



INSTITUIÇÃO AFYA
CENTRO UNIVERSITÁRIO DE BARREIRAS
BACHARELADO EM DIREITO

VITÓRIA BEATRIZ DO BOMFIM SILVA

**OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS COM ENFOQUE
NAS REDES SOCIAIS**

Barreiras - Bahia

2026

VITÓRIA BEATRIZ DO BOMFIM SILVA.

**OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS COM ENFOQUE
NAS REDES SOCIAIS.**

Artigo Científico submetido como requisito
para a obtenção do grau de Bacharel em
Direito da Faculdade Afya Centro
Universitário de Barreiras.

Orientador: Dr. Mateus Baldin

Barreiras - Bahia

2026

VITÓRIA BEATRIZ DO BOMFIM SILVA.

**OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS COM ENFOQUE
NAS REDES SOCIAIS.**

Trabalho de conclusão do curso de Bacharelado em Direito da AFYA Centro
Universitário – Barreiras – BA, como requisito para conclusão de graduação.

Barreiras - BA, 07 de Julho de 2026

BANCA EXAMINADORA

Professor(a) Orientador: Dr. Mateus Baldin

Membro da Banca 1

Membro da Banca 2

S586d Silva, Vitória Beatriz do Bomfim

Os desafios no combate aos crimes cibernéticos com enfoque nas redes sociais. / Vitória Beatriz do Bomfim Silva -- Barreiras, 2026.
22 p.

Trabalho de Conclusão de Curso – Artigo científico (Graduação – Curso de Direito) Faculdade Afya Centro Universitário de Barreiras.
Orientador (a): Prof. Dr. Mateus de Campos Baldin.

1. Crimes cibernéticos. 2. Redes sociais. 3. Segurança digital. I. Baldin, Mateus de Campos II. Título.

CDU 343
CDD 345.02

Ficha catalográfica elaborada pelo Bibliotecário
Ednilson M. Brito Filho – CRB 5/1743

AGRADECIMENTOS

Agradeço a Deus, por ter segurado minha mão durante toda caminhada. Em muitos momentos pensei que não conseguiria chegar até aqui. Teve dias de cansaço, medo, insegurança e noites em que dormi chorando, sem saber como as coisas iriam acontecer. E mesmo quando tudo parecia difícil demais, o Senhor me sustentou e me deu forças para continuar. Sua presença me deu a certeza de que eu nunca estive sozinha. Obrigada por acalmar meu coração e sempre renovar minha fé.

À minha mãe, Vivaldina, os meus sinceros agradecimentos. Em você sempre enxerguei o verdadeiro significado da força. Se hoje celebro esse momento, foi porque antes de mim existiu uma mulher forte, feita de esforços, renúncias, orações e amor, sustentando cada etapa da minha caminhada. Durante toda minha vida, a senhora trabalhou incansavelmente para que eu e meu irmão tivéssemos oportunidades, que muitas vezes lhe foram negadas. A senhora acreditou na educação como instrumento de transformação e fez dela uma ponte para os nossos sonhos. Nada do que conquistei será capaz de retribuir tudo o que fez por mim. Esse trabalho é a prova de que cada sacrifício valeu a pena. Obrigada por nunca medir esforços pela minha educação, por me mostrar, através da sua própria história, que a determinação é capaz de transformar vidas. Minha eterna gratidão, amor e admiração serão sempre seus, Dona Vivi.

Dedico esse trabalho ao meu namorado, Danilo Franco. Que esteve ao meu lado durante toda essa caminhada, você foi uma das razões pelas quais essa conquista se tornou possível. A sua presença fez diferença em cada etapa deste percurso, especialmente nos momentos de dúvida e dificuldade, quando suas palavras e apoio sustentaram meus passos. Esse trabalho consta apenas a minha autoria, mas inúmeras pessoas contribuíram, em especial, meu namorado Danilo Franco, a quem sempre esteve por perto, me apoiando e sempre me motivando. Sua ajuda foi fundamental, não apenas com suas orientações jurídicas, mas toda sua paciência, companheirismo e amor genuíno, contribuíram de forma significativa para que esse trabalho fosse concluído. Por isso, se essa conquista tem uma história, Danilo ocupa algumas das suas páginas mais importantes, mesmo que seu nome não esteja formalmente registrado. Sua dedicação ao Direito, sua sabedoria e sua disposição em compartilhar aquilo que sabe contribuíram de forma significativa para

o meu crescimento acadêmico e pessoal. Em muitos momentos, teve a paciência de ensinar, orientar e incentivar, despertando em mim uma vontade ainda maior de aprender e evoluir. Seu exemplo reforçou em mim o valor do conhecimento, da disciplina e da persistência. Por isso, esse trabalho leva meu nome, mas carrega parte da sua dedicação e apoio. Mais do que um agradecimento, fica o reconhecimento: esta conquista também é sua, meu amor.

Ao meu orientador Mateus Baldin, expresso minha sincera gratidão por todos os ensinamentos, pela orientação atenta e pela disponibilidade ao longo deste trabalho. A sua contribuição foi essencial para o desenvolvimento dessa pesquisa, guiando cada etapa com conhecimento, paciência e compromisso acadêmico. Agradeço por compartilhar sua experiência e por contribuir de forma significativa para a minha formação.

Aos professores, expresso minha sincera gratidão por todos os ensinamentos ao longo da graduação. Cada disciplina, orientação e troca de conhecimento foi essencial para minha formação acadêmica e pessoal. A dedicação e o compromisso de cada docente contribuíram diretamente para a construção do meu aprendizado, ampliando minha visão e fortalecendo minha trajetória no curso de direito. Levo comigo o respeito e a admiração por todos que fizeram parte desse processo.

Às minhas colegas de sala, agradeço a convivência, parceria e pelos momentos compartilhados ao longo dessa fase. Em especial, Ana Beatriz, Andressa Vilaça, Laysa Shauanne.

OS DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS COM ENFOQUE NAS REDES SOCIAIS.

Vitória Beatriz Do Bomfim Silva.¹

Dr. Mateus Baldin.²

RESUMO

O presente projeto de pesquisa aborda os principais desafios enfrentados no combate aos crimes cibernéticos com enfoque nas redes sociais, diante do aumento das práticas criminosas no ambiente digital. A pesquisa analisa delitos como fraudes eletrônicas, estelionato digital, invasão de contas, crimes contra a honra e discurso de ódio, destacando as dificuldades existentes na identificação dos autores e na produção de provas no meio virtual. O estudo também analisa a influência da impunidade, das cifras negras e das deficiências estruturais dos órgãos responsáveis pela investigação criminal no crescimento da criminalidade digital. Além disso, discute o fenômeno da mancha criminal no ambiente virtual e a relevância desses dados para subsidiar o poder público na formulação de políticas e estratégias voltadas à prevenção, investigação e redução da incidência dos crimes cibernéticos. Ademais, o trabalho apresenta medidas de prevenção e enfrentamento desses delitos, destacando a importância da educação digital, da conscientização dos usuários, do fortalecimento das atividades investigativas e da utilização de ferramentas tecnológicas especializadas. Tais ações visam promover maior segurança no ambiente virtual e contribuir para a eficácia do combate aos crimes cibernéticos.

Palavras-chave: Crimes cibernéticos. Redes sociais. Segurança digital. Investigação criminal. Educação digital. Cifras negras. Inteligência artificial.

ABSTRACT

This research project addresses the main challenges faced in combating cybercrimes, particularly those occurring on social media, given the increase in criminal activity in the digital environment. The research analyzes crimes such as electronic fraud, digital scams, account hacking, crimes against honor, and hate speech, highlighting the difficulties in identifying perpetrators and gathering evidence in the virtual world. The study also analyzes the influence of impunity, unreported crimes, and structural deficiencies in the agencies responsible for criminal investigation on the growth of digital crime. Furthermore, it discusses the appearance of the criminal landscape in the virtual environment and the relevance of this data to support public authorities in formulating policies and strategies aimed at preventing, investigating, and reducing the incidence of cybercrimes. In addition, the work presents measures for preventing and combating these crimes, emphasizing the importance of digital education, user awareness, strengthening investigative activities, and the use of specialized technological tools. These actions aim to promote greater security in the virtual environment and contribute to the effectiveness of combating cybercrimes.

Keywords: Cybercrime. Social Media. Digital Security. Criminal Investigation. Digital Education. Dark Figure of Crime. Artificial Intelligence.

¹ Discente do curso de Direito da AFYA Centro Universitário – Barreiras – BA

² Graduado em Ciências Jurídicas e Sociais – Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). Mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). Doutor em Filosofia pela Universidade Federal do Rio Grande do Sul (UFRGS). Professor universitário, com experiência nas áreas de Filosofia do Direito, Ética, Filosofia Política e Introdução à Filosofia.

SUMÁRIO

1. INTRODUÇÃO.....	7
2. CRIME CIBERNÉTICO E EVOLUÇÃO TECNOLÓGICA	8
3. TEORIA DAS JANELAS QUEBRADAS.....	9
4. CRIME CIBERNÉTICO	11
5. MECANISMO DE ACESSO.....	13
6. MANCHA CRIMINAL	15
7. CIFRAS DO DIREITO PENAL	16
7.1. CIFRAS NEGRAS E CINZAS	16
8. SUCATEAMENTO DAS POLÍCIAS.....	17
CONCLUSÃO.....	20

1. INTRODUÇÃO.

O combate aos crimes cibernéticos é um assunto que requer um conjunto de ações coordenadas, objetivando a diminuição da mancha criminal. Levando em consideração o ambiente virtual. Nesse sentido, um dos principais desafios é regulamentar, de forma efetiva, o acesso ao meio digital, pois tratar-se de um ambiente virtual amplo. Algumas medidas a curto, médio e longo prazo devem ser implementadas a fim de coibir as reiteraões delituosas. Já que a efetividade do combate aos crimes cibernéticos perpassa por uma questão multifatorial que merece uma maior atenção da política criminal.

Com o avanço das tecnologias digitais e o surgimento de novas redes sociais, também emergiram novas modalidades de delitos praticados no ambiente virtual, resultando em um crescimento constante da incidência dos crimes cibernéticos. Nesse contexto, o combate a essas práticas ilícitas exige uma atuação integrada, eficiente e célere por parte dos órgãos competentes, bem como o aprimoramento contínuo dos mecanismos de prevenção e repressão. Dessa forma, este trabalho, com enfoque nas redes sociais, justifica-se pela relevância social e jurídica da temática, considerando a necessidade de compreender e combater o avanço dos crimes cibernéticos nesses ambientes digitais, que se tornaram espaços amplamente utilizados para comunicação, interação e compartilhamento de informações.

A presente pesquisa tem como objetivo analisar os desafios enfrentados no combate aos crimes cibernéticos com enfoque nas redes sociais. Para alcançar os objetivos propostos e conferir o rigor científico necessário à pesquisa, o trabalho busca examinar os principais obstáculos jurídicos, tecnológicos e institucionais relacionados à prevenção e repressão dessas infrações. Além disso, pretende analisar o cenário dos crimes cibernéticos no Brasil, com base em dados oficiais divulgados por órgãos públicos e em informações fornecidas por instituições privadas, a fim de compreender a dimensão do problema e suas implicações no contexto da política criminal contemporânea. O trabalho tem como Hipótese: A dificuldade de identificação dos infratores, a velocidade de propagação dos crimes digitais e a necessidade de

aprimoramento dos mecanismos de investigações. A Metodologia utilizada foi a revisão bibliográfica, utilizando livros, artigos científicos, legislação, publicação de órgãos públicos e órgãos de segurança digital e crimes cibernéticos. Tendo como referencial teórico os autores: Rogério Sanches, Rogério Greco, José César Naves de Lima Junior.

2. CRIME CIBERNÉTICO E EVOLUÇÃO TECNOLÓGICA

Os crimes migraram para um novo ambiente, o virtual, e vêm crescendo de forma vertiginosa. A facilidade e a falta de regulamentação e fiscalização do ambiente virtual favorecem a prática de crimes, como, por exemplo, os crimes contra a honra e os crimes patrimoniais. Há indivíduos que agem como se a internet fosse uma terra sem lei, o que, de fato, não é verdade. Em um cenário bastante preocupante, as polícias e os órgãos públicos não dispõem de meios e ferramentas suficientes para combater a ação delituosa. Cada vez mais, os cibercriminosos lançam mão de recursos tecnológicos avançados para burlar as diretrizes das plataformas, que não conseguem identificar tais práticas nem realizar o banimento dos infratores com a rapidez necessária.

Diante disso surgem desafios a serem superados para alcançar um ambiente virtual seguro, que envolve as próprias plataformas, os usuários, especialistas de segurança em crimes cibernéticos, governo, e as autoridades policiais. É incluído a conscientização dos usuários, a implementação de novas tecnologias para combater a expansão dos crimes cibernéticos, a melhoria da política de segurança e privacidade das plataformas, assim o trabalho conjunto irá desenvolver em um ambiente virtual mais seguro para os usuários.

O avanço das tecnologias de informação e comunicação, notadamente a proliferação das redes sociais, redefiniu o espaço de interação humana e paralelamente a essa evolução, a sociedade assiste à transposição de condutas delituosas do meio físico para o virtual, dando origem aos crimes cibernéticos. Tais ilícitos, que englobam desde o estelionato eletrônico até crimes contra a honra e a dignidade da pessoa humana, fato esse, preocupante, tendo em vista o crescimento alarmante desses delitos no âmbito virtual.

3. TEORIA DAS JANELAS QUEBRADAS

Em sua obra de Manual de Criminologia, o Professor José César Naves de Lima Júnior, relata o experimento que deu origem a chamada Teoria das Janelas Quebradas, desenvolvida a partir de um estudo sobre a relação desordem social e criminalidade. Sobre o tema, o autor destaca:

A Teoria das Janelas Quebras baseou-se em um trabalho acerca da relação de causalidade entre desordem e criminalidade, intitulado *The Police and Neighborhood Safety* (A Polícia e Segurança da Comunidade). Na qual baseou-se, conforme o magistério de Sumariva, em experimento realizado por Philip Zimbardo, psicólogo da Universidade de Stanford, consistente em abandonar um automóvel em bairro de classe alta de Palo Alto, Califórnia. Na primeira semana o veículo não foi danificado. Assim, o pesquisador quebrou uma das janelas do carro, e depois disso o veículo foi destruído e roubado por vândalos em curto espaço de tempo.

A teoria defende a repressão de delitos menores para inibição dos mais graves. Essa teoria criou o movimento de tolerância zero implementado na cidade de New York pelo ex-prefeito Rudolph Giuliani.

Buscando compreender a dinâmica da criminalidade, os cientistas sociais James Q. Wilson e George Kelling desenvolveram a Teoria das Janelas Quebradas. Segundo essa teoria, toda conduta criminosa que não recebe uma resposta estatal adequada, suficiente e proporcional tende a estimular a prática de novos delitos. Em outras palavras, a ausência de repressão ou de intervenção eficaz pode contribuir para o aumento da criminalidade, conforme se observa a seguir:

Psicólogos sociais e policiais tendem a concordar que, se uma janela de um prédio for quebrada e não for consertada, todas as outras janelas logo serão quebradas. Isso é tão verdadeiro em bairros agradáveis quanto em bairros degradados. A quebra de janelas não ocorre necessariamente em grande escala porque algumas áreas são habitadas por pessoas determinadas a quebrar janelas, enquanto outras são povoadas por pessoas que gostam de quebrar janelas; em vez disso, uma janela quebrada não consertada é um sinal de que ninguém se importa, e, portanto, quebrar mais janelas não custa nada. (Sempre foi divertido.)

Pautado nos experimentos feitos por Philip Zimbardo, psicólogo da Universidade de Stanford. James Wilson e George Kelling, deram origem, assim, a teoria das janelas quebradas. Afirmavam que que pode ser traduzida da seguinte forma teoria bem recorrente em assunto de política criminal. Inúmeros autores criaram teorias criminológicas que dão amparo para que condutas que as vezes são consideradas de menor potencial ofensivo tenham a necessidade de reprimidas de forma mais gravosa. Posteriormente George Kelling e Catharine Coles, afirmavam

que se os crimes forem reprimidos de forma mais rápida enquanto são pequenos, as chances de uma reiteração criminosa ocorrer, caem drasticamente. políticas criminais pautadas na teoria das janelas quebradas mostraram resultados significativos, em Nova Iorque, cidade onde a teoria foi desenvolvida e colocada em prática. Diante da crescente onda de crimes cibernéticos, a política de tolerância zero, seria uma alternativa muito viável a ser implantado no Brasil, tendo em vista, o crescimento acelerado dos crimes cibernéticos.

Vários pontos devem ser enfrentados para que os índices de criminalidade diminuam. Entre eles, destaca-se a necessidade de maior atenção aos grupos vulneráveis, que figuram entre as principais vítimas dos crimes cibernéticos, tais como crianças, idosos e pessoas com baixa instrução digital.

Outro ponto crucial a ser levado em consideração são os baixos investimentos e o sucateamento das Polícias investigativas, os baixos salários, a sobrecarga de trabalho, decorrente do déficit de servidores e falta de concurso públicos, o que acaba sobrecarregando todo o efetivo policial, a falta de estrutura, e falta condições adequadas de trabalho impedem a prestação de um serviço público eficiente e humanizado, além da lentidão crônica do judiciário que cria um gargalo em todo sistema de justiça. Todos esses fatores contribuem de forma direta e indireta para aumento da mancha criminal no meio digital.

A dinâmica de atuação dos criminosos no ambiente virtual é um fator determinante para a impunidade dos criminosos, tendo em vista, que esses utilizam perfis “fakes” para ocultar sua real identidade, tornando assim um desafio ainda mais difícil combater os crimes cibernéticos.

O aumento exponencial do uso da internet e a democratização do acesso a redes sociais através dos computadores e smartphones, trouxe inúmeros benefícios. Como por exemplo, a facilitação na intercomunicabilidade, no entanto, também trouxe algumas mazelas sociais para o cenário cotidiano do brasileiro, como por exemplo o aumento dos crimes de estelionato digital, crime de stalking, e o induzimento ou instigação, através das redes sociais, alguém a suicidar-se ou a praticar automutilação.

Segundo o IBGE nos últimos 10 anos o alcance da internet nas famílias brasileira cresceu de 54% para 77%. A população brasileira ocupa a terceira colocação no cenário mundial em horas conectada a internet com uma média de mais de 10 horas de conexão diária, isso conseqüentemente, faz com que os crimes

cibernéticos cresçam na mesma proporção pois, mais usuários na rede maior será a incidência de crimes cibernéticos. Entre os crimes com maior incidência são: Delitos envolvendo discurso do ódio, discriminação, racismo, Fraudes bancárias e pornografia infantojuvenil no meio digital. Todos esses delitos têm impactado de forma prejudicial a convivência social.

4. CRIME CIBERNÉTICO

Os crimes cibernéticos constituem condutas criminosas praticadas pela rede mundial de computadores ou por qualquer sistema informático, como, por exemplo, tablets, smartphones e computadores. A doutrina moderna faz uma distinção pedagógica, classificando os crimes cibernéticos em próprios e impróprios. Os crimes próprios são aqueles cujo tipo penal descreve uma conduta que somente se configura quando praticada por meio digital, como a prevista no artigo 313-A (inserção de dados falsos em sistema de informações). Já os crimes cibernéticos impróprios são aqueles que podem ou não ser praticados no meio digital, como, por exemplo, as fraudes bancárias previstas nos artigos 155 e 171 do Código Penal. De acordo com Silva (2016), o desenvolvimento dos crimes virtuais caminha de forma paralela ao aprimoramento tecnológico das técnicas de cifragem de dados

A criptografia ressaltando a definição de crimes virtuais, é importante compreender que ela está ligada ao conceito de criptografia. Eis alguns aspectos relevantes para o avanço desse estudo: conceitualmente, criptografia se traduz em esconder ou mascarar informações por meio de linguagem codificada, essa é uma prática quase tão antiga quanto a própria humanidade, pois já no período de conflitos entre a Grécia e a Pérsia emergia-se a necessidade de transmitir informações secretamente, ocultando-as, de maneira que somente o destinatário final da mensagem seria capaz de decifrá-la. (Silva, 2016).

Nos crimes cibernéticos, a percepção dos indícios pode ser um pouco mais sensível, pois as provas apresentam uma volatilidade muito grande, o que contribui para a perda dos indícios. Sendo assim, a investigação deve ser rápida e ágil. No mundo digital, a volatilidade dos vestígios é muito grande, podendo ocorrer inúmeras transformações e até mesmo a perda definitiva das informações que transitam no meio digital, ou a quebra da cadeia de custódia, o que inviabiliza a utilização dos elementos de prova coletados.

Os crimes cibernéticos têm um alcance que transpõe fronteiras, essa peculiaridade dos crimes cibernéticos contribui ainda mais para um cenário social de

insegurança e prejuízos financeiros, já que mesmo descobrindo a identidade dos criminosos, não é certeza que ele será punido ou que os bens sejam recuperados, tendo em vista que a jurisdição brasileira esbarra na questão da soberania dos países onde os criminosos encontra-se e de onde partiu o ataque. Dessa forma esclarece Daniel Menah Cury Soares quando afirma que:

Uma das características marcantes dos crimes informáticas é a transnacionalidade, o que significa que uma pessoa de qualquer cidade, estado ou país pode cometer crimes contra qualquer pessoa conectada à rede, não importando o local onde a vítima e o agressor se conectam. Isso traz problemas quanto à questão da territorialidade do crime. Apesar dessa “quebra de fronteiras”, cada país possui a sua própria soberania acerca da investigação e punição à crimes informáticos. (Soares, 2026, p. 12)

Os desafios para combater os crimes cibernéticos e consequentemente a redução da mancha criminal é muito complexo e multifatorial, considerando que a internet não abrange um espaço territorial físico, mas sim um amplo ambiente virtual que se consubstancia em um conjunto binário e “amontoadado de bits”. Muitos criminosos utilizam dessa complexidade para cometer diversos crimes, esses indivíduos sabem da dificuldade enfrentadas pela polícia investigadora e as plataformas para chegar na identidade dos criminosos

Ciente disso os cibercriminosos compreende que a impunidade é um incentivo à prática criminosa, porque é como se os cibercriminosos fossem bonificados ao invés de punidos, ou seja, há um encorajamento para que as práticas delituosas sejam cada vez mais proliferadas e difundidas no nosso país. Os criminosos têm ciência das limitações enfrentadas pelas autoridades públicas.

Além disso, com a expansão do acesso à internet e a comunicação digital, tornou-se um vetor disseminador de crimes, e seu foco principal tem sido através das redes sociais, território fértil para disseminar e propagar discursos de ódio crimes contra a hora, *bullying*, e crimes patrimoniais, crimes comuns nas redes sociais.

Os registros de ocorrências de crimes praticados por meio das redes sociais têm apresentado crescimento significativo nos últimos anos. Além dos casos oficialmente registrados pelos órgãos competentes, muitos usuários dessas plataformas relatam ter sido vítimas de condutas criminosas no ambiente virtual, embora frequentemente deixem de formalizar a denúncia junto às autoridades responsáveis.

A internet e as redes sociais estão intrinsecamente interligadas, estabelecendo uma rede de comunicação que possibilita a interação contínua entre os usuários. Nesse contexto, a internet funciona como a principal infraestrutura para o acesso às redes sociais, permitindo que essas plataformas alcancem um número cada vez maior de pessoas. Dessa forma, ambas desempenham papel fundamental na promoção da comunicação, do compartilhamento de informações e da participação dos indivíduos no ambiente digital.

Uma das principais dificuldades ao combate aos crimes cibernéticos está justamente no lapso temporal entre o cometimento do crime e a ação da polícia. Pois, a busca pela preservação dos dados referentes aos criminosos deve ser solicitada às plataformas digitais o mais rápido possível, tendo em vista a volatilidade dos dados digitais o que refletirá diretamente na cadeia de custódia, implicando diretamente na punibilidade dos criminosos.

Os crimes cibernéticos se propagam de forma muito rápida e atinge um número imensurável de pessoas ultrapassando fronteiras, os efeitos deletérios dos crimes cibernéticos podem ser considerados maiores que os crimes tradicionalmente praticados, tendo como exemplo o crime de estelionato 171, código penal, uma conduta praticada fora do mudo virtual pode ter alcance limitado de pessoas, já o mesmo crime de estelionato praticado no meio digital será bem mais maléfico, alcançando maior número de pessoas e causando um prejuízo financeiro vultoso.

Diante do atual cenário, muito breve o número de ocorrências policiais será bem maior no meio digital que fora dele, e conseqüentemente a atuação do poder público deverá ser pautada na atuação digital, atuando de forma mais analítica, no processamento dos dados, dando mais ênfase na prevenção, tendo em vista as peculiaridades dos crimes cibernéticos.

5. MECANISMO DE ACESSO

Uma medida que pode ser usada de forma mais ampla são os tokens de certificação digital ou o acesso biométrico. Para obter acesso à internet, cada cidadão apenas conseguiria acessar a rede se fizesse login no servidor por meio de tokens físicos ou virtuais, ou através de sua biometria ou de sua íris. Sendo assim, os usuários seriam facilmente identificados, o que diminuiria drasticamente o cometimento de crimes cibernéticos, já que a autoria dos delitos seria mais facilmente desvendada.

Essas poderiam ser consideradas medidas de curto prazo que surtiriam efeitos imediatos; no entanto, não resolveriam os crimes como um todo, tendo em vista que o crime em si é um fenômeno determinado por diversos fatores.

O desenvolvimento de políticas públicas voltadas para a educação digital seria uma boa medida de médio prazo, tendo em vista que seus efeitos não seriam sentidos de forma tão imediata, mas que, a médio prazo, refletiriam na diminuição das ocorrências criminais no meio digital. Pode-se citar, como medida de longo prazo, o endurecimento das penas em abstrato dos crimes praticados no meio digital, tendo em vista que o Estado agiria para coibir, em vez de apenas reagir à ocorrência do crime.

O desenvolvimento de políticas públicas voltada para a educação digital seria uma boa medida a médio prazo tendo em vista que seus efeitos não seriam sentidos de forma tão imediata, mas que a médio prazo iria refletir na diminuição das ocorrências criminal no meio digital. Pode-se citar como medida a longo prazo o endurecimento das penas em abstrato dos crimes praticados no meio digital, tendo em vista que o estado agiria para coibir ao invés de prevenir a ocorrência do crime.

Especialista recomenda as algumas sugestões de comportamento para reduzir à exposição aos crimes digitais, muito embora a forma que são praticados podem ser diferentes todos utilizam de gatilhos mentais e engenharia social para explorar a vulnerabilidade da vítima, exigindo uma ação positiva da vítima.

Tendo isso em mente, recomenda-se sempre a autentificação em dois fatores para evitar principalmente o sequestro de perfis digitais, que são utilizados posteriormente para aplicar inúmeros golpes. Evitar clicar em links desconhecidos evita, consideravelmente, a ocorrência do crime, pois quase 80% dos casos de crimes cibernéticos decorrem de links maliciosos.

Os usuários de redes sociais devem redobrar a atenção aos gatilhos mentais que estão muito presente nas redes sociais, pois, são capazes de provocar, por exemplo, o gatilho da escassez, criando um sentimento de perda ou urgência,

Com as famosas frases: “click aqui” e “resgate seu prêmio”, “últimas unidades”, “não perca essa chance”. Recomenda-se cautela e ponderação. Nesse mesmo fala-se sobre a alta exposição, onde alguns dados sensíveis são expostos nas redes sociais, como por exemplo, o endereço, a placa do carro, qual escola os filhos estudam, todos esses dados são utilizados por criminosos para aplicar golpes com a ajuda da engenharia social. Sendo assim, os cuidados básicos não devem ser

negligenciados, visto que na maioria das vezes os crimes digitais contam com a participação da própria vítima.

6. MANCHA CRIMINAL

A mancha criminal corresponde ao conjunto de dados estatísticos agrupados referentes às ocorrências de crimes e contravenções penais, além de outros dados correlacionados com os delitos. Tais dados têm o objetivo de facilitar a atividade do poder público, assim como servir de parâmetro para o direcionamento de políticas públicas e para definir onde as polícias deverão ter maior atenção e destinar maior efetivo, tendo em vista que a força de trabalho deve ser direcionada proporcionalmente para os locais ou ambientes com maior mancha criminal. Ou seja, a mancha criminal serve para estabelecer padrões de atuação dos órgãos e entidades envolvidos no combate à criminalidade, como, por exemplo, os órgãos policiais, o sistema de saúde e as secretarias de educação, os quais, conjuntamente, reunirão esforços para elaborar estratégias em determinadas áreas ou ambientes. Como no caso deste artigo, a mancha criminal, mais especificamente, será voltada para o ambiente virtual.

Com o propósito de criar atuações padronizadas, a mancha criminal tem como definição de uso o georreferenciamento, que é propriamente dito o local específico da ocorrência, geralmente consubstanciado por meio dos boletins de ocorrência. Nesse sentido, a análise e o planejamento consistem na análise dos dados coletados e, posteriormente, no planejamento para atuação dos órgãos envolvidos.

Um passo importante no combate ao crime foi a criação da Secretaria da Segurança Pública da Bahia. Em seu portal digital, a instituição explica como funcionará o novo Núcleo de Cartografia e Geoprocessamento, criado para dar mais exatidão às manchas criminais desenvolvidas no Estado e subsidiar políticas criminais. A matéria explica:

O geoprocessamento compreende um conjunto de tecnologias voltadas para o tratamento, manipulação e apresentação de dados espaciais. No âmbito da segurança pública, tem possibilitado a elaboração de análises criminais mais qualificadas e uma melhor interpretação dos dados.

Neste contexto, são realizados trabalhos de mapeamentos de ocorrências, manchas criminais, georreferenciamento de crimes, monitoramento da qualidade de dados espaciais, entre outros. Com o uso dessas tecnologias também foram delimitados os territórios de atuação do aparato policial.

Mapear os dados acerca da criminalidade e violência no Estado da

Bahia, objetivando subsidiar a avaliação e o planejamento das ações operacionais;

Elaborar e manter atualizadas as bases cartográficas necessárias para o mapeamento dos crimes no Estado da Bahia, implementando-as nos sistemas existentes no âmbito da Secretaria da Segurança Pública;

Elaborar estudos e relatórios técnicos que analisem os padrões espaciais dos crimes em todo Estado;

Georreferenciar dados de competência da Secretaria da Segurança Pública na Bahia;

A grande problemática são como essas políticas criminais são implementadas, esbarrando-se em excesso de burocrático e políticas públicas inacabadas, gerando morosidade e dispêndio de dinheiro público, contribuindo ainda mais para impunidade.

7. CIFRAS DO DIREITO PENAL

As cifras penais estão diretamente ligadas à mancha criminal. As estatísticas criminais servem para fundamentar a política criminal e a doutrina de segurança pública quanto à prevenção e à repressão criminais. No entanto, é preciso ter cuidado ao analisar as estatísticas criminais oficiais, na medida em que há uma quantia significativa de delitos não comunicados ao Poder Público, quer por inércia ou desinteresse das vítimas, quer por outras causas, entre as quais os erros de coleta e a manipulação de dados pelo Estado.

A doutrina classificou os crimes em “cifras”, a depender da modalidade praticada. Destacamos aquelas apontadas pelo professor Fernando Abreu em seu livro de Direito Penal Geral. Mais especificamente as cifras negras e cinzas chamam mais atenção.

7.1. CIFRAS NEGRAS E CINZAS

As cifras negras são tidas como a categoria originária das cifras, relacionando-se àqueles crimes que não chegam ao conhecimento do Estado ou que chegando à esfera de conhecimento das autoridades, não conduzem a um processo, gerando impunidade.

As cifras cinzas nas situações em que as ocorrências são registradas, porém, não há o encerramento conclusivo da persecução penal, normalmente por razões de ordem administrativa ou jurídica. Um exemplo é quando o atraso nas investigações acarreta a prescrição ou mesmo a ausência da representação da vítima.

Diante do cenário que encontra-se o sistema de justiça brasileiro, o qual envolve, por exemplo os órgãos policiais, ministério Público e Judiciário, esses órgãos estão cada vez mais ineficientes no combate aos crimes cibernéticos, contribuindo cada vez para o aumento das cifras negras e cinzas que dentro da criminologia são considerados indicadores de ineficiências, pois são crimes que não são solucionados e a sociedade não obtém uma resposta por parte do poder público, desse modo banalizando ainda mais a ocorrência de crimes cibernéticos já que a impunidade se traduz como premiação para praticar ou continuar praticando esses delitos.

8. SUCATEAMENTO DAS POLÍCIAS

A estrutura policial historicamente específica passou por enormes dificuldades estruturais tanto de pessoal, material, financeira e tecnológica, fazendo com que sempre esteja um passo atrás dos criminosos, e no que diz respeito no combate aos crimes cibernéticos essa defasagem se torna ainda mais evidente, pois trata-se de uma atuação mais especializada e específica, envolvendo mecanismos tecnológicos de alto custo e mão de obra especializada, ou seja policias mais bem preparados e com formação específica em análise de sistema e programação, o que não é uma realidade dentro das delegacias brasileiras, onde falta até mesmo a mão de obra trivial para atividade policial.

Um grupo de pesquisadores, publicou um estudo, na Revista Ibero-Americana de Humanidades, *Ciências e Educação, referente Segurança Pública, Racionalidade Criminal e Inércia Institucional*. A pesquisa estabelece uma relação entre a inércia estatal e a coexistência desigual de diferentes ordens normativas, evidenciando que essa dinâmica contribui para o fortalecimento e a expansão da criminalidade.

Corroborando essa perspectiva, o sistema de justiça brasileiro possui raízes históricas profundas e mantém estreita articulação com o campo político. Nesse contexto, a dimensão da prevenção social da violência está diretamente relacionada às políticas públicas de caráter social, que constituem um dos principais instrumentos estatais para a promoção do bem-estar coletivo. Autores como Boaventura de Sousa Santos (1997) e Michel Misse (2010) demonstram que a informalidade de determinadas práticas policiais, a seletividade penal e a crescente descrença no sistema de justiça refletem um cenário de pluralismo jurídico, no qual diferentes ordens normativas coexistem de maneira desigual. Essa configuração contribui para a perpetuação da impunidade e para o aprofundamento das desigualdades sociais,

evidenciando disfunções estruturais que caracterizam a inércia institucional e favorecem a reprodução da violência, além de comprometerem a efetividade das políticas públicas.

Diante desse panorama, o governo federal esboçou uma reação e em abril, de 2025, enviou a Proposta de Emenda à Constituição. (PEC) da Segurança Pública. (PEC 18/2025) a fim de reformular o Sistema de Segurança Pública, que até o atual momento encontra-se em tramitação. A PEC propõe a reestruturação do sistema de Segurança Pública, criando fontes de financiamento, a PEC busca injetar mais dinheiro no sistema de segurança, criando repasses obrigatório da união para os estados. A proposta prevê o repasse de 30% da arrecadação com as “Bets”, “as apostas online”, vai gerar uma contribuição importante para o sistema de segurança. Em matéria publicada no portal exame, especialistas analisaram a proposta de emenda constitucional e segundo os mesmos a proposta pode trazer muitos benefícios ao sistema, como foi explicitado na matéria:

De acordo com o governo, a PEC da Segurança visa reforçar o papel da União, reorganizar e fortalecer o sistema nacional de segurança, estruturar mecanismos de coordenação e integração e enfrentar de forma mais eficaz o crime organizado, cuja atuação tem se expandido territorial e economicamente no país.

A PEC também busca constitucionalizar fundos essenciais, como o Fundo Nacional de segurança Pública nacional (FNSP) e o fundo penitenciário nacional (FUNPEN), impedindo o contingenciamento de seus recursos. (EXAME, 2025.)

Em entrevista recente ao espaço democrático, o sociólogo, Tulio Kahn, onde ele defende esse repasse de verbas aos estados a fim de criar um incentivo ao cumprimento de metas estabelecidas pelo Governo Federal, transformando-se em uma ferramenta importante ao combate aos crimes no Brasil. Vejamos:

Entre outros pontos, a PEC propõe constitucionalizar o SUSP e os fundos unificados de Segurança e Penitenciário, medida que pode garantir maior segurança institucional a estas regras, evitando que sejam extintos em futuras gestões. Mas a unificação dos fundos nacionais (o FUNAD ficou de fora da PEC) poderia ter sido acompanhada de um incremento considerável no montante, apontando, claro, de onde viriam os recursos, sempre escassos. O problema principal dos fundos nacionais não é contingenciamento de recursos, mas o seu volume insignificante, além da falta de bons projetos.

Assim, estes fundos nacionais robustos seriam a cenoura para que os Estados seguissem as diretrizes nacionais, em vez de propor a obrigatoriedade para os Estados (Espaço Democrático.)

Outro ponto de suma relevância tratado na Proposta de Emenda à Constituição. (PEC) da Segurança Pública. (PEC 18/2025). Diz respeito a ampliação da atuação da Polícia Federal, ampliando a sua atuação frente as organizações criminosas com atuação transnacional. Em matéria publicada no jornal o globo em 04/03/2026, a jornalista

Luísa Marzullo, defende essa atuação mais ampla e coordenada da Polícia Federal.

O texto da Proposta De Emenda Constitucional. (PEC). reforça a competência da Polícia Federal para investigar crimes que ultrapassem fronteiras estaduais ou tenham repercussão internacional. A mudança tem como foco especialmente as organizações criminosas e milícias que operam em diferentes regiões do país e utilizam estruturas transnacionais para tráfico de drogas, armas e lavagem de dinheiro. A intenção é permitir uma atuação federal mais coordenada nesses casos, sem depender exclusivamente das polícias estaduais.

Diante do cenário atual, enquanto a PEC da Segurança Pública não é aprovada, fica evidente que a atuação das Polícias e dos outros integrantes do sistema de justiça brasileiro vem demonstrando-se pouco eficiente. Gerando na população uma corrosão da credibilidade institucional, não conseguindo acreditar que a polícia vá solucionar seu problema, dessa forma há uma perda de credibilidade e as pessoas são desestimuladas a procurar às delegacias de polícia para registrar suas ocorrências.

No meio digital a situação é ainda mais sensível pois, a própria natureza dos crimes ali praticados, que na maioria das vezes envolve situações vexatórias e constrangedoras, como por exemplo, os crimes de discurso de ódio, crimes contra a dignidade sexual. Além desses crimes os crimes contra o patrimônio, tendo maior incidência o estelionato digital, onde as vítimas são ludibriadas através da engenharia social a cair em golpes, causando-lhes um constrangimento enorme, as vítimas além de sofrerem as consequências do crime ainda são acometidas pela baixa eficiência da polícia no solucionamento do seu problema e dessa forma o desestímulo cresce fazendo com que as pessoas não procure às delegacias de polícia contribuindo assim para o aumento do número das cifras negra e cinza.

Em reunião recente entre a Febraban (Federação Brasileira de Bancos) apresentou à PF (Polícia Federal) relatório sobre os prejuízos decorrente dos crimes cibernéticos, os prejuízos são estratosféricos, apenas entre os anos de 2023 e 2024 o prejuízo sofrido pelas instituições bancárias o valor totalizou R\$ 4,5 bilhões apenas

envolvendo fraudes relacionadas ao Pix, nesse mesmo período, catalogando todas as fraudes cibernéticas o valor ultrapassa R\$ 18,7 bilhões de reais. Uma matéria publicada no portal CNN em outubro de 2024, trouxe relatórios de especialista da área de prevenção aos crimes cibernéticos, afirmando ser o Brasil o vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo.

Uma das pesquisadoras, Chelsea Jarvie, alerta sobre o panorama atual do Brasil e dos riscos inerentes ao meio digital, mostrando a necessidade de treinamento e conscientização da população.

O Brasil carrega o título (não tão agradável) de segundo país com mais ataques cibernéticos no mundo. Em um período de 12 meses, foram registrados mais de 700 milhões de ataques cibernéticos no país, totalizando 1.379 por minuto, segundo Panorama de Ameaças para a América Latina 2024. E o que tem representado um desafio para a segurança cibernética é a própria tecnologia. Chelsea Jarvie, escocesa que é especialista em cibersegurança, alerta para a sofisticação dos ataques, promovida principalmente pela evolução da inteligência artificial "As tecnologias são essenciais, mas a resiliência cibernética depende tanto das pessoas, quanto da cultura. O foco excessivo em tecnologia pode acabar negligenciando a capacitação e a conscientização dos colaboradores", argumenta Jarvie. (NAKAMURA, 2024).

É importante a implementação de processos e campanhas que integrem a segurança na vida cotidiana dos funcionários, a adoção de treinamento psicológico que os ajude a entender os objetivos dos atacantes e como evitar cair em tantas armadilhas", conclui a especialista. (Jarvie, 2024).

O esforço deve ser conjunto entre instituições bancárias e poder público com o objetivo de trocar informações relevantes para dar mais efetividade às ações da Polícia e Ministério Público, mas apenas isso não basta é muito relevante que a população também esteja alerta sobre os riscos do meio digital.

Em 2024 o senado federal através do O DataSenado apurou o percentual de brasileiros que foram vítimas de algum crime cibernético no Brasil, a pesquisa chegou aos impressionantes números: 24% dos brasileiros com mais de 16 anos, foram vítimas de algum golpe digital nos últimos 12 meses. São mais de 40,85 milhões de pessoas que perderam dinheiro em função de algum crime cibernético, como clonagem de cartão, fraude na internet ou invasão de contas bancárias.

CONCLUSÃO

Este trabalho buscou analisar o cenário dos crimes cibernéticos e sua difusão nas redes sociais no Brasil, cruzando dados oficiais, tendo como referencial a mancha

criminal e a correlação entre impunidade e o fomento dos crimes cibernéticos. Foram analisados os impactos da falta de estrutura policial, ineficiência e morosidade das investigações e suas implicações nas cifras negras e cinzas. Foram traçadas possíveis soluções a curto e médio e longo prazo, referenciando-se na teoria das janelas quebradas e na política criminal da tolerância zero.

As políticas públicas devem ser voltadas para o combate os crimes cibernéticos no seu contexto multifatorial pautadas no fomento à educação digital e diminuição das desigualdades sociais.

O objetivo do trabalho foi preparar um panorama realístico dos cibercrimes, mas acima de tudo contribuir para formação de um ambiente digital seguro e humano, onde o crime não seja vantajoso econômica e socialmente, mas que a resposta estatal seja célere e eficiente, formando assim, um instrumento de dissuasão mais eficaz que a dureza das penas que são criadas no contexto de clamores sociais momentâneos, resultando em leis simbólicas sem eficiência. O que leva a erosão da confiança estatal e consequentemente as subnotificações criminais e o alargamento das cifras negras e cinza, criando cada vez mais desordem e caos social. Parafraseando o eminente jurista baiano Ruy Barbosa, na sua obra *Oração dos moços*: “*Justiça atrasada não é justiça, senão injustiça qualificada e manifesta.*”

REFERÊNCIAS

- SILVA, Vitória Beatriz do Bomfim. *Os desafios no combate aos crimes cibernéticos com enfoque nas redes sociais*. 2025. Projeto de Pesquisa – Centro Universitário UNIDOMPEDRO Afya, Barreiras, BA, 2025.
- BAHIA. Secretaria da Segurança Pública. ***O NCGEO***. Salvador: SSP/BA, [20--]. Disponível em: <https://www.ba.gov.br>. Acesso em: 29 maio 2026.
- BARBOSA, Rui. ***Oração aos moços***. Organização de Adriano da Gama Kury. 5. ed. Rio de Janeiro: Casa de Rui Barbosa, 1999.
- BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: Planalto – Marco Civil da Internet. Acesso em: 30 set. 2025.
- CÂMARA aprova PEC da Segurança; texto será analisado pelo Senado. ***Senado Notícias***, Brasília, DF, 5 mar. 2026. Disponível em: <https://www12.senado.leg.br>. Acesso em: 29 maio 2026.
- CUNHA, Rogério Sanches. *Manual de direito penal: parte especial (arts. 121 a 361) – volume único*. 18. ed. rev., atual. e ampl. São Paulo: JusPodivm, 2025.
- GRECO, Rogério. *Curso de direito penal: artigos 121 a 212 do Código Penal*. 22. ed. rev. e atual. São Paulo: Atlas, 2022. v. 2.
- DEFEITOS e virtudes da PEC da Segurança Pública. ***Espaço Democrático***, [s. l.], [2026?]. Disponível em: <https://espacodemocratico.org.br>. Acesso em: 29 maio 2026.
- ESPAÇO DEMOCRÁTICO. debate a expansão do crime organizado para a economia formal. Notícias, 3 set. 2025. Disponível em: <https://espacodemocratico.org.br/noticias/espaco-democratico-debate-a-expansao-do-crime-organizado-para-a-economia-formal/>. Acesso em: 23 nov. 2025.
- KASPERSKY. *Panorama de ameaças para a América Latina 2024*. São Paulo: Kaspersky Lab, 2024. Disponível em: <https://www.kaspersky.com.br>. Acesso em: 9 abr. 2026.
- LIMA JÚNIOR, José César Naves de. ***Manual de criminologia***. 4. ed. rev., ampl. e atual. Salvador: Juspodivm, 2017.
- MASSON, Cleber. *Direito penal: parte especial (arts. 121 a 212)*. v. 2. 17. ed. rev., atual. e ampl. São Paulo: Método, 2024.
- MONARD, Maria Carolina; BARANAUSKAS, Maria Cecília Calani. Aprendizado de máquina. In: REZENDE, Solange Oliveira (org.). *Sistemas inteligentes: fundamentos e aplicações*. Barueri: Manole, 2003. p. 89-114.

MARZULLO, Luísa. Entenda os principais pontos da PEC da Segurança, que deve ser votada nesta quarta. ***O Globo***, Brasília, DF, 4 mar. 2026. Política. Disponível em: <https://oglobo.globo.com/politica/noticia/2026/03/04/entenda-os-principais-pontos-da-pec-da-seguranca-que-deve-ser-votada-nsta-quarta.ghtml>. Acesso em: 29 maio 2026.

NAKAMURA, João. Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo. CNN Brasil, São Paulo, 30 out. 2024. Economia. Disponível em: <https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/>. Acesso em: 23 nov. 2025.

SENADO FEDERAL. Golpes digitais atingem 24% da população brasileira, revela DataSenado. *Agência Senado*, Brasília, DF, 1 out. 2024. Disponível em: Agência Senado – Golpes digitais atingem 24% da população brasileira. Acesso em: 4 nov. 2025.

SILVA, Willian Wallace de Matteus. *A evolução da criptografia e suas técnicas ao longo da história*. 2016. 41 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Instituto Federal de Educação, Ciência e Tecnologia Goiano, Urutaí, 2016.

PEC da Segurança Pública: especialistas divergem sobre eficácia da proposta. ***Exame***, [s. l.], 2026. Disponível em: <https://exame.com>. Acesso em: 29 maio 2026.

PICANÇO, Luhan Ammy Andrade et al. Segurança pública, racionalidade criminal e inércia institucional: uma análise multidimensional do crime urbano no Brasil. ***Revista Ibero-Americana de Humanidades, Ciências e Educação***, [s. l.], v. 12, n. 3, p. 1-16, mar. 2026. DOI: <https://doi.org/10.51891/rease.v12i3.24772>. Disponível em: <https://periodicorease.pro.br/rease/article/view/24772>. Acesso em: 29 maio 2026.

WILSON, James Q.; KELLING, George L. Broken windows: the police and neighborhood safety. *The Atlantic Monthly*, Boston, v. 249, n. 3, p. 29-38, mar. 1982.