doi.org/10.51891/rease.v9i10.11580

CRIMES CIBERNÉTICOS

CYBER CRIMES

CRÍMENES CIBERNÉTICOS

Karolline Barbosa Maia[1]
Cezar Henrique Ferreira Costa[2]

RESUMO: O presente artigo analisa a evolução histórica dos crimes cibernéticos, desde suas origens até os desafios contemporâneos, abordando a legislação aplicável e a crucial importância do poder público na prevenção e punição desses delitos. Os crimes cibernéticos, ao longo de décadas, passaram de incidentes isolados para uma ameaça global, acompanhando o crescimento da Internet e da tecnologia. Investigamos como esses crimes se transformaram de atos de curiosidade tecnológica em empreendimentos criminosos altamente lucrativos, explorando as motivações e métodos por trás dessa evolução. No que diz respeito à legislação, exploramos como os governos têm buscado se adaptar a essa realidade em constante mutação. Analisamos a criação e o desenvolvimento de leis e tratados internacionais destinados a combater crimes cibernéticos, destacando a necessidade de uma abordagem transnacional para enfrentar uma ameaça que transcende fronteiras. O papel do poder público é crucial na prevenção e punição de crimes cibernéticos. Discutimos como as agências de aplicação da lei, departamentos de segurança cibernética e organismos internacionais desempenham um papel vital na identificação, investigação e responsabilização dos perpetradores. Além disso, destacamos a importância da colaboração entre o setor público e privado para fortalecer a segurança cibernética e promover a troca de informações. Conclui-se que devido a rápida evolução da tecnologia, a batalha contra os crimes cibernéticos é uma tarefa contínua que requer uma legislação dinâmica e ação coordenada entre os governos e as empresas. A segurança cibernética não é apenas uma preocupação técnica, mas uma questão de segurança nacional e bem-estar público, e é essencial que o poder público desempenhe um papel proativo na proteção dos cidadãos e organizações contra essa ameaça em constante evolução.

Palavras-chave: Crimes Cibernéticos. Internet. Inovações Tecnológicas.

[1] Graduanda em Direito pela Universidade de Gurupi-UNIRG.
[2] Pós-Graduado em Direito Público. Direito Processual Civil. Gestão Pública e Mestrando em Direito pela Universidade Must University.

ABSTRACT: This article analyzes the historical evolution of cybercrimes, from its origins to contemporary challenges, addressing the applicable legislation and the crucial importance of public authorities in preventing and punishing these crimes. Cybercrimes, over the decades, have gone from isolated incidents to a global threat, following the growth of the Internet and technology. We investigate how these crimes transformed from acts of technological curiosity into highly profitable criminal enterprises, exploring the motivations and methods behind this evolution. With regard to legislation, we explore how governments have sought to adapt to this constantly changing reality. We analyze the creation and development of international laws and treaties aimed at combating cybercrime, highlighting the need for a transnational approach to confront a threat that transcends borders. The role of public authorities is crucial in preventing and punishing cybercrimes. We discuss how law enforcement agencies, cybersecurity departments, and international bodies play a vital role in identifying, investigating, and holding perpetrators accountable. Furthermore, we highlight the importance of collaboration between the public and private sector to strengthen cybersecurity and promote the exchange of information. It is concluded that due to the rapid evolution of technology, the battle against cybercrime is an ongoing task that requires dynamic legislation and coordinated action between governments and companies. Cybersecurity is not just a technical concern, but a matter of national security and public well-being, and it is essential that public authorities play a proactive role in protecting citizens and organizations against this constantly evolving threat.

Keywords: Cybercrimes. Internet. Technological Innovations.

RESUMEN: Este artículo analiza la evolución histórica de los ciberdelitos, desde sus orígenes hasta los desafíos contemporáneos, abordando la legislación aplicable y la importancia crucial de los poderes públicos en la prevención y sanción de estos delitos. Los delitos cibernéticos, a lo largo de las décadas, han pasado de incidentes aislados a una amenaza global, tras el crecimiento de Internet y la tecnología. Investigamos cómo estos delitos pasaron de ser actos de curiosidad tecnológica a empresas criminales altamente rentables, explorando las motivaciones y métodos detrás de esta evolución. Con respecto a la legislación, exploramos cómo los gobiernos han buscado adaptarse a esta realidad en constante cambio. Analizamos la creación y desarrollo de leyes y tratados internacionales destinados a combatir el cibercrimen, destacando la necesidad de un enfoque transnacional para enfrentar una amenaza que trasciende las fronteras. El papel de las autoridades públicas es crucial para prevenir y castigar los delitos cibernéticos. Discutimos cómo las agencias encargadas de hacer cumplir la ley, los departamentos de ciberseguridad y los organismos internacionales desempeñan un papel vital en la identificación, investigación y responsabilización de los perpetradores. Además, destacamos la importancia de la colaboración entre el sector público y privado para fortalecer la ciberseguridad y promover el intercambio de información. Se concluye que debido a la rápida evolución de la tecnología, la batalla contra el cibercrimen es una tarea constante que requiere legislación dinámica y acción coordinada entre gobiernos y empresas. La ciberseguridad no es sólo una preocupación técnica, sino una cuestión de seguridad nacional y bienestar público, y es esencial que las autoridades públicas desempeñen un papel proactivo en la protección de los ciudadanos y las organizaciones contra esta amenaza en constante evolución.

Palabras clave: Ciberdelitos. Internet. Innovaciones tecnológicas.

1. INTRODUÇÃO

Os crimes cibernéticos representam uma ameaça crescente e onipresente no cenário global da atualidade. Com o avanço da tecnologia e a proliferação da internet, a prática de delitos virtuais evoluiu de forma substancial, moldando o cenário da segurança digital e desafiando a capacidade dos governos em todo o mundo de controlar e reprimir essas atividades ilícitas. Neste contexto, este artigo busca traçar um panorama abrangente da evolução histórica dos crimes cibernéticos, desde suas origens até a contemporaneidade, com foco especial na legislação brasileira aplicável e na relevância do poder público na prevenção e punição desses crimes.

O cenário da cibercriminalidade vem sofrendo uma metamorfose constante nas últimas décadas, à medida que o mundo se torna cada vez mais interconectado e dependente da tecnologia. Os crimes cibernéticos representam um desafio multifacetado, que transcende fronteiras e afeta indivíduos, organizações e governos.

A história dos crimes cibernéticos remonta aos primórdios da computação, quando as ações maliciosas eram frequentemente movidas pela curiosidade e desafio técnico. No entanto, à medida que a tecnologia evoluiu, também evoluíram as motivações por trás desses atos, que passaram a incluir o enriquecimento ilícito, o ciberterrorismo, a espionagem e outros atos maliciosos que afetam a segurança nacional e a privacidade dos cidadãos. Portanto, é imperativo compreender a evolução desse fenômeno para estabelecer medidas eficazes de combate.

A legislação brasileira relativa aos crimes cibernéticos passou por um processo de aprimoramento ao longo do tempo. Desde a promulgação da Lei nº 9.296/1996, que regulamentou a interceptação de comunicações telefônicas, até a mais recente Lei nº 14.155/2021, que tipifica o crime de furto mediante fraude eletrônica, o Brasil tem buscado adaptar seu arcabouço legal para abordar as complexas questões inerentes à cibercriminalidade. No entanto, a legislação deve continuar a evoluir para enfrentar os desafios emergentes.

O poder público desempenha um papel central na prevenção e punição de crimes cibernéticos. As forças de segurança, os órgãos de inteligência e as agências especializadas desempenham um papel crucial na identificação e investigação de criminosos cibernéticos, bem como na colaboração com entidades internacionais para combater ameaças

transnacionais. Além disso, o governo tem a responsabilidade de promover a conscientização pública, fornecer recursos para a segurança cibernética e estabelecer políticas que incentivem a adoção de boas práticas.

Assim, este artigo visa não apenas analisar a evolução dos crimes cibernéticos e da legislação no Brasil, mas também enfatizar a necessidade de uma abordagem abrangente, na qual o poder público desempenhe um papel proativo na proteção da sociedade contra ameaças digitais. A segurança cibernética é uma preocupação que atravessa fronteiras e exige esforços conjuntos para proteger a integridade das informações, a privacidade e a estabilidade das infraestruturas críticas em nosso mundo cada vez mais digitalizado.

2. CRIMES CIBERNÉTICOS

Os crimes cibernéticos, são crimes cometidos no ambiente digital, utilizando a tecnologia de informação como ferramenta principal para perpetrar atos ilegais. Esses crimes envolvem uma ampla gama de atividades específicas que vão desde ataques direcionados a sistemas de computadores até a exploração de vulnerabilidades online com objetivos financeiros, políticos ou pessoais.

Os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento (WENDT; JORGE, 2012).

Os autores destes crimes utilizam dos computadores, notebooks, celulares, dentre outros dispositivos que podem ser conectados à rede, para a prática de crimes. Atualmente, estes crimes tem se desenvolvido de forma crescente e gradual.

Os crimes cibernéticos, geralmente, ocorrem por motivos relacionados ao lucro, ou seja, com a finalidade de obterem resultado monetário. No entanto, tais crimes, podem causar danos psicológicos de difícil reparação para às vítimas. Dentre os crimes cibernéticos mais comuns podemos apontar o hacking e invasão de sistemas, phishing, o ransomware, as fraudes financeiras, a disseminação de malware, e o assédio cibernético.

O crime cibernético de hacking e invasão de sistemas é uma prática em que indivíduos ou grupos mal-intencionados buscam acessar redes, sistemas de computadores ou dispositivos eletrônicos sem a devida autorização. Eles utilizam técnicas e vulnerabilidades para contornar medidas de segurança e obter acesso não autorizado a

informações eventuais, causando danos substanciais. Esses variam desde a busca por dados confidenciais, como informações financeiras ou segredos comerciais, até o comprometimento de sistemas para fins de espionagem ou sabotagem. O hacking é um crime cibernético com implicações graves, que frequentemente exige medidas de segurança avançadas e uma ação rápida para detectar e mitigar os riscos associados a essa prática.

É um ato ilícito que envolve uma invasão não autorizada de sistemas de computadores, redes ou dispositivos. Os hackers utilizam suas habilidades técnicas para roubar medidas de segurança e acessar informações confidenciais, muitas vezes com desejo de lucro, espionagem, ou simplesmente para demonstrar sua destreza técnica.

Esse tipo de atividade criminosa representa uma ameaça séria tanto para indivíduos quanto para organizações, uma vez que pode resultar em perda de dados confidenciais, violação de privacidade e danos financeiros significativos. A prevenção e a proteção contra essas invasões desabilitam a implementação de medidas robustas de segurança cibernética e uma compreensão aprofundada das técnicas e técnicas utilizadas pelos hackers. Além disso, a legislação em muitos países, incluindo o Brasil, criminaliza essas atividades, estabelecendo punições para os responsáveis por tais invasões não autorizadas.

No mesmo sentido, o crime cibernético denominado phishing é uma tática enganosa amplamente utilizada por criminosos online. O phishing envolve o envio de mensagens fraudulentas, muitas vezes por e-mail, que se disfarçam como comunicações legítimas de instituições, empresas ou serviços confidenciais. O objetivo principal é enganar o destinatário e levá-lo a revelar informações pessoais, como números de cartão de crédito ou dados financeiros. Os cibercriminosos frequentemente passam por bancos, empresas de tecnologia ou órgãos governamentais, explorando a confiança das vítimas.

O phishing é uma ameaça insidiosa que pode resultar em roubo de identidade, fraudes financeiras e visíveis de privacidade, tornando crucial para que os usuários tenham consciência das táticas e adotem medidas de precaução para se protegerem contra esse tipo de golpe. Além disso, a legislação em muitos países permite o phishing como um crime, com punições para os perpetradores.

Já o crime de ransomware é uma ameaça virtual cada vez mais preocupante. Trata-se de um tipo de malware que criptografa os arquivos de uma vítima, tornando-os inacessíveis, e, em seguida, exige um resgate em dinheiro para desbloquear os dados. Esses

ataques podem causar prejuízos a indivíduos e organizações, já que a vítima é confrontada com uma escolha difícil, entre pagar o resgate aos criminosos ou arriscar a perda permanente de dados importantes.

O ransomware tem sido amplamente utilizado com fins lucrativos, tornando-se uma das principais ameaças cibernéticas. A prevenção desse tipo de crime cibernético envolve a adoção de práticas de segurança rigorosas, como a realização de backups regulares e a educação dos usuários sobre os perigos do ransomware. Além disso, as autoridades em muitos países consideram a prática do ransomware ilegal e trabalham para identificar e processar os responsáveis por esses ataques.

No mesmo contexto, os crimes cibernéticos que envolvem fraudes financeiras e a propagação de malware representam uma ameaça substancial à segurança digital. As fraudes financeiras abrangem uma ampla gama de atividades, desde clonagem de cartões de crédito até esquemas de phishing que visam obter informações financeiras pessoais. Essas práticas ilegais frequentemente resultam em perda de dinheiro para as vítimas e podem ter implicações a longo prazo.

Por outro lado, a propagação de malware envolve uma propagação de software malicioso que pode infectar dispositivos e sistemas, permitindo que os criminosos acessem informações prejudiciais ou causem danos.

A prevenção desses tipos de crimes cibernéticos requer uma combinação de medidas de segurança, como o uso de software atualizado, a vigilância de atividades financeiras suspeitas e a educação dos usuários para identificar ameaças. Além disso, as autoridades em todo o mundo têm trabalhado para rastrear e processar os indivíduos envolvidos nesses tipos de crimes, buscando a justiça e a proteção dos cidadãos e das empresas contra essas ameaças.

E por último, o crime de assédio cibernético é uma forma de violência digital que se manifesta por meio de mensagens ameaçadoras, difamatórias, experimentais ou constrangedoras direcionadas a indivíduos, muitas vezes de forma repetitiva. O assédio cibernético, também chamado de cyberbullying, ocorre em plataformas online, redes sociais, mensagens eletrônicas e outras formas de comunicação digital, tornando-se uma ameaça significativa, principalmente para jovens e adolescentes. As vítimas de assédio

cibernético enfrentam frequentemente sérios impactos emocionais, sociais e psicológicos, incluindo ansiedade, depressão e isolamento.

A prevenção e o combate a esse tipo de crime cibernético exigem um esforço conjunto da sociedade, das escolas, das autoridades e das plataformas online para promover a conscientização, educar sobre o comportamento online responsável e tomar medidas legais quando necessário, a fim de garantir a segurança e o bem-estar das vítimas.

3. EVOLUÇÃO HISTÓRICA DOS CRIMES CIBERNÉTICOS

Os primeiros ataques cibernéticos representam os primeiros passos de uma era digital que se desdobraria em uma paisagem virtual complexa e, por vezes, perigosa. Na década de 1970, à medida que os sistemas de computadores se interligaram, as primeiras declarações de ataques cibernéticos emergiram. No entanto, é importante destacar que, nessa época, os motivos foram muitas vezes movidos pela curiosidade e desafio técnico, em vez de objetivos financeiros ou políticos, como são comuns atualmente.

Neste contexto, o crime cibernético não é algo pertinente apenas na atualidade, pois desde os tempos arcaicos, cujo, o meio tecnológico era algo mais longínquo e inacessível para a maioria dos cidadãos. É necessário compreender que estes crimes começaram a ser praticados ainda na década de 1960, nos Estados Unidos da América.

Os primeiros crimes digitais, em sua grande maioria, eram praticados por especialistas que utilizavam de sua inteligência para arquitetar planos relacionados a aplicar golpes em instituições financeiras. A Câmara dos Deputados se dispôs a explicar o início dessa dramaturgia existente no meio tecnológico. Segundo a Câmara dos Deputados:

> *"Na época, começaram a aparecer na imprensa e na literatura científica norte-americana os primeiros casos de uso de computadores para cometer delitos como sabotagens e espionagem. Somente na década seguinte, foram iniciados estudos sistemáticos e científicos sobre o tema. A partir de 1980, as ações criminosas intensificaram-se, envolvendo principalmente manipulação de dados bancários, pirataria de programas de computador, abusos nas telecomunicações e pornografia infantil".*

Os primeiros ataques foram frequentemente realizados por entusiastas da computação, que procuravam explorar as possibilidades dos sistemas recém-conectados. Entre os primeiros incidentes noticiados está o caso do Wabbit, um programa autorreplicante que se inclui de sistema para sistema, não com interesse malicioso, mas para demonstrar a capacidade de replicação de código.

O surgimento de redes de computadores, como a ARPANET (predecessora da internet moderna), possibilitou novos tipos de ataques, como o Morris Worm em 1988, que se envolveu inadvertidamente e causou interrupções na rede.

O que torna esses ataques notáveis é a ausência de motivações financeiras ou políticas. Eles eram, em grande parte, uma expressão da curiosidade inerente aos pioneiros da computação. No entanto, à medida que a tecnologia avançada e a internet se tornaram onipresentes, os motivos e métodos por trás dos ataques cibernéticos evoluíram significativamente.

Os primeiros ataques cibernéticos representam o início de uma trajetória que levaria a uma compreensão mais profunda dos sistemas digitais, mas também à necessidade de segurança cibernética robusta para proteger sistemas e informações sensíveis em um mundo cada vez mais interconectado.

A evolução desses ataques ao longo das décadas seguintes demonstra como a tecnologia e a motivação por trás dos crimes cibernéticos se tornaram mais sofisticadas e, por vezes, mais tecnológicas, tornando a segurança cibernética uma prioridade crucial nos dias de hoje.

Dessa forma, é notório entender que os crimes cibernéticos estão no meio social a algumas décadas. Tanto no meio internacional quanto no nacional. Alguns casos marcaram a história dos crimes cibernéticos, no início de suas práticas.

À medida que a tecnologia avançou e a sociedade se tornou cada vez mais dependente da internet, as motivações por trás dos crimes cibernéticos evoluíram consideravelmente. O que antes era um terreno de exploradores digitais e curiosos técnicos se transformou em um campo de atuação para criminosos com uma ampla gama de objetivos. Dentre as principais motivações emergentes de crimes cibernéticos, destacamos as financeiras, políticas, a espionagem cibernética, motivações ideológicas e hacktivismo e o entretenimento e reconhecimento.

Umas das principais motivações para os crimes cibernéticos é o ganho financeiro. Criminosos cibernéticos agora veem na internet como uma oportunidade de obter lucros substanciais. Isso inclui a realização de fraudes financeiras, como a clonagem de cartões de crédito, a extorsão por meio de ransomware e esquemas de phishing destinados a roubar informações financeiras de vítimas desavisadas.

Um dos casos internacionais que mais marcaram a história dos crimes cibernéticos, em sua fase inicial, foi o caso Equity Founding Life INsurance Company, em Los Angeles. Este caso configurou-se em uma das maiores fraudes de computadores já mencionada, esta situação se caracterizou por ter chegado à marca de 2 bilhões de reais.

Dessa forma, é notório entender que os crimes cibernéticos estão no meio social a algumas décadas. Tanto no meio internacional quanto no nacional. Alguns casos marcaram a história dos crimes cibernéticos, no início de suas práticas.

Mas além de finalidade monetária, o crime cibernético pode interferir, também, no psicológico das vítimas. Os criminosos utilizam o meio tecnológico para instigar ou coagir suas vítimas a realizarem atos catastróficos. Um dos casos que marcou o Estado brasileiro em relação a esta temática, foi o caso da "Baleia azul".

Este não foi o primeiro caso relacionado a crimes cibernéticos envolvendo o psicológico, principalmente dos jovens. De acordo com a revista "El País":

> O jogo, entretanto, não é um fenômeno novo de Facebook, que tem equipes 24 horas ativas para remover esse tipo de conteúdo, nem dos milennials, ou muito menos do século XXI. Já nos anos 90, muito antes da rede social existir e quando os computadores ainda eram um engendro tecnológico quase desconhecido, os grupos que induziam ao suicídio preocupavam as autoridades. "Nessa época, tive notícia, através de uma mãe desesperada, que seu filho adolescente havia se jogado da cobertura do seu prédio na Barra da Tijuca [zona oeste do Rio] por orientação criminosa de um site", relembra o promotor Romero Lyra, que chefiou a Promotoria de Investigação de Crimes Eletrônicos no Rio, a primeira a combater a criminalidade cibernética no Brasil e na América do Sul. "A página oferecia vantagens, superpoderes e contatos com a divindade para os jovens que aceitassem participar de competições radicais", completa Lyra. "O problema é muito complexo, e não é de hoje".

O jogo da "Baleia Azul", instigava os jovens, de forma virtual, a participar de fases que ao final delas, levava ao suicídio do participante. O que alarmou os agentes voltados a analisar a criminalidade cibernética no Brasil.

Os ataques cibernéticos também são frequentemente motivados por objetivos políticos. Grupos hacktivistas e governos muitas vezes realizam ciberataques para obter informações estratégicas, espionagem industrial, influenciar eleições ou promover suas agendas políticas. Esses ataques podem causar instabilidade em escalas nacionais e internacionais.

Neste cenário, a busca por informações úteis tornou-se uma motivação central para os ciberataques. A espionagem cibernética é realizada por governos, grupos de hackers e empresas interessadas em adquirir dados confidenciais, como segredos comerciais, propriedade intelectual e informações de defesa.

Assim, os grupos de hacktivistas, muitas vezes motivados por causas ideológicas, usam a internet para promover suas agendas políticas, sociais ou ambientais. Isso pode incluir a divulgação de informações sensíveis ou ataques de negação de serviço para interrupção de serviços online.

Noutro giro, alguns crimes cibernéticos são realizados em formas de ataques a sistemas por pura diversão ou para alcançar reconhecimento dentro da comunidade de hackers. Isso pode resultar em atos de vandalismo digital, como invasões de sites, sem motivações financeiras ou políticas claras.

Essas motivações emergentes demonstram a complexidade e a diversidade do cenário de crimes cibernéticos atuais. À medida que a tecnologia continua a evoluir, é essencial que a sociedade, governos e empresas adotem medidas para proteger sistemas e informações críticas, bem como para desenvolver estratégias que possam identificar e responsabilizar os autores de crimes cibernéticos. A prevenção e a proteção contra esses delitos requerem uma abordagem multidisciplinar, que envolve segurança cibernética, legislação atualizada e a cooperação internacional para enfrentar ameaças transnacionais.

4. LEGISLAÇÃO BRASILEIRA APLICÁVEL

O Brasil atualizou o Marco Civil da Internet (Lei 12.965/2014) como um marco legal que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. O Marco Civil regula a neutralidade da rede, a privacidade dos usuários e a responsabilidade dos provedores de serviços online.

Assim, o Marco Civil da Internet, representa um importante avanço na regulamentação da internet no Brasil. Promulgado em 23 de abril de 2014, ele distribui princípios, garantias, direitos e deveres para o uso da internet no país, consolidando um marco legal para a rede no contexto brasileiro.

Uma das características mais notáveis do Marco Civil da Internet é a proteção da neutralidade da rede. Isso significa que os provedores de internet devem tratar todos os dados de forma igual, sem discriminação de conteúdo, aplicativos ou serviços. A neutralidade da rede visa garantir a liberdade de expressão e o acesso igualitário à informação, impedindo que os provedores de internet privilegiem ou bloqueiem conteúdos de sua escolha. Além disso, o Marco Civil transmitiu direitos relacionados à privacidade

dos usuários. Ele exige que as empresas respeitem a privacidade dos dados pessoais dos usuários, recebendo sua autorização para a coleta e tratamento de informações. Isso é fundamental para proteger a privacidade e a segurança dos indivíduos online.

Outro aspecto crucial é a responsabilidade dos provedores de serviços online, que não podem ser responsabilizados pelo conteúdo gerado pelos usuários, a menos que não cumpram ordens judiciais específicas para a remoção desse conteúdo. Essa disposição visa proteger a liberdade de expressão e a inovação online.

O Marco Civil da Internet também define diretrizes para a atuação do Estado na promoção da inclusão digital, incentivando a universalização do acesso à internet e a promoção da infraestrutura de banda larga.

Além disso, a lei regulamenta a retenção de registros de conexão, permitindo que as autoridades tenham acesso a esses registros em casos específicos, como investigações criminais, mas estabelece limites claros para garantir a proteção da privacidade dos usuários.

O Marco Civil da Internet estabeleceu um equilíbrio importante entre a promoção da liberdade na Internet e a proteção dos direitos e interesses dos cidadãos e empresas. Ele se tornou um exemplo internacional de legislação progressista para a governança da internet, destacando a importância de princípios como a neutralidade da rede, a privacidade dos dados e a liberdade de expressão. No entanto, sua melhoria e adaptação contínua às mudanças tecnológicas e sociais são desafios contínuos à medida que a Internet continua a evoluir. O Marco Civil da Internet do Brasil é uma legislação fundamental que molda a relação dos cidadãos com a internet e serve como uma referência global para a regulação digital responsável.

O Código Penal Brasileiro (Decreto-Lei 2.848/1940) foi atualizado para incluir disposições específicas sobre crimes cibernéticos. Ele aborda questões como invasão de dispositivos, roubo de informações, acesso indevido a sistemas e divulgação não autorizada de dados.Os crimes cibernéticos, em sua diversidade, estão cada vez mais presentes na sociedade digital, e o Brasil não é uma exceção.

O Código Penal - CP, em vigor desde 1940, passou por diversas alterações para lidar com essa realidade emergente, criminalizando condutas relacionadas à esfera digital. Dentre os crimes cibernéticos reconhecidos em seu texto legal, destacamos a invasão de

dispositivos (artigo 154-a), falsificação de documentos eletrônicos (artigo 298), o estelionato eletrônico (artigo 171, § 2º), a divulgação de segredos (artigo 153), calúnia, difamação e injúria eletrônica (artigos 138, 139 e 140).

O artigo 154-A do CP pune a invasão de dispositivos, como computadores, smartphones ou redes, quando não autorizada, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. A pena pode variar de 1 (um) a 4 (quatro) anos de reclusão, além de multa. Essa lei é crucial para coibir ataques de hackers e a invasão de sistemas, evoluindo para a proteção da privacidade e segurança digital dos cidadãos.

O Código Penal também aborda a falsificação de documentos particulares que podem ser físicos ou eletrônicos, um crime que se tornou mais sofisticado com o avanço da tecnologia. O artigo 298 prevê pena de reclusão de 1 a 5 anos, além de multa, para aqueles que falsificarem documentos, selos ou marcas com o objetivo de obter vantagem indevida. O parágrafo único do referido artigo afirma que o equipara-se a documento particular o cartão de crédito ou débito.

A mesma lei penal pune também o estelionato eletrônico, crime que envolve a obtenção de vantagem ilícita por meio de fraudes online. O Código Penal, em seu artigo 171, § 2º-A, prevê a pena de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

A divulgação de segredos, muitas vezes relacionada ao vazamento de informações sensíveis, é abordada pelo artigo 153 do Código Penal. Aqueles que divulgam segredos que deveriam permanecer em sigilo podem ser punidos com pena de detenção de 1 a 6 meses, além de multa.

Os crimes contra a honra, tipificados como calúnia, difamação e injúria, previstos nos artigos 138, 139 e 140 do Código Penal, podem também ser punidos em condutas pela internet, conhecidas como injúrias eletrônicas, como a calúnia e a difamação online, estão sujeitas às mesmas situações do Código Penal que se aplicam aos casos ocorridos no mundo físico, as penas são variáveis, dependendo do caso concreto. É importante notar que

o Código Penal Brasileiro está em constante evolução para acompanhar as mudanças no cenário digital.

No ambiente da internet, os crimes de calúnia e difamação, consideradas ofensas à honra objetiva, são caracterizados caso a ofensa seja enviada para grande público e não somente para a vítima, já tratando-se de injúria, considerada ofensa à honra subjetiva, a ofensa é direcionada para a própria vítima (SANTOS; MARTINS; TYBUCSH, 2017).

Em resumo, o Código Penal Brasileiro aborda uma variedade de crimes cibernéticos, confirmando que a legislação precisa se adaptar ao avanço tecnológico. A proteção dos cidadãos, a privacidade e a segurança digital são questões fundamentais refletidas nas disposições legais que visam combater os crimes cibernéticos no Brasil. A atualização constante da legislação é essencial para acompanhar o ritmo das mudanças tecnológicas e garantir a justiça no mundo digital.

Além das disposições mencionadas, existem leis específicas, como a Lei Carolina Dieckmann (Lei 12.737/2012), que se concentra em crimes cibernéticos, como a divulgação não autorizada de imagens íntimas. Tal lei, é um marco na legislação brasileira que aborda crimes cibernéticos, com foco especial na proteção da privacidade e da intimidação dos cidadãos. Essa lei recebeu esse apelido em referência a um notório caso envolvendo a atriz Carolina Dieckmann, que teve suas fotos íntimas divulgadas na internet sem seu consentimento.

Essa legislação foi criada em resposta ao aumento significativo de crimes cibernéticos que envolvem a invasão de dispositivos eletrônicos e a divulgação não autorizada de imagens e informações pessoais. A Lei Carolina Dieckmann trouxe mudanças importantes para a proteção da intimidação online, incluindo a criminalização de condutas, a definição de crimes cibernéticos, o agravamento de pena, a proteção da vítima, a responsabilidade.

A lei estabelece punições para invasões de dispositivos eletrônicos e obtenção não autorizada de informações pessoais, incluindo fotos e dados sensíveis. Aqueles que cometem tais atos sem autorização estão sujeitos a julgamentos legais. A lei define claramente o que constitui crimes cibernéticos, como a invasão de dispositivos alheios e a divulgação não autorizada de imagens. Estas definições ajudam na aplicação consistente da legislação.

Além disso, a Lei Carolina Dieckmann prevê agravamento de pena quando os crimes cibernéticos são crimes contra crianças, adolescentes, idosos ou pessoas vulneráveis, reconhecendo a necessidade de proteção adicional para esses grupos. Importante ressaltar, que a legislação também estabelece medidas para proteger a vítima, incluindo a exclusão da divulgação, comercialização e exposição de imagens obtidas ilegalmente.

Ademais, além de punir os perpetradores, a lei impõe responsabilidades a terceiros que distribuam imagens obtidas ilegalmente, ampliando a proteção da privacidade da vítima.

Assim, a Lei Carolina Dieckmann desempenha um papel fundamental na defesa da privacidade e na prevenção de crimes cibernéticos que violam a intimidação das pessoas. Além disso, ela conscientiza a sociedade sobre a importância de proteger informações pessoais e a necessidade de promover comportamentos éticos na internet. No entanto, o desafio permanece na aplicação eficaz da lei e na educação contínua do público sobre a segurança cibernética, destacando a importância da prevenção como elemento-chave na luta contra os crimes cibernéticos.

5. O PAPEL DO PODER PÚBLICO NA PREVENÇÃO E PROTEÇÃO

Em um mundo cada vez mais interconectado, o combate aos crimes cibernéticos tornou-se uma prioridade global, com o poder público desempenhando um papel fundamental na prevenção e proteção contra essas ameaças. Quatro elementos essenciais que são reforçados significativamente para essa luta são o investimento em tecnologia, a sensibilização a educação, a cooperação internacional e a criação de legislação abrangente.

O investimento em tecnologia desempenha um papel crucial na prevenção e combate aos crimes cibernéticos. Isso envolve uma alocação de recursos para desenvolver sistemas de segurança cibernética robustos, atualizados e proativos. Isso inclui o aprimoramento de firewalls, sistemas de detecção de intrusões e criptografia de dados. Além disso, os governos devem investir em treinamento e capacitação para seus especialistas em segurança cibernética, para que estejam preparados para enfrentar ameaças em constante evolução.

A sensibilização e a educação são ferramentas poderosas na luta contra os crimes cibernéticos. Os governos podem desempenhar um papel fundamental na conscientização

da população sobre práticas seguras na internet. Isso inclui campanhas educativas que alertam sobre os perigos do phishing, da engenharia social e da divulgação de informações pessoais online. Além disso, programas de educação cibernética em escolas e ajudam a criar uma sociedade mais consciente dos riscos e capaz de tomar medidas preventivas.

Os crimes cibernéticos muitas vezes transcendem fronteiras, tornando a cooperação internacional fundamental. Os governos devem colaborar com outros países para investigar e processar crimes cibernéticos que operam além de suas jurisdições. Acordos de compartilhamento de informações, tratados de extradição e forças-tarefa internacionais são mecanismos que facilitam essa cooperação. A cooperação entre países fortalece a capacidade de identificar, rastrear e deter cibercriminosos.

Outra forma de combate e prevenção aos crimes cibernéticos é a criação de legislação abrangente que define claramente os crimes, deliberações e procedimentos legais. Isso permite que as autoridades ajam de maneira eficaz contra infratores. No Brasil, por exemplo, a já citada alhures, Lei Carolina Dieckmann (Lei 12.737/2012), é um exemplo dessa abordagem, estabelecendo punições específicas para crimes cibernéticos, como a invasão de dispositivos eletrônicos e a divulgação não autorizada de imagens.

Uma legislação forte deve incluir penas graves para os crimes cibernéticos, a fim de dissuadir futuras infrações. Isso não apenas protege as vítimas, mas também envia uma mensagem clara de que a prática de crimes cibernéticos não será tolerada. Penas de prisão, multas substanciais e outras avaliações podem servir como um forte dissuasor.

A aplicação eficaz da legislação é essencial para proteger a sociedade. As autoridades deverão dispor de recursos e capacidade técnica para investigar e rastrear os ataques cibernéticos. Isso inclui o uso de tecnologia avançada e a colaboração com especialistas em segurança cibernética. Além disso, é importante que as leis sejam aplicadas de maneira consistente, independentemente da localização do infrator.

Além da legislação forte, o poder público deve promover a conscientização e a educação sobre os perigos dos crimes cibernéticos. Isso não só ajuda a proteger as pessoas, mas também reduz a probabilidade de serem vítimas de ataques. Campanhas de sensibilização podem informar sobre boas práticas de segurança digital e como denunciar atividades suspeitas.

A criação de legislação forte e punitiva aos criminosos cibernéticos é um passo crucial na luta contra os crimes cibernéticos. Essas leis não apenas punem os infratores, mas também enviam um sinal claro de que a sociedade valoriza a segurança digital e está disposta a tomar medidas rigorosas para examiná-la. No entanto, esta abordagem deve ser complementada com ações para prevenir ataques, como investimento em tecnologia e cooperação internacional, a fim de criar um ambiente digital mais seguro e resiliente.

Em resumo, o poder público desempenha um papel crítico na prevenção e proteção contra crimes cibernéticos. O investimento em tecnologia, a sensibilização e educação da população, a cooperação internacional e a criação de legislação eficaz, são fundamentais para enfrentar ameaças cibernéticas. À medida que o cenário digital continua a evoluir, a colaboração entre governos e setor privado é essencial para criar um ambiente cibernético mais seguro e protegido contra os perigos que surgem na era digital. O poder público tem a responsabilidade de liderar esses esforços e garantir a segurança cibernética de seus cidadãos e instituições.

CONSIDERAÇÕES FINAIS

Os crimes cibernéticos evoluíram de curiosidades técnicas para ameaças globais, afetando empresas, governos e indivíduos. A legislação brasileira avançou para abordar essas ameaças, mas o desafio permanece significativo. O poder público desempenha um papel crucial na prevenção e proteção contra crimes cibernéticos, exigindo investimento em tecnologia, conscientização e cooperação internacional. A constante adaptação às mudanças tecnológicas é essencial para enfrentar essa crescente ameaça à segurança cibernética.

Neste contexto, é importante destacar a complexidade e a relevância crescente dos crimes cibernéticos em nossa sociedade digital. O avanço tecnológico proporcionou inúmeras oportunidades, mas também lançou desafios significativos em relação à segurança e privacidade de indivíduos e organizações.

Na conceituação e condutas relacionadas aos crimes cibernéticos, incluem-se atividades que abrangem uma ampla gama de ações abordadas, desde invasões de sistemas até fraudes financeiras e assédio online. Observa-se que o cenário dos crimes cibernéticos

está em constante evolução, à medida que os cibercriminosos se adaptam às novas tecnologias e oportunidades.

Ao traçar a evolução histórica dos crimes cibernéticos, registramos que eles tiveram sua origem em atos curiosos de entusiastas digitais, mas rapidamente se tornaram uma forma de crime sofisticado e lucrativo. Hoje, grupos de hackers, organizações criminosas e até mesmo estados-nação se envolvem em atividades cibernéticas ilegais que têm implicações para a segurança global.

No contexto da legislação brasileira, analisamos a Lei Carolina Dieckmann e os artigos do Código Penal que abordam crimes cibernéticos. Vimos que o Brasil tem se esforçado para criar uma base jurídica sólida para reforçar essas ameaças, com ênfase na proteção da privacidade, punição de infratores e responsabilização de terceiros por informações ilegalmente obtidas ou adulteradas.

Por fim, enfatizamos o papel vital do poder público na prevenção e proteção contra crimes cibernéticos. O governo desempenha um papel central na criação de legislação e na garantia de sua aplicação. Investir em tecnologia, sensibilização e educação, e a cooperação internacional são elementos-chave para enfrentar essa ameaça em constante mutação.

Neste contexto, é essencial que a sociedade como um todo, juntamente com empresas, instituições acadêmicas e o governo, trabalhem de forma colaborativa para enfrentar os desafios dos crimes cibernéticos. A cibernética é uma responsabilidade coletiva, e a conscientização, a educação e a conformidade com a legislação são as bases sobre as quais podemos construir um ambiente digital mais seguro e resiliente. A proteção dos dados, da privacidade e da segurança de todos os cidadãos é um objetivo fundamental que requer esforços coordenados para atingir.

REFERÊNCIAS BIBLIOGRÁFICAS

1. BRASIL. Lei nº 12.737, de 30 de novembro de 2012. "**Dispõe sobre a tipificação criminal de delitos informáticos**". Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 21 de outubro de 2023.

2. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. "**Lei Geral de Proteção de Dados Pessoais**". Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em 21 de outubro de 2023.

3. Brasil. Decreto Decreto-Lei N° 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 21 de outubro de 2023.

4. BRASIL. Polícia Federal. **Crimes Cibernéticos**. Brasília: Departamento de Polícia Federal, [s.d.]". Disponível em: https://www.pf.gov.br/servicos-pf/criminalidade/crimes-ciberneticos . Acesso em 16 de março de 2023.

5. CANALTECH. **"Impactos financeiros dos crimes cibernéticos"**. São Paulo: NZN, [s.d.]. Disponível em: https://canaltech.com.br/seguranca/o-que-e-cybercrime-e- quais-os-impactos-financeiros-dos-crimes-ciberneticos-180106/ . Acesso em 20 de março de 2023.

6. COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **"Crimes Cibernéticos"**. São Paulo: Comitê Gestor da Internet no Brasil, [s.d.]. Disponível em: https://cgi.br/acoes-e-programas/crimes-ciberneticos/ . Acesso em 20 de março de 2023.

7. FELICIANO, Guilherme. **"Impactos do cibercrime no Brasil"**. Revista Brasileira de Inteligência, [S.l.], v. 2, n. 3, p. 55-69, dez. 2014. ISSN 2317-1253. Disponível em: https://rbinacional.org.br/rbi/article/view/20 . Acesso em 14 de abril de 2023.

8. INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). **"Cyberbullying e impactos na educação"**. Brasília: IPEA, [s.d.]. Disponível em: http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=2642 8 . Acesso em 04 de abril de 2023.

9. MINISTÉRIO PÚBLICO FEDERAL. **"Crimes cibernéticos e impactos na sociedade"**. Brasília: Procuradoria-Geral da República, [s.d.]. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/crimes-ciberneticos-e-impactos-na-sociedade. Acesso em 30 de março de 2023.

10. SAFERNET BRASIL. **"Impactos psicológicos do cyberbullying**. [s.d.]". Disponível em: https://new.safernet.org.br/content/o-que-e-cyberbullying-e-quais-os-impactos- psicologicos . Acesso em 16 de março de 2023.

11. SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. 2017.

12. WENDT, Emerson; JORGE, Higor Vinícius Nogueira. Crimes cibernéticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012. p 10.