a residências (-13,3%).** (marco meu)

Os dados disponíveis no Anuário destacam que, em 2022, o número de estelionatos no Brasil atingiu 1.819.409 ocorrências, com uma média de 207,7 casos por hora, registrando um aumento de 37,9% em relação ao ano anterior. Entre esses, 200.322 foram fraudes eletrônicas – aumento de 65,2% comparado a 2021, o ano da tipificação desse crime. Diferente de roubos e furtos, que caíram durante a pandemia, fraudes por redes sociais e aplicativos cresceram significativamente, refletindo uma tendência global[161].

De acordo com Renato Sérgio de Lima e Samira Bueno (2023, p. 92) destacam que:

> O que antes era obtido primordialmente na interação violenta entre as pessoas parece **se deslocar, de modo até mais rentável**, para o campo das fraudes e das ocorrências que exploram o fenômeno da migração da vida social para o ambiente híbrido que conecta o físico e virtual. A porta de entrada para as atividades criminais continua sendo física, pois essas últimas dependem, preponderantemente, do acesso a aparelhos celulares ou dispositivos móveis que cada vez mais fazem parte da vida dos indivíduos. Só que, **cada vez mais, as atividades criminosas passam a ocorrer na arena virtual**. O tipo criminal típico deixa de ser o roubo e passa a ser o **estelionato e/ou o golpe virtual**, em muito dependente de redes de receptação dos equipamentos furtados/roubados. (marco meu)

A referida análise foi ilustrada da seguinte forma:

---

[160] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2023. São Paulo: Fórum Brasileiro de Segurança Pública, ano 17, 2023. ISSN 1983-7364. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/fbsp/57>. Acesso em: 10 nov. 2024.
[161] *Idem*.

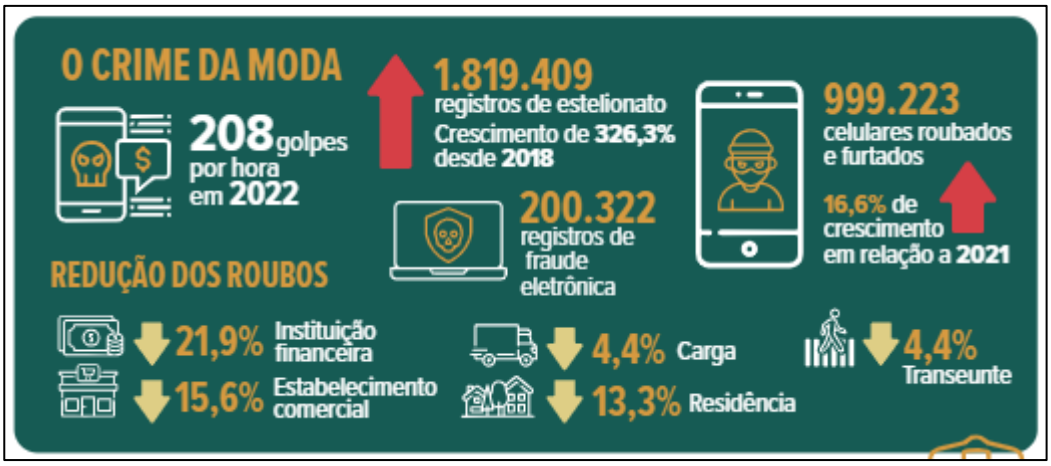

Figura 6 - Anuário Brasileiro de Segurança Pública (2023, p. 15)

Por fim, em **2024**, o Anuário Brasileiro de Segurança Pública (o último publicado até a finalização desta pesquisa) trouxe relevantes dados referentes aos crimes de estelionato, fraude e roubo e furto de celulares. Especificamente quanto a esse último, a pesquisa realiza uma extensa análise quanto a quantidade de roubos e furtos dos aparelhos, relacionando a marca dos telefones, horário da ocorrência do crime e outros fatores.

Em artigo disponível no Anuário, os pesquisadores Samira Bueno, Renato Sérgio de Lima e Isabela Sobral (2024, p. 83) destacam que em 2023 os registros de roubo e furto de celulares caíram 4,7% em relação a 2022, mas ainda somam quase 1 milhão de ocorrências, mostrando como esses aparelhos têm grande impacto na sensação de insegurança da população. Os celulares se destacam na dinâmica dos crimes patrimoniais não apenas pelo volume de ocorrências, mas por serem porta de entrada para outros crimes, como estelionatos e fraudes digitais, que fortalecem o crime organizado. Esse padrão reflete uma tendência mundial, associada à popularização dos smartphones. Segundo a Fundação Getúlio Vargas (FGV), em maio de 2024, o Brasil possuía 258 milhões de smartphones, com média de 1,2 aparelhos por habitante[162].

Em outro artigo publicado na mesma edição, Rafael Alcadipani, Renato Sérgio de Lima e Samira Bueno (2024, p. 96) demonstram o crescimento dos crimes cibernéticos no Brasil, aliado à redução dos crimes de rua, reflete uma transformação nas dinâmicas criminais do país. De acordo com os pesquisadores[163]:

---

[162] ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2024. São Paulo: Fórum Brasileiro de Segurança Pública, ano 18, 2024. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/123456789/253>. Acesso em: 10 nov. 2024.
[163] *Idem*.

> A análise dos dados sobre crimes patrimoniais publicados nesta edição do Anuário Brasileiro de Segurança Pública confirma e reforça o que Lima e Bueno (2023)1 constataram na edição anterior da publicação, quando esses autores sinalizavam para uma forte reconfiguração do modus operandi de tais delitos iniciada a partir do isolamento social imposto pela Pandemia de Covid-19, em 2020. Essa tendência é marcada pelo movimento de substituição dos roubos por modalidades como estelionatos, golpes virtuais e furtos e que, em 2023, não só se manteve como ganhou tração no país. O gráfico (...) mostra que os estelionatos (gerais e virtuais) e os furtos de celulares crescem, enquanto caem todas as modalidades de roubos monitoradas ao longo dos anos pelo Anuário. Entre 2022 e 2023, os estelionatos por meio virtual subiram 13,6%; o total de estelionatos cresceu 8,2%; e, ainda, os furtos de celulares oscilou 0,7% para cima. Na ponta oposta, chama atenção a forte queda no registro de roubos a bancos e demais instituições financeiras, de quase 30% no mesmo período, seguidos dos roubos a estabelecimentos comerciais (-18,8%).

O aumento dos crimes cibernéticos e a redução dos crimes de rua no Brasil foram ilustrados da seguinte forma:

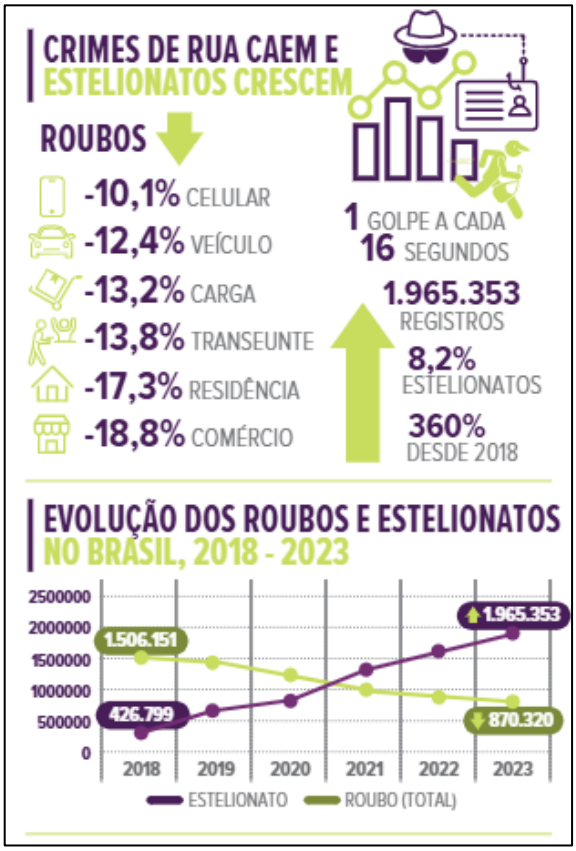

Figura 7 - Anuário Brasileiro de Segurança Pública (2024, p. 15)

Uma análise detalhada dos dados divulgados pelos Anuários Brasileiros de Segurança Pública dos anos de 2022 e 2024 possibilitou uma investigação mais aprofundada acerca da evolução dos crimes de estelionato e estelionato praticado por meios eletrônicos no Brasil e em suas respectivas unidades da federação, considerando os dados disponibilizados pelas Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Polícia Civil do Distrito

Federal; Polícia Civil de Minas Gerais; Instituto de Segurança Pública/RJ (ISP); Polícia Civil do Estado do Acre; Polícia Civil do Estado de Roraima; Instituto Brasileiro de Geografia e Estatística (IBGE) – Censo Demográfico 2022; Fórum Brasileiro de Segurança Pública.

O levantamento comparativo, realizado com base nos registros oficiais compartilhados no documento, abrange o período de 2018 a 2023, permitindo uma avaliação quantitativa que evidencia o crescimento progressivo dos delitos relacionados à fraude digital. Esses dados revelam tendências importantes no cenário da criminalidade moderna, destacando a necessidade de políticas públicas voltadas à prevenção e combate a crimes cibernéticos, que se mostram cada vez mais presentes na realidade brasileira.

Com base nos dados apresentados na Tabela 15 dos Anuários Brasileiros de Segurança Pública de 2022 (p. 110-111) e 2024 (p. 77), foram elaboradas duas tabelas comparativas. A primeira tabela evidencia, em números absolutos, os registros de crimes de estelionato no Brasil e nas respectivas unidades da federação, organizados em ordem decrescente conforme o volume de ocorrências. A segunda tabela apresenta os registros de delitos de estelionato praticado por meios eletrônicos nas mesmas localidades e sob os mesmos critérios, permitindo uma análise comparativa consistente entre os diferentes tipos de crime. Destaca-se que as legendas das tabelas acompanham àquelas mencionadas nos Anuários mencionados.

Veja-se, em números absolutos, o resultado comparativo:

Tabela 1 - Estelionato em números absolutos [1]

Federação	2018	2019	2020	2021	2022 [7]	2023	Total
Brasil	**426.799**	**523.820**	**927.898**	**1.265.073**	**1.816.438**	**1.965.353**	**6.925.381**
SP [6]	122.603	153.234	289.570	382.110	611.572	750.430	**2.309.519**
MG	42.669	57.032	92.061	112.899	132.120	141.649	**578.430**
PR	29.845	40.681	69.548	113.420	141.777	145.205	**540.476**
RJ	34.493	41.253	48.552	70.075	123.841	120.218	**438.432**
RS [8]	23.858	28.942	65.771	90.007	95.182	87.627	**391.387**
SC	17.359	21.973	42.221	64.375	95.706	94.944	**336.578**
CE	23.877	26.227	51.424	57.089	68.754	68.235	**295.606**
BA	16.589	18.801	28.649	31.784	91.223	98.934	**285.980**
GO	18.173	21.847	35.290	55.603	74.163	74.906	**279.982**
PE	18.724	21.602	45.038	51.185	59.499	58.460	**254.508**
DF	13.911	15.815	25.078	40.533	52.995	50.387	**198.719**
PA [5]	7.509	9.377	20.533	31.875	35.038	36.845	**141.177**
ES [4]	7.272	9.213	18.464	29.515	37.391	35.168	**137.023**
MT	7.421	8.934	13.862	15.768	20.261	20.565	**86.811**
AL	4.977	4.825	11.808	15.460	20.087	21.058	**78.215**
SE	5.492	7.272	9.344	15.132	19.734	17.763	**74.737**
RN	1.646	2.715	3.440	8.774	25.945	26.018	**68.538**
PI	5.996	7.025	9.437	12.927	15.310	16.663	**67.358**
RO [4]	4.754	6.491	9.596	10.487	15.376	18.393	**65.097**
MS	4.221	5.069	6.996	11.266	13.647	13.357	**54.556**
MA	...	...	10.728	13.148	14.799	14.782	**53.457**
AM	3.812	3.522	5.699	6.369	15.430	17.464	**52.296**
TO	5.693	4.101	4.083	8.432	11.287	11.796	**45.392**
AP [2] [3]	1.254	2.341	2.993	5.577	8.587	7.146	**27.898**
PB	2.792	2.949	2.885	3.929	5.669	6.443	**24.667**
AC	1.079	1.469	2.526	3.812	5.649	5.538	**20.073**
RR	780	1.110	2.302	3.522	5.396	5.359	**18.469**

Fonte: Anuário Brasileiro de Segurança Pública, 2022, p. 110-111; Anuário Brasileiro de Segurança Pública, 2024, p. 77.

Tabela 2 - Estelionato eletrônico em números absolutos [1]

Federação	2018	2019	2020	2021	2022 [7]	2023	Total
Brasil	7.591	14.677	34.713	60.590	207.125	235.393	**560.089**
SC	...	...	2.429	7.174	64.646	64.482	**138.731**
MG	4.343	8.547	18.892	28.581	35.878	40.906	**137.147**
DF	1.799	3.084	7.524	9.813	15.749	16.060	**54.029**
PA [5]	561	1.305	1.838	2.764	13.099	16.884	**36.451**
ES [4]	...	...	...	...	15.277	14.578	**29.855**
PE	...	...	...	...	14.164	13.941	**28.105**
MT	345	547	1.839	2.232	9.253	11.257	**25.473**
AL	205	452	1.003	3.248	4.973	5.729	**15.610**
PR	-	3	21	1.850	5.738	7.029	**14.641**
MA	...	...	...	1.114	5.781	6.278	**13.173**
RO [4]	...	...	...	...	5.932	6.532	**12.464**
BA	...	...	...	...	4.183	7.515	**11.698**
MS	...	...	...	876	5.027	5.414	**11.317**
TO	269	616	673	1.644	3.078	4.043	**10.323**
RS [8]	...	...	...	...	...	6.577	**6.577**
RR	40	95	470	840	778	1.893	**4.116**
GO	4	11	12	112	1.488	2.167	**3.794**
PB	-	-	-	70	406	1.030	**1.506**
SE	20	14	8	73	446	751	**1.312**
AM	...	...	...	...	419	877	**1.296**
AP [2] [3]	...	...	3	59	380	618	**1.060**
PI	-	-	-	48	276	584	**908**
AC	5	3	1	53	154	248	**464**
RN	...	...	...	39	...	...	**39**
CE	...	...	...	...	...	...	**0**
RJ	...	...	...	...	...	...	**0**
SP [6]	...	...	...	...	...	...	**0**

Fonte: Anuário Brasileiro de Segurança Pública, 2022, p. 110-111; Anuário Brasileiro de Segurança Pública, 2024, p. 77.

Legenda:
(...) Informação não disponível.
(-) Fenômeno inexistente.
(1) Em 2021, o crime de Estelionato - Fraude eletrônica passou a ser tipificado pelos parágrafos 2ºA, 2ºB e 3º do art. 171 do Código Penal.
(2) Para os anos de 2018 e 2019, os números referem-se apenas à capital do Estado.
(3) No que concerne à tipificação Estelionato - fraude eletrônica, os dados são referentes ao parágrafo 2ºA do art. 171 do Código Penal.
(4) Nos campos de parâmetro utilizado pelos Estados, não é possível distinguir se o crime se refere ao estelionato ou ao estelionato - fraude eletrônica, pois ambos são computados conjuntamente.
(5) A UF informou que os dados de Estelionato e Estelionato - fraude eletrônica incluem os oriundos da delegacia virtual, registrados diretamente pelos cidadãos, e que não passam por supervisão ou tratamento, podendo haver sobrenotificação por duplicidade ou erro de tipificação.
(6) Para a tipificação de Estelionato, o Estado registra os casos tentados ou consumados.
(7) Atualização das informações publicadas no Anuário Brasileiro de Segurança Pública, ano 17, 2023.
(8) A tipificação de Estelionato por meio eletrônico passou a ser registrada pelo Estado do Rio Grande do Sul em 27/07/2023. Os dados da tabela, portanto, correspondem aos registros de 27/07/23 a 31/12/23.

Conforme se verifica, os dados apresentados nos Anuários de Segurança Pública revelam um crescimento expressivo nos registros de estelionato e estelionato eletrônico no Brasil entre os anos de 2018 e 2023. O crime de estelionato acumulou um total de 6.925.381 ocorrências no período, com destaque para os estados de São Paulo, Minas Gerais e Paraná, que juntos representam uma parcela significativa dos casos. Em termos absolutos, o estado de São Paulo se destaca como líder, com mais de 2,3 milhões de registros, evidenciando uma tendência contínua de crescimento nos crimes relacionados à fraude.

Quando analisado o estelionato eletrônico, os números mostram um aumento ainda mais acentuado, passando de 7.591 registros em 2018 para 235.393 em 2023, totalizando 560.089 ocorrências no período. Observa-se, contudo, que nem todos os estados, como São Paulo e Rio de Janeiro, disponibilizaram informações completas e consistentes para a análise, o que compromete a precisão do levantamento e a comparação entre as unidades da federação.

Nesse contexto, considerando apenas os dados existentes, Santa Catarina e Minas Gerais aparecem como os estados com os maiores volumes de registros desse tipo de crime, demonstrando o impacto significativo da digitalização nas práticas delituosas. O salto nos números após 2020 pode ser atribuído à pandemia por Covid-19, que, como mencionado anteriormente, intensificou o uso de meios digitais para transações comerciais e interações sociais.

A partir dos referidos dados, foram criados dois gráficos por meio dos quais foi possível notar o crescimento acelerado dos registros de estelionato e estelionato eletrônico ao longo dos anos, destacando o impacto das mudanças tecnológicas no perfil das práticas criminosas, sendo possível, ainda, fazer uma projeção (por meio de uma linha de tendência, considerando os valores absolutos existentes) de um possível cenário desses delitos nos próximos três anos, quais sejam, 2024, 2025 e 2026. Veja-se:

Figura 8 - Estelionato em números absolutos

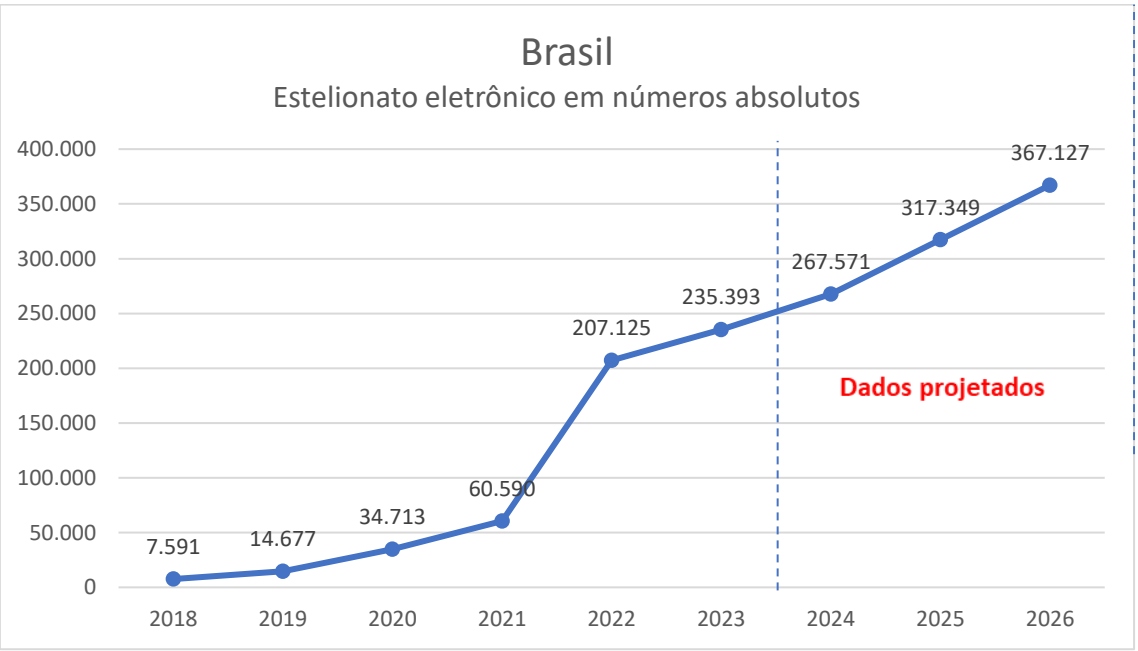

Figura 9 - Estelionato eletrônico em números absolutos

Os gráficos evidenciam não apenas o aumento expressivo no número de ocorrências, mas também a diferença na distribuição desses crimes entre os estados brasileiros, apontando disparidades regionais que precisam ser consideradas na formulação de políticas públicas. Além disso, é possível visualizar a transição das modalidades tradicionais de estelionato para o

ambiente digital, especialmente após 2020, quando o uso de tecnologias digitais se intensificou devido à pandemia. Essa transição indica que as fraudes eletrônicas têm se tornado cada vez mais sofisticadas, exigindo novas abordagens investigativas e preventivas por parte das autoridades de segurança pública.

Outro ponto relevante observado nos gráficos é o impacto da falta de dados completos em alguns estados, o que dificulta uma análise comparativa mais precisa. O gráfico que apresenta os registros de estelionato eletrônico evidencia uma diferença significativa entre os anos de 2021 e 2022, que pode ser explicada, em parte, pela ausência de dados completos de alguns estados. Essa lacuna de informações impacta diretamente a análise da evolução dos casos, dificultando a compreensão real do crescimento do crime no período.

A falta de dados, principalmente em estados que passaram a registrar o estelionato eletrônico apenas em anos mais recentes, cria uma descontinuidade na série histórica, prejudicando a consistência da comparação entre os anos. Essa situação reforça a importância de padronizar os mecanismos de coleta e registro de informações em todas as unidades da federação, garantindo que os dados sejam completos, uniformes e atualizados.

De todo modo, a partir dos dados analisados observa-se uma mudança radical no cenário dos delitos patrimoniais no país. O aumento substancial no número de usuários das redes sociais e da internet durante o período analisado (2019 a 2024) foi primordialmente impulsionado pela pandemia da Covid-19. Ao limitar a mobilidade das pessoas, que se viram obrigadas a ajustar suas rotinas para aderir às medidas de distanciamento social e às restrições de deslocamento, a pandemia catalisou o uso dessas tecnologias como meios de comunicação privada e com empresas, consumo, entretenimento, transações bancárias e trabalho remoto.

A análise comparativa entre as duas modalidades de estelionato aponta para uma mudança no perfil da criminalidade. Enquanto o estelionato tradicional mantém um crescimento constante, o estelionato eletrônico apresenta uma expansão exponencial, evidenciando a vulnerabilidade dos meios digitais e a necessidade de medidas mais robustas de segurança cibernética. Essa tendência reforça a importância de políticas públicas que visem a prevenção de crimes cibernéticos e a capacitação das autoridades para lidar com essa nova realidade.

Como se vê, as atividades criminosas que antes eram realizadas de maneira convencional estão sendo progressivamente substituídas por ações ilícitas executadas por meio de plataformas digitais, explorando as brechas nas medidas de segurança, a vigilância limitada e a crescente dependência da sociedade em relação à tecnologia e à internet.

Evidentemente, essa nova configuração social trouxe nova preocupação aos órgãos de segurança pública brasileiros – razão pela qual o Fórum Nacional de Segurança Pública passou a incluir dados estatísticos quanto a esse tipo de criminalidade em seu Anuário, já que, como se observa, até 2021 não havia sequer menção a esses delitos.

A partir dos referidos dados, torna-se possível analisar o cenário brasileiro por meio da Teoria das Atividades Rotineiras e, ainda, entender melhor as formas que a referida teoria contribui para a compreensão das dinâmicas de criminalidade na era digital. Dessa forma, será possível perceber como as mudanças nos comportamentos cotidianos da sociedade, especialmente impulsionadas pelo aumento da conectividade e pela digitalização de serviços pós-pandemia, influenciam a exposição aos cibercrimes.

4. AS CONTRIBUIÇÕES DA TEORIA DAS ATIVIDADES ROTINEIRAS NA ANÁLISE DOS CRIMES CIBERNÉTICOS PATRIMONIAIS

O panorama dos crimes cibernéticos no Brasil permite compreender, em números absolutos, mesmo que parcialmente (dada a ausência de dados de alguns estados), um novo cenário de crimes no país: aquele que dispensa a presencialidade para acontecer, podendo se dar por meio de um mero dispositivo digital que possui conexão com a internet.

Diante desse novo cenário, a Teoria das Atividades Rotineiras oferece uma base teórica para compreender como os crimes patrimoniais se manifestam no ambiente digital. Conforme discutido anteriormente (ver Capítulo 2), embora originalmente formulada para explicar crimes patrimoniais em contextos físicos, no ambiente cibernético a teoria se adapta ao identificar três elementos essenciais: *(i)* indivíduos motivados a realizar atos ilícitos online, *(ii)* alvos vulneráveis e disponíveis para ataque e *(iii)* a ausência de guardiões eficazes para proteger esses alvos.

Proponha-se, nesse sentido, que a figura triangular da teoria pode, portanto, ser entendida da seguinte forma:

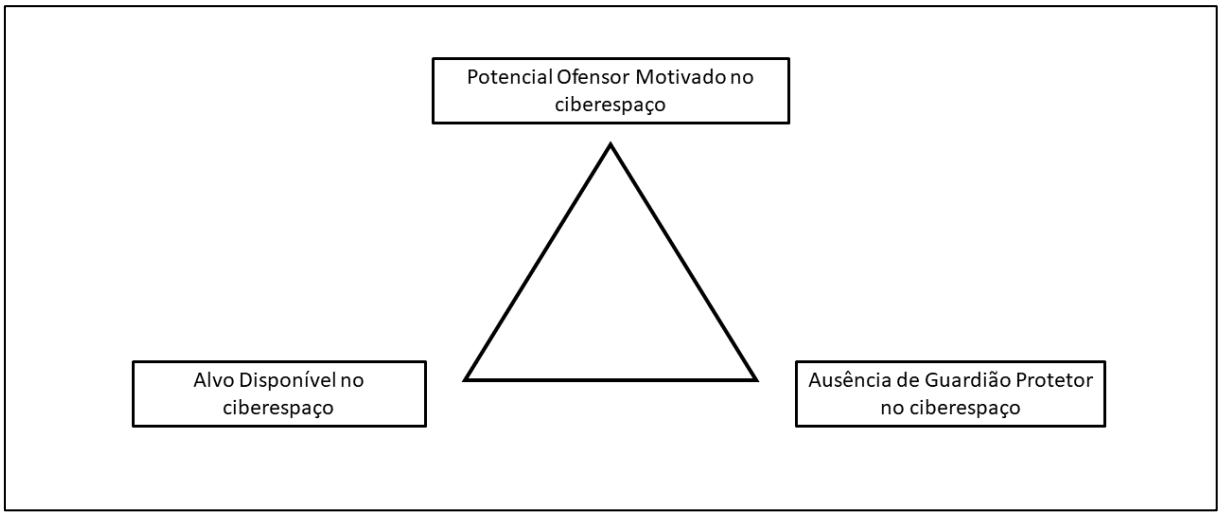

Figura 10 - Teoria das Atividades Rotineiras no cibercrime

Conforme observado no capítulo anterior, os dados ofertados pelos Anuários Brasileiros de Segurança Pública não revelam (ainda) o possível perfil das vítimas dos crimes cibernéticos registrados no país, nem fornecem informações detalhadas sobre os métodos mais utilizados para a prática desses crimes. Essa ausência de dados impede uma análise mais aprofundada sobre as características dos agentes criminosos, os comportamentos das vítimas e as circunstâncias que favorecem a ocorrência desses delitos. Além disso, dificulta a identificação

de padrões que poderiam orientar o desenvolvimento de políticas públicas mais eficazes e a implementação de estratégias específicas de prevenção e combate.

No entanto, alguns fatores evidentes no contexto brasileiro, como o analfabetismo digital, o aumento da conectividade e a digitalização crescente das atividades diárias, contribuem para a análise da expansão e sofisticação dos crimes cibernéticos no país. Conforme observado nos dados apresentados anteriormente, o perfil dos usuários das redes no Brasil é marcado pela diversidade socioeconômica, com uma parcela significativa da população acessando cada vez mais a internet nos últimos anos. Esse processo, embora positivo em termos de inclusão digital, expõe muitos usuários sem habilidades suficientes para identificar ameaças ou adotar medidas básicas de proteção, tornando-os alvos fáceis para golpes online.

Afinal, como visto, os dados apresentados revelam que apenas 24% da população brasileira possui habilidades digitais básicas, enquanto cerca de 76% são considerados analfabetos digitais, incapazes de utilizar adequadamente ferramentas essenciais no ambiente digital. Esse cenário de baixo preparo digital contribui para a maior exposição a golpes online, já que muitos usuários não têm capacidade crítica para reconhecer ameaças ou adotar medidas preventivas.

O aumento da conectividade, impulsionado pela popularização de dispositivos móveis e pela expansão da infraestrutura de internet, agrava esse quadro. Essa ampliação, apesar de democratizar o acesso à tecnologia, também amplia as oportunidades para criminosos explorarem vulnerabilidades. A digitalização de atividades cotidianas, como transações bancárias, compras online e interações sociais, também cria novas superfícies de ataque. A conexão entre crimes patrimoniais tradicionais e crimes digitais é evidente: dispositivos como celulares roubados ou furtados frequentemente se tornam a porta de entrada para fraudes cibernéticas, dada a quantidade de dados pessoais e financeiros armazenados neles.

A Teoria das Atividades Rotineiras reforça essa análise ao destacar que o aumento das atividades digitais expõe vítimas vulneráveis (usuários desatentos ou com pouco conhecimento crítico) a criminosos motivados, enquanto a ausência de guardiões adequados (como práticas seguras ou tecnologias robustas de proteção) facilita a ocorrência dos delitos. Nesse contexto, as rotinas digitais, antes vistas como ferramentas de conveniência, tornam-se também elementos-chave na dinâmica de risco e oportunidade para o crime, evidenciando a necessidade de políticas públicas que combinem educação digital, regulamentação tecnológica e fortalecimento das capacidades investigativas no ambiente virtual.

No mesmo sentido, a teoria reforça a importância de uma análise aprofundada sobre como as mudanças nas rotinas diárias dos indivíduos alteram as condições de segurança. A alteração nas atividades rotineiras dos indivíduos, especialmente com o crescente uso do ambiente on-line, impacta diretamente nas taxas de vitimização de maneira complexa. O conceito de “guardião natural”, que se refere a fatores físicos ou sociais que ajudam a proteger os indivíduos de crimes (como vizinhos, segurança de bairro, presença de câmeras, entre outros), tem grande relevância nesse contexto.

No ambiente tradicional, as estratégias de proteção, como evitar ter sistemas de segurança física em casa (alarmes, cercas) ou até manter a bolsa junto ao corpo, são eficazes porque o delito é visível ou detectável. Ou seja, os indivíduos podem se proteger ao observar sua localização, seu entorno e outras pessoas ao seu redor. Além disso, a presença de “guardas naturais”, como vizinhos atentos ou câmeras de vigilância oferece uma camada de segurança adicional.

Contudo, quando a rotina se desloca para o mundo digital, essas estratégias tradicionais de proteção tornam-se ineficazes. Isso ocorre porque a exposição ao risco no ambiente online é menos visível, mais difusa e frequentemente não detectável de forma imediata. Um exemplo claro disso é o furto de dados ou fraude financeira que ocorre sem que a vítima perceba o ataque em tempo real. Ao navegar na internet, a pessoa pode, sem saber, expor suas informações pessoais, realizar transações inseguras ou interagir com golpistas, sem perceber os sinais de alerta.

Esse novo contexto de vitimização digital também envolve a ausência de guardiães naturais, uma vez que os usuários estão, muitas vezes, sozinhos em sua interação com a tecnologia, sem a vigilância direta de outras pessoas que poderiam identificar comportamentos suspeitos. A ausência de uma presença física de proteção aumenta a vulnerabilidade, uma vez que crimes cibernéticos acontecem de maneira invisível, sem a percepção imediata da vítima.

Além disso, a anonimização e a descentralização proporcionadas pela internet dificultam a identificação dos supostos criminosos, o que torna a ação de prevenção ainda mais desafiadora. Uma pessoa pode se tornar alvo de crimes virtuais sem perceber a ameaça, uma vez que, muitas vezes, as medidas preventivas (como antivírus, senhas fortes, autenticação em dois fatores) são negligenciadas ou mal aplicadas, contribuindo para uma falsa sensação de segurança.

Em resumo, a transição para o ambiente on-line implica em uma redefinição da vitimização e das estratégias de proteção. A ausência dos guardiães naturais e a invisibilidade dos riscos no ambiente virtual criam um cenário em que as medidas tradicionais de segurança se tornam obsoletas. Nesse contexto, novas formas de proteção precisam ser desenvolvidas, incluindo a conscientização e alfabetização digital, a educação sobre segurança cibernética e o fortalecimento de sistemas de segurança online, para lidar com a nova realidade da vitimização na era digital.

Reforça-se, novamente, que a proteção dos usuários também é uma responsabilidade do Estado. Seja por meio de iniciativas educacionais, seja pela implementação de medidas de segurança que incentivem a conscientização e a prevenção de riscos no ambiente digital, é fundamental que o Estado atue para garantir a proteção de dados, a segurança cibernética e a prevenção de fraudes digitais.

CONSIDERAÇÕES FINAIS

O presente trabalho buscou estudar o fenômeno dos crimes contra o patrimônio praticados no âmbito virtual e teve como objetivo compreender as mudanças nos padrões de crimes patrimoniais no Brasil por meio da Teoria das Atividades Rotineiras (TAR), de Cohen e Felson (1979).

Conforme revelado neste estudo, a utilização das TICs e da internet no país tem sido cada vez mais constante, o que, por sua vez, impacta na incidência de maiores números de crimes cometidos no âmbito virtual, sobretudo os crimes patrimoniais, tais como fraudes eletrônicas e estelionatos. O Brasil, assim como outros países no mundo, vivenciou mudanças consideráveis no acesso às tecnologias durante a pandemia por Covid-19, tendo em vista o distanciamento social e o crescimento do trabalho remoto e do ensino online. Diante desse contexto, houve, por consequência, um aumento expressivo nas atividades online, intensificando a exposição dos usuários a potenciais riscos de segurança cibernética e ampliando as oportunidades para cibercriminosos explorarem vulnerabilidades.

As práticas criminosas que anteriormente eram cometidas de forma tradicional têm sido substituídas por atividades ilícitas realizadas por meio de meios eletrônicos, aproveitando-se das oportunidades (aumento imensurável de bens e pessoas que podem ser subtraídos e das vulnerabilidades dos diferentes perfis de usuários), da vigilância incipiente (baixo risco de identificação e, por vezes, de responsabilização penal) e da dependência da sociedade em relação à tecnologia e à internet, que passaram a rotineiramente executar suas atividades por esses meios.

Aplicando-se a Teoria das Atividades Rotineiras aos cibercrimes, observa-se que os três elementos essenciais para explicar a ocorrência desses delitos seriam, em suma: *(i)* um alvo online vulnerável, caracterizado como comportamentos de uso da internet de uma pessoa ou objeto que se torna uma vítima potencial para a criminalidade; *(ii)* exposição a um criminoso motivado no ambiente digital, definida como ações que colocam indivíduos em risco de ataque por cibercriminosos enquanto estão conectados à rede; e, por fim, o *(iii)* guardião eficaz, que abrange tanto indivíduos, estratégias pessoais quanto ferramentas tecnológicas capazes de prevenir ou mitigar a ocorrência de crimes virtuais.

De fato, é possível concluir que, em consonância com o que propõe a Teoria das Atividades Rotineiras, a crescente utilização dos meios digitais, desacompanhada de medidas efetivas de proteção e conscientização sobre segurança cibernética, contribui para a vulnerabilidade dos usuários e a facilidade de acesso por parte de potenciais criminosos.

Assumindo as premissas e o modelo causal da Teoria das Atividades Rotineiras, pode-se afirmar que a expansão acelerada numa escala global do uso das TIC´s leva a mudanças nos padrões dos crimes contra o patrimônio. À toda evidência, há um aumento sem precedentes dos crimes contra o patrimônio na era digital.

No caso brasileiro, que atualmente é o terceiro maior consumidor de redes sociais no mundo, observa-se que há um alto índice de indivíduos sem habilidades digitais básicas, o que aumenta a vulnerabilidade dessas pessoas, uma vez que elas carecem de conhecimento e familiaridade para utilizar ferramentas digitais comuns e seus respectivos aplicativos. Sob o viés da Teoria, pode-se entender que essa realidade torna alvos vulneráveis para os cibercriminosos.

Entender toda essa realidade por meio da Teoria das Atividades Rotineiras permite (re)pensar a formulação de políticas públicas voltadas a esse tipo de criminalidade no país. Os consideráveis números referentes aos casos de estelionatos e fraudes cometidas no ciberespaço e os dados referentes ao perfil dos usuários das redes sociais e internet no país devem ser levados em conta para desenvolver estratégias eficazes de segurança cibernética, incluindo a mitigação da desigualdade digital e a prevenção e proteção dos cidadãos por meio da educação digital.

REFERÊNCIAS BIBLIOGRÁFICAS

161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022. **Agência IBGE Notícias, 2023**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022#:~:text=O%20equipamento%20mais%20utilizado%20para,35%2C5%25%20de%202022>. Acesso em: 04 jun. 2024.

ANALFABETISMO digital segura avanço do acesso à internet no Brasil. **Exame, 2019**. Disponível em: <https://exame.com/tecnologia/alfabetizacao-digital-segura-avanco-do-acesso-a-internet-no-brasil/>. Acesso em: 25 jun. 2024.

ANALFABETISMO digital: 76% dos brasileiros não têm habilidades digitais básicas. **Diário do Grande ABC, 2023**. Disponível em: <https://www.dgabc.com.br/Noticia/4063023/analfabetismo-digital-76-dos-brasileiros-nao-tem-habilidades-digitais-basicas>. Acesso em: 17 jun. 2024.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2019. São Paulo: Fórum Brasileiro de Segurança Pública, ano 13, 2019. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/62>. Acesso em: 10 nov. 2024.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2020. São Paulo: Fórum Brasileiro de Segurança Pública, ano 14, 2020. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/61>. Acesso em: 10 nov. 2024.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2021. São Paulo: Fórum Brasileiro de Segurança Pública, ano 15, 2021. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/60>. Acesso em: 10 nov. 2024.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2022. São Paulo: Fórum Brasileiro de Segurança Pública, ano 16, 2022. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/fbsp/58>. Acesso em: 10 nov. 2024.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2023. São Paulo: Fórum Brasileiro de Segurança Pública, ano 17, 2023. ISSN 1983-7364. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/fbsp/57>. Acesso em: 10 nov. 2024.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2024. São Paulo: Fórum Brasileiro de Segurança Pública, ano 18, 2024. ISSN 1983-7364. Disponível em: < https://publicacoes.forumseguranca.org.br/handle/123456789/253>. Acesso em: 10 nov. 2024.

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal**: introdução à sociologia do direito penal. Tradução Juarez Cirino dos Santos – 3ª ed. – Rio de Janeiro: Editora Revan: Instituto Carioca de Criminologia, 2002.

BARBOSA, R. da S.; CURY, L. V. M.; BOTELHO, G. S. Induzimento, instigação e auxílio ao suicídio no ambiente virtual a partir da Lei 13.968/2019. **STUDIES IN SOCIAL SCIENCES REVIEW**, [S. l.], v. 5, n. 1, p. 39–57, 2024. DOI: 10.54018/sssrv5n1-003. Disponível em:

https://ojs.studiespublicacoes.com.br/ojs/index.php/sssr/article/view/4468. Acesso em: 24 oct. 2024.

BC aperfeiçoa os mecanismos de segurança do Pix e estabelece 16 de junho de 2025 como nova data de lançamento do Pix Automático. **Banco Central do Brasil, 2024**. Disponível em: < https://www.bcb.gov.br/detalhenoticia/20227/nota>. Acesso em: 09 nov. 2024.

BEATO F, Cláudio; PEIXOTO, Betânia Totino; ANDRADE, Mônica Viegas. Crime, oportunidade e vitimização. **Revista brasileira de ciências sociais**, 2004, 19: 73-89.

BECCARIA, Cesare. **Dos delitos e das penas**. Trad. Flórido De Angelis. Ed. Edipro. Bauru, 2001.

BRASIL é o terceiro maior consumidor de redes sociais em todo o mundo. **Forbes, 2023**. Disponível em <https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>. Acesso em: 11 jun. 2024.

BRASIL. Fórum Brasileiro de Segurança Pública. Disponível em <https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/>. Acesso em: 18 nov. 2024.

BRASIL já é o 5º país com mais usuários de internet no mundo. **Forbes, 2022**. Disponível em: <https://forbes.com.br/forbes-tech/2022/10/brasil-ja-e-o-5o-pais-com-mais-usuarios-de-internet-no-mundo/>. Acesso em: 20 mar. 2024.

BRASIL vive aumento no número de crimes cibernéticos. **Valor Econômico, 2023**. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2023/08/01/brasil-vive-aumento-no-numero-de-crimes-ciberneticos.ghtml>. Acesso em: 06 nov. 2024.

CAPOBIANCO, Ligia. A Revolução em Curso: Internet, Sociedade da Informação e Cibercultura. **Estudos em Comunicação** nº7 - Volume 2, 175-193, 2010.

CASTELLS, Manuel. **A sociedade em rede**. Tradução de Roneide Venâncio Majer. 6 ed. São Paulo: Paz e Terra, 2002.

CELLA, Patrícia de Oliveira Gasieri. Cibercultura: Uma realidade no Mundo Virtual. **Revista CESUMAR – Ciências Humanas e Sociais Aplicadas**, v. 10 n. 1 (2005): jan./jun.

CELULAR segue como aparelho mais utilizado para acesso à internet no Brasil. **Ministério das Comunicações (Governo brasileiro), 2022**. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2022/setembro/celular-segue-como-aparelho-mais-utilizado-para-acesso-a-internet-no-brasil>. Acesso em: 20 mar. 2024.

COHEN, Lawrence E.; FELSON, Marcus. Social Change and Crime Rate Trends: A Routine Activity Approach. **American Sociological Review**, vol. 44, no. 4, 1979, pp. 588–608. JSTOR, https://doi.org/10.2307/2094589. Acesso em: 08 nov. 2024.

COOK, Steven; GIOMMOLI, Luca; PAREJA, Nicolas Trajtenberg; LEVI, Michael; WILLIAMS, Matthew L. Fear of Economic Cybercrime Across Europe: A Multilevel

Application of Routine Activity Theory. **The British Journal of Criminology**, 2023, 63, 384–406. DOI: https://doi.org/10.1093/bjc/azac021.

COX III, Raymond W. et al. Routine Activity Theory and Internet Crime. In **Crimes of the Internet**. Pearson Prentice Hall, New Jersey, 2008.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
DURKHEIM, Émile, 1858-1917. **As regras do método sociológico**. Tradução: Paulo Neves, revisão da tradução Eduardo Brandão – 3ª ed. – São Paulo: Martins Fontes, 2007 – (Coleção tópicos).

ELLOVITCH, Mauro da Fonseca. Extorsão cibernética, estupro virtual e sextorsão: a chantagem na era digital. **Consultor Jurídico, 2023**. Disponível em: <https://www.conjur.com.br/2023-dez-16/extorsao-cibernetica-estupro-virtual-e-sextorsao-a-chantagem-na-era-digital/>. Acesso em: 05 nov. 2024.

EM 2022, Internet estava presente em 91,5% dos domicílios do país. **Agência Gov, 2023**. Disponível em: <https://agenciagov.ebc.com.br/noticias/202311/em-2022-streaming-estava-presente-em-43-4-dos-domicilios-com-tv>. Acesso em: 03 jun. 2024.

ESTUDO mostra que pandemia intensificou uso das tecnologias digitais. **Agência Brasil, 2021**. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais>. Acesso em: 10 nov. 2024.

FARIAS, P. J. L. Respeito às Funções Urbanísticas e a Prevenção da Criminalidade Urbana: Uma Visão Integrada à Luz da Escola de Chicago. **Direito Público**, [S. l.], v. 4, n. 15, 2010. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/1416. Acesso em: 8 nov. 2024.

FERNANDES, Rodrigo Alisson. **Efeitos contextuais no risco de vitimização criminal: testando teorias de Atividades Rotineiras e Estilo de Vida/Exposição em diferentes estratos urbanos de Belo Horizonte**. Dissertação (Mestrado em Sociologia) – Faculdade de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais. Belo Horizonte, 2006.

FONSECA, Mayara de Sousa Guimarães. CIBERESPAÇO E SUAS CONTRADIÇÕES: a questão do analfabetismo digital. **Revista Igapó**, [S. l.], v. 5, n. 1, 2022. Disponível em: https://igapo.ifam.edu.br/index.php/igapo/article/view/61. Acesso em: 17 jun. 2024.

FONTES, Gabriela Scroczynski; LIMA E GOMES, Icléia Rodrigues de. Cibercidades: as tecnologias de comunicação e a reconfiguração de práticas sociais. **Informação & Informação**, [S. l.], v. 18, n. 2, p. 60–76, 2013. DOI: 10.5433/1981-8920.2013v18n2p60. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/16161. Acesso em: 30 jul. 2024.

GONTIJO, Cynthia Rúbia Braga; SILVA, Ivone Maria Mendes; VIGGIANO, Adalci Righi; PAIXÃO, Edmilson Leite; TOMASI, Antônio de Pádua Nunes. Ciberespaço: que território é esse?. **Educ. Tecnol.**, Belo Horizonte, v. 12, n. 3, p. 34-38, set./dez. 2007.

IBGE: Internet está em 91,5% dos domicílios. **ABRANET, 2023**. Disponível em: <https://www.abranet.org.br/Noticias/IBGE%3A-Internet-esta-em-91%2C5%25-dos-domicilios-4623.html>. Acesso em: 04 jun. 2024.

INTERNET chega a 87,2% dos brasileiros com mais de 10 anos em 2022, revela IBGE. **Ministério das Comunicações (Governo brasileiro), 2023**. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2023/novembro/internet-chega-a-87-2-dos-brasileiros-com-mais-de-10-anos-em-2022-revela-ibge>. Acesso em: 04 jun. 2024.

LEI com penas mais duras contra crimes cibernéticos é sancionada. **Agência Senado, 2021**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada>. Acesso em: 24 out. 2024.

LEMOS, André, **Cibercultura, tecnologia e vida social na cultura contemporânea**, Porto Alegre, Sulina, 2004.

LEMOS, André. Cibercultura y movilidad: una era de conexión. **Razón y Palabra**, [S. l.], v. 22, n. 1_100, p. 107–133, 2018. Disponível em: https://www.revistarazonypalabra.org/index.php/ryp/article/view/1145. Acesso em: 17 set. 2024.

LEMOS, André. Ciber-socialidade: tecnologia e vida social na cultura contemporânea. **Logos**, [S. l.], v. 4, n. 1, p. 15–19, 2015. Disponível em: https://www.e-publicacoes.uerj.br/logos/article/view/14575. Acesso em: 3 out. 2024.
LEMOS, André. Cidade-ciborgue: a cidade na cibercultura. **Galáxia**, n. 8, p. 129-148, 2004.

LÉVY, Pierre. **A inteligência coletiva por uma antropologia do ciberespaço**. Tradução: Luiz Paulo Rouanet. São Paulo: Editora Loyola, 1998.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu Costa – São Paulo: Ed. 34, 1999.

LUMI KAMIMURA MURATA, Ana Maria; RITZMANN TORRES, Paula. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?. **Boletim IBCCRIM**, [S. l.], v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 15 out. 2024.

MACHADO, Luís Antônio Licks Missel; SILVA, Jardel Luís da. Crimes digitais: o aumento da complexidade das relações sociais e os novos espaços de intervenção estatal. **Revista Eletrônica de Ciências Contábeis**, 2013, n. 3, p. 64-73. Acesso em: 29 mai. 2024.

MALHEIRO, Emerson Penha. DIREITOS HUMANOS NA SOCIEDADE DA INFORMAÇÃO. **Revista Paradigma**, [S. l.], v. 25, n. 1, 2017. Disponível em: https://revistas.unaerp.br/paradigma/article/view/218-230. Acesso em: 17 jun. 2024.

MORILLO PUENTE, Solbey; RÍOS HERNÁNDEZ, Iván Neftalí. Cibervictimización en el marco de la Teoría de Actividades Rutinarias en la era digital. **Revista de Psicología** (PUCP), 2022, 40.1: 265-291.

MOURA, Grégore Moreira de. **Curso de direito penal informático** – 1. ed. – Belo Horizonte, São Paulo: D'Plácido, 2021.

O QUE são crimes cibernéticos e como se proteger deles?. **Kaspersky, 2024**. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acesso em: 15 out. 2024.

OMS declara fim da Emergência de Saúde Pública de Importância Internacional referente à COVID-19. **OPAS, 2023**. Disponível em: <https://www.paho.org/pt/noticias/5-5-2023-oms-declara-fim-da-emergencia-saude-publica-importancia-internacional-referente>. Acesso em: 10 nov. 2024.

PABLOS DE MOLINA, Antônio Garcia. **Criminologia**: uma introdução a seus fundamentos teóricos. Tradução de: Luiz Flávio Gomes. 3ª. ed. Revista dos tribunais. São Paulo, 2002.

PABLOS DE MOLINA, Antonio Garcia. **Criminologia**, 5ª edição revista e atualizada, São Paulo: Revista dos Tribunais, 2006.

PINOCHET, Luis Hernan Contreras. **Tecnologia da informação e comunicação** - 1. ed. - Rio de Janeiro: Elsevier, 2014.

PINTO, Liliana Patrícia Peralta. **Impacto da pandemia de Covid-19 no uso da Internet e nos comportamentos de interação sexual online**. Dissertação (Mestrado em Psicologia) – Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto. Porto/Portugal, 2021.

PNAD Contínua - Pesquisa Nacional por Amostra de Domicílios Contínua. **IBGE.** Disponível em: <https://www.ibge.gov.br/estatisticas/sociais/populacao/9171-pesquisa-nacional-por-amostra-de-domicilios-continua-mensal.html?=&t=o-que-e>. Acesso em: 03 jun. 2024.

PRATT, Travis C.; HOLTFRETER, Kristy; REISIG, Michael D.. Routine Online Activity and Internet Fraud
Targeting: Extending the Generality of Routine Activity Theory. **Journal of Research in Crime and Delinquency, 2010**. DOI: 10.1177/0022427810365903.

PORTO, Ana Paula Teixeira; FADANELLI, Eberson Luiz. CIBERCULTURA, TECNOLOGIAS E EXCLUSÃO DIGITAL. **Revista Literatura em Debate**, [S. l.], v. 14, n. 26, p. 33–44, 2020. Disponível em: https://revistas.fw.uri.br/literaturaemdebate/article/view/2407. Acesso em: 7 out. 2024.

QUANTIDADE de brasileiros com internet, mas sem saneamento básico, equivale à população do Equador. **Revista Piauí, 2023**. Disponível em: <https://piaui.folha.uol.com.br/quantidade-de-brasileiros-com-internet-mas-sem-saneamento-basico-equivale-populacao-do-equador/#:~:text=Em%20janeiro%20deste%20ano,a%20servi%C3%A7os%20de%20saneamento%20b%C3%A1sico.>. Acesso em: 13 jun. 2024.

SANTOS, Gláucia Regina Silva; BARROS, Glhevysson Santos. Um olhar sobre as cidades contemporâneas: dinâmica de organização e funcionamento. **Revista Eletrônica do Instituto de Humanidades**, [S. l.], v. 24, n. 50, p. 26–36, 2020. Disponível em: https://publicacoes.unigranrio.edu.br/reihm/article/view/6333. Acesso em: 1 out. 2024.

SANTOS, Juarez Cirino dos. **Direito penal**: parte geral I - 6. ed., ampl. e atual. - Curitiba, PR: ICPC Cursos e Edições, 2014.

SATUF, Ivan. Onde está o ciberespaço? A metáfora da "nuvem" aplicada aos estudos da cibercultura. **AÇÃO MIDIÁTICA**, n.11. Jan/jun. 2016. Curitiba. PPGCOM-UFPR. ISSN 2238-0701.

SILVA, Cristiane. Determinantes da vitimização no Brasil. **Revista Cadernos de Economia**, Chapecó, v. 19, n. 35, p. 30-46, jan./jun. 2015.

SILVA, Taziane Mara da; TEIXEIRA, Talita de Oliveira; FREITAS, Sylvia Mara Pires de. Ciberespaço: uma nova configuração do ser no mundo. **Psicol. rev. (Belo Horizonte)**, Belo Horizonte, v. 21, n. 1, p. 176-196, jan. 2015. Disponível em <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-11682015000100012&lng=pt&nrm=iso>. Acesso em 01 ago. 2024.

SIMÕES, Isabella de Araújo Garcia. A Sociedade em Rede e a Cibercultura: dialogando com o pensamento de Manuel Castells e de Pierre Lévy na era das novas tecnologias de comunicação. **Revista eletrônica Temática**. Ano V, n. 05 – Maio/2009.

SOCIOLOGIAS, C. E.; MADEIRA, L. M. "Espaço urbano e criminalidade: lições da Escola de Chicago" - FREITAS, Wagner Cinelli de Paula. O retorno da cidade como objeto de estudo da sociologia do crime. **Sociologias**, [S. l.], v. 5, n. 9, 2008. Disponível em: https://seer.ufrgs.br/index.php/sociologias/article/view/5885. Acesso em: 8 nov. 2024.

SOUZA, Ludimila de Freitas; VIANA, André de Paula. Marco civil da internet e os crimes virtuais. **Conteúdo Jurídico, 2021**. Disponível em:https://conteudojuridico.com.br/consulta/Artigos/51965/marco-civil-da-internet-e-os-crimes-virtuais. Acesso em: 05 nov. 2024.

SPINELLI, Egle Müller; RAMOS, Daniela Osvald. Desordem informacional no ecossistema digital das eleições brasileiras de 2018. **As fake news e a nova ordem (des)informativa na era da pós-verdade.** FIGUEIRA, João; SANTOS, Sílvio (Orgs.). Imprensa da Universidade de Coimbra, 2019. Disponível em: <https://books.uc.pt/chapter?chapter=67856>. Acesso em: 27 jun. 2024.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático** – Partes Geral e Especial – 4. ed. rev. e atual. – São Paulo: Editora Juspodivm, 2023.

TRÊS em cada 10 brasileiros são analfabetos funcionais**. Revista Educação, 2018**. Disponível em: <https://revistaeducacao.com.br/2018/08/08/tres-em-cada-10-brasileiros-sao-analfabetos-funcionais-1/>. Acesso em: 27 jun. 2024.

USO educacional do celular com internet ajudaria a reduzir analfabetismo funcional. **Inaf, 2020**. Disponível em: <https://alfabetismofuncional.org.br/uso-educacional-do-celular-com-internet-poderia-ajudar-a-reduzir-o-analfabetismo-funcional-no-brasil/>. Acesso em: 27 jun. 2024.

VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito Processual) - Universidade Federal de São Paulo, São Paulo, 2012. Acesso em: 29 mai. 2024.

VIANA, Eduardo. **Criminologia**. Salvador: JusPodivm, 2023.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2003.

WALDMAN, Ricardo; ZAMBRANO, Virginia; RONHA, Amanda Nunes. Erosão do ciberespaço e da cibercultura na privacidade a luz das teorias de Pierre Levy e Manuel Castells. **Revista Direito Mackenzie**, v. 17 n. 1 (2023).

WEISS, Marcos Cesar. Sociedade sensoriada: a sociedade da transformação digital. **Estudos Avançados**, v. 33, n. 95, p. 203–214, jan. 2019. Disponível em: <https://doi.org/10.1590/s0103-4014.2019.3395.0013>. Acesso em: 03 jul. 2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação – 2. ed. – Rio de Janeiro: Brasport, 2013.

WILLIAMS, Matthew L. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level, **The British Journal of Criminology**, Volume 56, Issue 1, January 2016, Pages 21–48, DOI: https://doi.org/10.1093/bjc/azv011.

WOJCIECHOWSKI, Paola Bianchi. A fábrica midiática de inimigos e o risco à democracia. Uma análise do papel dos grandes meios de comunicação na elaboração e adoção de leis penais casuísticas no Brasil. **Sistema Penal & Violência**, Porto Alegre, v. 7, n. 1, p. 49-65, jan.-jun. 2015.

XAVIER, Arnaldo. A construção do conceito de criminoso na sociedade capitalista: um debate para o Serviço Social. **Rev. Katál.** Florianópolis v. 11 n. 2 p. 274-282 jul./dez. 2008.

ZACARIAS, Fabiana; FREIRE, Lucas Zacharias. Crimes virtuais: análise das dificuldades e limitações ao combate. **REVISTA JurES** - v.16, n.29, p. 29-61, jun. 2023.

ZANI MORGADO, H. Criminalização do bullying e do cyberbulliyng: o Estado penal ataca novamente. **Boletim IBCCRIM**, [S. l.], v. 32, n. 376, p. 27–30, 2024. DOI: 10.5281/zenodo.10685205. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/982. Acesso em: 24 out. 2024.