doi.org/10.51891/rease.v10i10.16023

OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL DE CRIMES VIRTUAIS NA ERA DIGITAL

Ludymilla Sena Costa[1]
Marco Antônio Alves Bezerra[2]

RESUMO: A regulação da internet no Brasil enfrenta desafios significativos devido à sua complexidade e à rápida evolução tecnológica. Embora existam leis específicas voltadas para a segurança digital, a eficácia dessas regulamentações é frequentemente questionada. O atual sistema não consegue abranger adequadamente todos os aspectos da internet, que incluem questões técnicas, econômicas, sociais e políticas. Empresas privadas e órgãos públicos, responsáveis pela proteção das informações virtuais, muitas vezes carecem da tecnologia e do conhecimento necessários para assegurar essa segurança, como evidenciado pelos repetidos vazamentos de dados no país. As leis vigentes tendem a tratar de situações específicas já ocorridas, o que limita sua capacidade de prever e enfrentar novas ameaças emergentes. O Direito, com sua dificuldade intrínseca em acompanhar a rápida evolução tecnológica, torna-se ainda mais desafiador quando se trata de tipificar crimes ainda não praticados. Em resposta a esses desafios, é imperativo que haja um esforço coordenado entre diversas partes interessadas, incluindo a capacitação contínua dos profissionais de investigação criminal e a melhoria da infraestrutura tecnológica das instituições. Somente através de um aprimoramento substancial na formação dos especialistas e na atualização das estruturas tecnológicas será possível garantir uma navegação segura e eficaz na internet, protegendo os usuários contra ameaças em constante evolução.

Palavras-Chave: Regulação da Internet. Segurança Digital. Legislação. Evolução Tecnológica. Capacitação Profissional.

[1]Acadêmica em direito, UnirG - Universidade de Gurupi.
[2]Orientador do curso de direito, UnirG - Universidade de Gurupi. Bacharel em Direito com Especialização em Direito Penal e Processual Penal (CES/Jataí) e em Processo Civil e Processual Civil (FAFICH), Mestre em Direito com área de concentração em Direito do Estado e Teoria do Direito (UFRGS). Promotor de Justiça do Ministério Público Estadual do Tocantins (1990-2006) e, nomeado e empossado como Procurador de Justiça da 11ª Procuradoria do MPE-TO (2006 -). Área de atuação investigativa e docência: recursos gerais do Código de Processo Civil e Código de Processo Penal, crimes e improbidade administrativa. Membro permanente do Colégio de Procuradores do MPE-TO.

ABSTRACT: Internet regulation in Brazil faces significant challenges due to its complexity and rapid technological evolution. Although there are specific laws aimed at digital security, the effectiveness of these regulations is often questioned. The current system cannot adequately cover all aspects of the internet, which include technical, economic, social and political issues. Private companies and public bodies, responsible for protecting virtual information, often lack the technology and knowledge necessary to ensure this security, as evidenced by repeated data leaks in the country. Current laws tend to deal with specific situations that have already occurred, which limits their ability to predict and face new emerging threats. Law, with its intrinsic difficulty in keeping up with rapid technological evolution, becomes even more challenging when it comes to classifying crimes that have not yet been committed. In response to these challenges, it is imperative that there is a coordinated effort between various stakeholders, including the continuous training of criminal investigation professionals and the improvement of the technological infrastructure of institutions. Only through a substantial improvement in the training of specialists and the updating of technological structures will it be possible to guarantee safe and effective browsing on the internet, protecting users against constantly evolving threats.

Keywords: Internet Regulation. Digital Security. Legislation. Technological Evolution. Professional Training.

1. INTRODUÇÃO

A internet, uma vasta rede que conecta o mundo, transformou radicalmente a maneira como interagimos e realizamos nossas tarefas diárias. Com o avanço tecnológico, as distâncias entre as pessoas se encurtaram, e uma infinidade de oportunidades surgiu. Estamos constantemente conectados, e a maioria das nossas atividades pode ser realizada na "palma da mão", por meio da internet.

Entretanto, esse progresso também trouxe consigo o risco da exposição nas redes sociais. Informações pessoais estão cada vez mais acessíveis, e os criminosos encontraram nesse ambiente um novo terreno para suas ações mal-intencionadas. A investigação desses crimes cibernéticos apresenta desafios consideráveis, como a identificação da origem da ação, do autor e do impacto causado. Essas são questões cruciais que as forças policiais enfrentam ao tentar resolver cada caso.

Nesse contexto, surgem perguntas relevantes: Como os crimes se manifestam no ciberespaço? O ordenamento jurídico penal atual possui normas adequadas para

proteger os bens jurídicos atingidos pela cibercriminalidade? E as forças policiais, estão preparadas e capacitadas para lidar com os crimes virtuais?

Atualmente, a sociedade está em alerta. Embora existam delegacias especializadas, muitos dos profissionais que nelas atuam não possuem especialização em informática e carecem de conhecimento e ferramentas para combater a cibercriminalidade. A seleção desses profissionais, geralmente realizada por meio de concurso público, exige apenas formação superior, sem especificar a necessidade de especialização na área.

O aumento da criminalidade virtual e a necessidade de novas leis são inegáveis. A internet, apesar de ser uma ferramenta transformadora, também tem sido associada ao crescimento dos crimes virtuais. Surge, portanto, a necessidade de normas eficazes que possam punir os criminosos e reduzir a ocorrência desses delitos.

O objetivo deste artigo é analisar a proteção penal dos crimes virtuais, refletir sobre os desafios jurídicos trazidos por essa nova forma de criminalidade, examinar as leis em vigor, os tipos de crimes mais comuns e como se proteger e buscar ajuda. Para alcançar esses objetivos, será realizada uma pesquisa bibliográfica em livros, doutrinas, leis, artigos científicos, jornais e outras publicações relevantes.

2. AVANÇOS TECNOLÓGICOS E CRIMES VIRTUAIS

O mundo contemporâneo demanda um acompanhamento atento das transformações sociais através de legislações, especialmente no campo dinâmico da tecnologia da informação. Essa evolução proporcionou novas conquistas, mas também originou novas ilegalidades. Neste contexto, o propósito das leis é estabelecer barreiras firmes contra os crimes virtuais. Atualmente, muitos brasileiros dependem de dispositivos digitais, onde armazenam dados e informações fundamentais para suas vidas pessoais e profissionais. Essas informações, intimamente ligadas a seus proprietários, sejam pessoas físicas, jurídicas, ou instituições bancárias, despertam o interesse de criminosos.

Conforme Coriolano Almeida Camargo e Cleórbete Santos, os crimes mais recorrentes no ambiente digital são aqueles cometidos contra o sistema financeiro, com destaque para o phishing, que envolve furtos por meio de fraude. Nesse crime, o

indivíduo recebe uma mensagem falsa pela internet, clicando em um arquivo malicioso que insere um vírus em seu dispositivo, permitindo que o criminoso obtenha seus dados bancários e retire valores da conta. Ao contrário do estelionato, em que a vítima entrega voluntariamente seus bens, no furto mediante fraude, o criminoso aproveita-se da distração da vítima, que acredita estar lidando com uma mensagem legítima. Embora o furto mediante fraude já seja tipificado, outros crimes, como invasões em sites e bancos de dados, ainda precisam ser regulamentados. Camargo e Santos observam que, em crimes que prejudicam serviços públicos via internet, o impacto pode ser maior, demandando penas mais rigorosas devido à propagação rápida das informações no meio virtual, seja para o bem ou para o mal (Camargo; Santos, 2018, p. 34).

As funções da polícia judiciária foram definidas no artigo 144 da Constituição Federal de 1988. A polícia, como uma instituição de direito público, foi criada para garantir a paz e a segurança pública na sociedade. Portanto, a polícia desempenha tanto funções administrativas quanto judiciais, atuando de forma preventiva e repressiva, com o objetivo de restringir, regular e fiscalizar os direitos e interesses dos cidadãos, sempre buscando manter a ordem e a segurança pública.

O artigo 144, parágrafo 4º, da Constituição Federal de 1988 estabelece que a Polícia Civil seja liderada por delegados, em cooperação com a Polícia Federal e Militar, para funções de polícia judiciária e investigações criminais. Assim, as investigações policiais são cruciais e determinam a eficácia na resolução dos crimes. O cibercrime, em particular, apresenta especificidades que exigem recursos adequados, sendo, muitas vezes, um desafio para a elucidação desses crimes.

Rocha (2013) destaca que especialistas defendem que uma alteração no Código Penal não é indispensável para combater e prevenir eficazmente os cibercrimes. O professor Túlio Lima Vianna, da Universidade Federal de Minas Gerais, argumenta que o ordenamento jurídico atual não precisa de novas leis, mas sim de uma estrutura técnica adequada nas investigações forenses e uma ação conjunta entre os diversos órgãos do Poder Judiciário e do Ministério Público (Rocha, 2013, p. 8).

Podemos considerar a Internet como a "mãe de todas as redes" por conectar computadores em todo o mundo. Surgiu na década de 1960 e chegou ao Brasil em 1992,

inicialmente conectando grandes universidades. Naquela época, era usada apenas para troca de e-mails. Em 1995, a Internet começou a ser utilizada comercialmente no país, e no mesmo ano foi criado o Comitê Gestor da Internet no Brasil (CGI.br), responsável por garantir a qualidade técnica da Internet no país e divulgar os serviços prestados.

A Internet transformou a forma como as pessoas compartilham informações. No passado, o acesso à Internet era lento e caro, o que limitava seu uso. Com a chegada das redes de banda larga, 3G, 4G e 5G, e com a queda nos preços, cada vez mais pessoas têm acesso à internet. Essa mudança permite que as pessoas acessem uma variedade de informações de maneira rápida e eficiente, possibilitando a comunicação global, o acesso a vídeos, músicas, notícias e compras online.

Nessa linha, Marcelo Crespo afirma:

> Toda essa evolução fez com que as relações comerciais, as administrações públicas e a sociedade em geral passassem a depender muito da eficiência e segurança da chamada tecnologia da informação. [...] As redes informáticas se tornaram os nervos da sociedade, que cada vez mais depende dos computadores e das intranets (redes internas de cada organização). (Crespo, 2011, p. 368).

O avanço tecnológico tem conduzido a sociedade a uma nova era, a era da informação. Nesse contexto, os sistemas de defesa passaram a depender cada vez mais da tecnologia da informação. Isso ocorre porque a internet, ao mesmo tempo em que trouxe importantes avanços na troca de informações, também trouxe grandes ameaças devido ao seu uso inadequado.

2.1 A Internet e o Direito

A conexão entre o Direito e a Informática tem se tornado cada vez mais estreita. Com o avanço tecnológico, surgem novas formas de crimes e violações de direitos a todo momento. Por essa razão, é imperativo que o Direito se adapte às novas realidades para garantir a justiça e a segurança da sociedade. Alguns especialistas defendem a criação de um novo ramo do Direito voltado especificamente para as questões relacionadas à Informática. Esse novo campo seria responsável por regulamentar o uso das tecnologias e punir os crimes cometidos por meio delas.

No entanto, independentemente da criação de um novo ramo, é essencial que o Direito tradicional se atualize para acompanhar as inovações tecnológicas. O Direito

precisa ser capaz de proteger os direitos dos cidadãos, mesmo quando esses direitos são violados através da tecnologia.

Nesse contexto, Miguel Reale esclarece: "O Direito é, por conseguinte, um fato ou fenômeno social; não existe senão na sociedade e não pode ser concebido fora dela. Uma das características da realidade jurídica é, como se vê, a sua socialidade, a sua qualidade de ser social." (Reale, 2010, p. 2).

De acordo com Pinheiro (2016, p. 77), o Direito Digital é, na verdade, o aprimoramento do próprio Direito, pois, além de incorporar seus princípios fundamentais, oferece novas ideias e perspectivas ao pensamento jurídico em geral (Direito Civil, Autoral, Econômico, Penal, Tributário, etc.). O Direito Digital deve ser aprofundado para fornecer ferramentas eficazes que atendam a essas novas demandas.

Sobre esses novos desafios, Patrícia Pinheiro afirma:

> [...] são os novos profissionais do Direito os responsáveis por garantir o direito à privacidade, a proteção do direito autoral, do direito de imagem, da propriedade intelectual, dos royalties, da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra hackers e muito mais.(Pinheiro, 2016, p. 77).

Na visão de Crespo (2011, p. 543), ao considerar o Direito Penal em sua relação com a informática, é necessário debater questões como a harmonização internacional, a definição do local do crime, spam, estelionato, acesso a sistemas, legítima defesa, vírus, engenharia social, entre outros.

Essas novas ameaças, até então desconhecidas pelo Direito, têm causado conflitos. Elas apresentam situações em que a vítima é a coletividade em geral, e não os bens jurídicos tradicionais, como a vida e o patrimônio, sendo comparáveis a atentados contra a ordem econômica e o meio ambiente, que são bens jurídicos supraindividuais, pertencentes à coletividade. Em outras palavras, a internet, apesar de ser crucial para o desenvolvimento econômico, também exige a definição de novos contratos sociais que deram origem a novos conflitos em uma nova área criminal. (Brito, 2013, p. 185).

Para Pinheiro (2016, p. 78), não existe e nem deve ser criado um "Direito da Internet", pois, ao longo da história, outros meios de comunicação, como a televisão, o telefone e o rádio, também adquiriram relevância jurídica. Existem peculiaridades

na internet que devem ser incorporadas pelas diferentes áreas do Direito, sem a necessidade de um ramo específico. A evolução tecnológica é sempre mais rápida que a legislativa, por isso, os princípios devem prevalecer sobre as regras.

As revoluções tecnológicas trouxeram muitos benefícios para a sociedade, como a democratização do acesso à informação, a facilitação da comunicação e o desenvolvimento de novas formas de entretenimento. Contudo, elas também trouxeram um lado sombrio, como o aumento da criminalidade virtual. Com o progresso tecnológico, surgem constantemente novas modalidades de crimes, como o cyberbullying, o roubo de dados e o terrorismo digital, que se tornam cada vez mais comuns. Esses crimes são cometidos por pessoas mal-intencionadas que buscam prejudicar outras pessoas ou a sociedade em geral.

É crucial estar ciente desse lado negativo da tecnologia para se proteger. Medidas como o uso de senhas fortes, a instalação de antivírus e softwares de segurança, e a cautela ao abrir e-mails ou arquivos suspeitos são essenciais para se proteger contra crimes virtuais.

3. LEGISLAÇÕES PENAIS NO ÂMBITO DIGITAL

Como mencionado anteriormente, o desenvolvimento tecnológico e a crescente utilização da internet impuseram a necessidade de uma investigação policial especializada. Essa evolução também gerou discussões sobre a proteção penal e, até o ano de 2012, a legislação brasileira não tipificava adequadamente os delitos cometidos via internet. Em respeito ao princípio da legalidade, previsto no artigo 5º, inciso XXXIX da Constituição Federal de 1988, crimes assim cometidos não poderiam ser punidos sem que estivessem devidamente tipificados em lei. A ausência de regulamentações específicas permitiu a rápida e diversificada disseminação dessas condutas, deixando uma lacuna que levou a intensos debates sobre a necessidade de o ordenamento jurídico brasileiro adaptar-se às novas práticas realizadas por meio de ferramentas informáticas.

Um dos episódios que mais acalorou esse debate foi o caso da atriz Carolina Dieckmann, que teve suas fotos íntimas vazadas após a invasão de seu computador.

Este incidente trouxe à tona a necessidade urgente de se criar leis específicas para crimes virtuais.

A falta de uma legislação específica para crimes virtuais no Brasil é um problema antigo. O Código Penal brasileiro foi promulgado em 1940, muito antes da existência da internet. O direito tem como função proteger os bens mais importantes da sociedade, mas com o mínimo de interferência na vida dos cidadãos. Criar leis que tipifiquem crimes virtuais sem infringir esses princípios foi um grande desafio. Apesar disso, os crimes virtuais representam uma ameaça crescente, e o Brasil precisava urgentemente de uma legislação que pudesse enfrentar essa nova realidade. A aprovação de leis específicas para crimes virtuais foi, portanto, um passo essencial para combater esse desafio【Milagre, 2016, p. 47】.

A inevitabilidade da aprovação de tais leis decorreu do fato de que o ambiente digital se tornou um espaço de constante troca de informações, abrangendo todas as esferas da sociedade. Desde conversas cotidianas até transações financeiras, quase tudo passou a ser realizado por meio da rede informática.

Ainda segundo Milagre (2016, p. 48), mesmo diante desses fatos, havia resistência quanto à criação de uma legislação específica para a informática. Foi necessário que uma figura pública, como a atriz Carolina Dieckmann, fosse vítima de um crime virtual para que uma demanda, que já estava há mais de dez anos no Congresso Nacional, fosse finalmente aprovada. O crime em questão deu origem à Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", sancionada em novembro de 2012.

Os crimes virtuais não se limitam a afetar bens jurídicos tradicionais, como patrimônio e vida. Os criminosos também visam sistemas, informações e outros bens específicos do ambiente digital. Por isso, é imprescindível uma legislação que aborde esses crimes de maneira abrangente e específica.

Conforme exposto por Brito (2013, p. 780), os crimes virtuais são pluriofensivos, ou seja, além de necessitarem de proteção dos bens jurídicos tradicionais, também exigem salvaguardas específicas que surgem da sociedade da informação. Não se deve limitar a análise apenas ao meio pelo qual o crime é cometido, mas deve-se também considerar a informação como um bem a ser protegido.

3.1 O Código Penal

O avanço tecnológico e a proliferação de crimes digitais levaram à necessidade de adaptar o Código Penal para enfrentar essas novas ameaças. As alterações introduzidas visam aumentar as penas para crimes como invasão de dispositivos, furto qualificado, e apropriação indébita que ocorram em meio digital, independentemente de estarem conectados à internet.

A partir dessas mudanças, o crime de invasão de dispositivo, assim como a alteração ou destruição de dados e a instalação de vírus (malware) para obtenção ilícita, passou a ser punido com pena de prisão de 1 a 4 anos e multa, sendo essa pena agravada em até um terço se houver perda econômica, podendo o aumento da pena ser de até dois terços. Anteriormente, essas condutas eram punidas com detenção de apenas três meses a um ano. Além disso, obter "comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais ou controle remoto não autorizado de equipamentos" pode resultar em uma pena de dois a cinco anos de prisão e multa, antes limitada a seis meses a dois anos.

A Lei n.º 12.735/2012, em seu artigo 4º, destaca que “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.

3.2 Lei Carolina Dieckmann (Lei N.º 12.737/12)

A Lei n.º 12.737/12, sancionada em 2012, ficou conhecida como "Lei Carolina Dieckmann" em referência à atriz que foi vítima de um escândalo após ter seu dispositivo eletrônico invadido, resultando na divulgação de suas fotos íntimas na internet. Os criminosos acessaram o e-mail da atriz, obtiveram as imagens e, posteriormente, passaram a extorqui-la, exigindo dinheiro para não divulgar o material. Como na época não havia uma legislação específica para esse tipo de invasão, os responsáveis foram condenados por extorsão, furto e difamação, mas não pela invasão do dispositivo em si, devido à falta de tipificação do crime.

A grande repercussão do caso na mídia gerou pressão pública para a criação de uma legislação que abordasse crimes cibernéticos. Como resultado, foi aprovado o

Projeto de Lei n.º 35/2012, que teve origem no PL n.º 2.793/2011. Essa foi a primeira lei do ordenamento jurídico brasileiro a tratar de crimes cometidos pela internet, especialmente através do dispositivo 154-A do Código Penal Brasileiro, que criminaliza a invasão de dispositivos eletrônicos alheios.

> Art. 154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o intuito de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular, ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena: Detenção, de 3 meses a 1 ano, e multa.
>
> § 1º A mesma pena se aplica a quem produz, oferece, distribui, vende ou dissemina dispositivo ou programa de computador destinado a facilitar a prática da conduta definida no caput.
>
> § 2º A pena é aumentada de um sexto a um terço se da invasão resultar prejuízo econômico.
>
> § 3º Se a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, ou no controle remoto não autorizado do dispositivo invadido:
>
> Pena: Reclusão, de 6 meses a 2 anos, e multa, se a conduta não constituir crime mais grave.
>
> § 4º Na hipótese do § 3º, a pena é aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiros, a qualquer título, dos dados ou informações obtidos.
>
> § 5º A pena é aumentada de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
>
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Brasil, 1940, online)

Os principais bens jurídicos protegidos pelo artigo 154-A são a segurança dos dispositivos eletrônicos, a privacidade e a liberdade individual. O crime é configurado somente quando a conduta envolve o dispositivo de outra pessoa, sendo um crime comum que pode ser praticado por qualquer indivíduo. A vítima pode ser qualquer pessoa física ou jurídica. Para a consumação do crime, não basta apenas invadir o dispositivo; é necessário obter, alterar ou destruir dados sem o consentimento do titular, ou buscar obter alguma vantagem ilícita, como dinheiro ou favores sexuais. A ação penal é pública condicionada à representação, exceto quando envolve a

administração pública, caso em que a ação é pública incondicionada, conforme o artigo 154-B do Código Penal.

Art. 154-B: Nos crimes definidos no art. 154-A, a ação penal procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, ou contra empresas concessionárias de serviços públicos.

Caso o crime seja consumado, a pena pode ser agravada se a conduta estiver enquadrada nas circunstâncias previstas nos parágrafos 2º e 4º, ou se constituir um crime mais grave, conforme o parágrafo 3º do artigo 154-A do Código Penal.

Essa lei também tipificou a indisponibilização de serviços por meio de ataques de negação de serviço (DoS), um dos crimes mais comuns na internet. Esses ataques sobrecarregam servidores, impedindo que usuários legítimos se conectem à rede. A Lei n.º 12.737/12 complementou o artigo 266 do Código Penal, que antes não abordava tais interrupções.

> Art. 266: Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar seu restabelecimento:
>
> Pena: Detenção, de 1 a 3 anos, e multa.
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta seu restabelecimento.
>
> § 2º As penas são aplicadas em dobro se o crime for cometido durante calamidade pública.

Além disso, a Lei Carolina Dieckmann alterou o artigo 298 do Código Penal, que trata da falsificação ou alteração de documento particular, equiparando cartões de débito e crédito a documentos particulares.

> Art. 298: Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro.
>
> Pena: Reclusão, de 1 a 5 anos, e multa.
>
> Parágrafo único: Para os fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Segundo Maués, Duarte e Carvalho (2018, p.173), a Lei 12.737/12 introduziu três novas tipificações penais no Código Penal: o artigo 154-A, sobre invasão de dispositivo informático; o artigo 266, §§1º e 2º, sobre interrupção ou perturbação de serviços telefônicos, telegráficos, informáticos ou de informação de utilidade pública; e o artigo 298, parágrafo único, que trata da falsificação de cartões de crédito ou débito.

Harakemiv e Vieira (2014, p. 425) também destacam que a nova lei modificou a redação do artigo 266 do Código Penal e acrescentou o parágrafo único ao artigo 298, que equipara cartões de crédito a documentos particulares.

Embora a aprovação da Lei n.º 12.737/2012 tenha sido um passo importante para a proteção da privacidade no ambiente digital, a lei ainda possui lacunas e inconsistências que podem comprometer sua eficácia. Por exemplo, a necessidade de violação de mecanismo de segurança para a configuração do crime deixa brechas para que criminosos obtenham ou excluam informações de dispositivos com o consentimento do proprietário sem serem penalizados. Além disso, a definição de "mecanismo de segurança" é ampla e pode gerar diferentes interpretações, o que pode enfraquecer a aplicação da lei.

Luis Flávio Gomes observa que a lei permite múltiplas interpretações e não é eficaz em sua função preventiva, em parte devido às penas baixas que prescrevem rapidamente (Gomes, 2013).

3.3 Marco civil da internet (lei nº 12.965/2014)

A introdução da internet trouxe uma nova dinâmica para a sociedade, exigindo que o direito penal se ajustasse para enfrentar os crimes cometidos no ambiente digital. Esses crimes, especialmente quando envolvem indivíduos ou entidades públicas, geram grande repercussão social, tornando-se uma preocupação tanto para a sociedade quanto para os profissionais do direito. Diante dessa preocupação, iniciou-se o debate sobre os direitos e deveres dos usuários da internet, com o intuito de estabelecer o que é permitido e o que é proibido no meio digital (Marcacini, 2016, p. 727).

O Marco Civil da Internet, estabelecido pela Lei nº 12.965/2014, foi criado para regulamentar os direitos e obrigações dos internautas. Esta lei se tornou uma ferramenta crucial para proteger os dados dos usuários, assegurando que o acesso a informações e conteúdos privados em sites e redes sociais só ocorra mediante ordem judicial. Além disso, a lei prevê a remoção de conteúdos ofensivos, violentos ou pornográficos. No caso específico de pornografia de vingança, a vítima pode solicitar diretamente ao site que hospeda o conteúdo que o remova, enquanto outros casos exigem ordem judicial e análise para retirada da web.

Vale destacar que o Marco Civil da Internet não tipifica crimes. Seu foco é regular o uso da internet no Brasil, baseando-se em seus princípios, e orientar as ações do Estado nesse âmbito.

A Lei nº 12.965/2014 estabelece seus fundamentos no artigo 3º, que são:

> Art. 3º: A regulamentação do uso da internet no Brasil segue os seguintes princípios:
>
> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, conforme a Constituição Federal;
>
> II - Proteção da privacidade;
>
> III - Proteção dos dados pessoais, conforme a lei;
>
> IV - Preservação e garantia da neutralidade da rede;
>
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com padrões internacionais e incentivo às boas práticas;
>
> VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - Preservação da natureza participativa da rede;
>
> VIII - Liberdade dos modelos de negócios promovidos na internet, desde que não contrariem os princípios estabelecidos nesta Lei.

A neutralidade da rede assegura que todos os usuários da internet possam acessar qualquer tipo de conteúdo, independentemente do provedor ou do plano de assinatura escolhido. Isso significa que os provedores de internet não podem cobrar taxas adicionais para acessar determinados sites ou serviços, como e-mail, streaming de vídeo ou redes sociais.

As empresas provedoras de internet argumentam que a neutralidade da rede impede a criação de planos mais baratos, pois não podem cobrar mais pelos serviços mais populares. Em contrapartida, os defensores da neutralidade afirmam que ela é essencial para garantir a liberdade de expressão e o acesso à informação, independentemente da classe social (Santino, 2014).

A lei também assegura a privacidade dos usuários da internet. Os provedores de internet devem armazenar os dados de conexão por um ano em um ambiente seguro e só podem compartilhar essas informações com terceiros mediante ordem judicial. As informações que os usuários divulgam na internet só podem ser utilizadas para os fins aos quais foram originalmente coletadas, pois esses dados podem ser facilmente armazenados e vendidos para outros propósitos.

Além disso, a lei determina que os provedores de internet não são responsáveis pelo conteúdo postado por seus usuários, prevenindo a censura caso fossem corresponsáveis. Aqueles que postam conteúdos ofensivos têm o direito ao contraditório, exceto quando as postagens violam algum tipo penal, como no caso de pornografia infantil, racismo, etc. (Amaral, 2016).

No passado, era difícil para uma pessoa comum se comunicar com um grande público, pois isso exigia acesso a equipamentos caros e sofisticados, como gráficas, rádios e TVs. Com a internet, essa realidade mudou, permitindo que qualquer pessoa, com um celular simples e barato, possa se expressar para o mundo inteiro. Por isso, é fundamental que existam leis que garantam o direito à liberdade de expressão na internet. O Marco Civil da Internet é uma conquista significativa para a democracia e a liberdade de expressão no Brasil, assegurando que todos os usuários tenham acesso à informação e possam se expressar livremente, sem censura ou discriminação.

4 CRIMES VIRTUAIS

Os crimes virtuais, também chamados de crimes cibernéticos, crimes tecnológicos, crimes informáticos ou crimes de informação, são atividades prejudiciais realizadas por meio de dispositivos eletrônicos ou contra sistemas informáticos. Esses crimes podem atingir indivíduos, empresas ou instituições públicas. No Brasil, as infrações virtuais mais frequentes incluem fraudes, roubo de dados e ataques cibernéticos. Outros delitos virtuais possíveis são pornografia infantil, discriminação racial ou religiosa e apoio a crimes ou terrorismo.

De acordo com Tarcísio Teixeira, “[...] crime de informática é aquele que, quando cometido, utiliza meios informáticos como ferramenta para alcançar o resultado desejado, assim como aquele perpetrado contra sistemas e meios informáticos” (Teixeira, 2018, p. 505-506).

Essas infrações podem ser classificadas em "crimes cibernéticos" e "condutas prejudiciais atípicas". O termo "comportamento lesivo atípico" refere-se a atos que causam dano à vítima, mas que não têm uma classificação criminal específica, e, portanto, o autor não pode ser punido dentro da categoria criminal. O "crime cibernético" pode ser "evidente" (inadequado) ou "totalmente cibercrime" (legítimo).

O termo "aberto" refere-se a conteúdos que podem ser transmitidos com ou sem o uso de computador, funcionando apenas como um meio de aplicação. Assim, existe uma distinção entre crimes “exclusivamente cibernéticos”, que só podem ser cometidos através de um computador ou outro dispositivo eletrônico com acesso à internet.

Os crimes cibernéticos abertos podem ser categorizados em três tipos: crimes puros, comuns e mistos. Crimes puros ocorrem unicamente no ambiente virtual, utilizando dispositivos eletrônicos. Exemplos incluem invasão de dispositivos informáticos, roubo de dados e pornografia infantil. Crimes comuns são aqueles que podem acontecer tanto no ambiente virtual quanto no físico, como estelionato, ameaças e difamação. Crimes mistos utilizam o ambiente virtual como meio para a realização de crimes que também podem ser cometidos no mundo físico, como fraude eletrônica, chantagem e tráfico de drogas.

Os crimes puros são mais complexos de investigar e punir devido ao anonimato dos criminosos, tornando sua identificação difícil. Crimes comuns são relativamente mais fáceis de investigar e punir, pois os infratores podem ser localizados e identificados no ambiente físico. Crimes híbridos combinam aspectos dos dois primeiros tipos e podem ser desafiadores para investigação e punição, já que os criminosos podem operar anonimamente online, dificultando a identificação no mundo físico.

Um estudo recente realizado pela SaferNet Brasil em parceria com o Ministério Público Federal (MPF) revelou que, no Brasil, são registrados diariamente pelo menos 366 (trezentos e sessenta e seis) crimes cibernéticos. A maioria desses crimes envolve pornografia infantil, seguida por apologia e incitação a crimes contra a vida e violência contra mulheres/misoginia (CRIMES cibernéticos [...], 2019).

O aumento dos crimes virtuais é cada vez mais frequente devido a dois principais fatores: a falsa sensação de anonimato e a falta de cuidado dos usuários. Os criminosos muitas vezes acreditam que podem agir sem consequências na internet, já que não são facilmente identificáveis. Além disso, muitos usuários não são conscientes dos riscos de fornecer suas informações pessoais online.

A falsa sensação de anonimato representa um problema real, pois a internet oferece um ambiente anônimo para muitos usuários, facilitando a prática de crimes.

Os criminosos podem se esconder atrás de perfis falsos e cometer infrações sem serem identificados.

A falta de cuidado dos usuários também contribui para o aumento dos crimes virtuais. Muitas pessoas não estão cientes dos riscos associados ao fornecimento de dados pessoais na internet, como nome, endereço, número de telefone e informações de cartões de crédito em sites e aplicativos não confiáveis.

4.1 Pornografia infantil

Conforme Moisés Cassanti (2014, p. 40):

> A pornografia infantil abrange a produção, publicação, venda, aquisição e armazenamento de materiais pornográficos envolvendo crianças através da internet, incluindo páginas da web, e-mails, newsgroups, salas de bate-papo (chat) ou outros meios. Também se refere ao uso da internet para aliciar crianças ou adolescentes a participar de atividades sexuais ou a se expor de maneira pornográfica.

Esse crime possui características próprias quando praticado online, pois elimina a necessidade de contato físico entre os envolvidos. Basta capturar imagens da criança ou do adolescente em contextos pornográficos para que o crime seja consumado. Além disso, o contato virtual entre a vítima e o abusador é possível, e, quando a vítima se recusa a obedecer às ordens do abusador, frequentemente é ameaçada com a divulgação do conteúdo, o que pode levar a vítima a ceder às exigências do abusador (Silva & Veronese, 2009).

É crucial distinguir pedofilia de pornografia infantil. Enquanto a pornografia infantil é abordada pelo Estatuto da Criança e do Adolescente (ECA), Lei n.° 8.069, a pedofilia é um transtorno psicológico caracterizado pela atração sexual por crianças. A pedofilia pode tornar o criminoso imputável ou semi-imputável, e a internet é um meio pelo qual essas pessoas podem satisfazer seus desejos de forma digital. Na pornografia infantil, os proprietários de sites recebem pagamento dos usuários em troca de vídeos e imagens, enquanto na pedofilia, as redes são visitadas e alimentadas por pedófilos. O material pornográfico infantil é frequentemente compartilhado por e-mail ou outros meios (Teixeira, 2018, p. 513-514).

A Lei n.° 11.829/2008 adicionou o artigo 241-A ao Estatuto da Criança e do Adolescente:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Pena – reclusão de 3 (três) a 6 (seis) anos, e multa.
>
> § 1º Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo."

Importa destacar que os crimes de pornografia infantil são de competência da Justiça Federal. O Congresso Nacional, por meio do Decreto Legislativo n.º 28, de 14 de setembro de 1990, e o Poder Executivo, pelo Decreto n.º 99.710, de 21 de novembro de 1990, aprovaram e promulgaram o texto da Convenção sobre os Direitos da Criança, adotada pela Assembleia Geral das Nações Unidas, o que implica a aplicação do inciso V do art. 109 da Constituição Federal.

4.2 CRIMES CONTRA A HONRA

A internet proporciona um vasto espaço para a diversidade de opiniões, o que é benéfico. No entanto, é fundamental lembrar que comentários ofensivos podem resultar em responsabilização. A liberdade de expressão é um direito fundamental, mas não deve ser confundida com o direito de ofender. Comentários prejudiciais podem causar danos psicológicos, morais e até financeiros às vítimas. Portanto, é importante pensar cuidadosamente antes de publicar qualquer comentário na internet, pois suas palavras podem ter repercussões.

Guilherme Nucci define a honra como a capacidade de avaliar a autoridade moral de uma pessoa, fundamentada em sua honestidade, comportamento adequado, respeito social e correção moral, estando, portanto, ligada à postura conforme os bons costumes (Nucci, 2018, p. 211).

Os crimes contra a honra são classificados em três tipos: calúnia, difamação e injúria, todos descritos no Código Penal Brasileiro:

> - Art. 138: Caluniar alguém, imputando-lhe falsamente um fato que é definido como crime.

> - Art. 139: Difamar alguém, imputando-lhe um fato que prejudica sua reputação.
>
> - Art. 140: Injuriar alguém, ofendendo sua dignidade ou decoro.

De acordo com Campanhola (2018), se a difamação for realizada por e-mail, cada pessoa que receber e compartilhar o e-mail pode ser considerada coautora. No caso de difamação, é necessário fazer uma retratação pública se houver arrependimento. Um insulto é uma acusação que ofende a imagem de outra pessoa.

O crime de racismo também é comum e está previsto no artigo 20 da Lei n.° 7.716/89:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

A pena para esse crime é de reclusão de 1 a 3 anos, além de multa. No entanto, se o crime for cometido em ambiente virtual, a pena aumenta para reclusão de 2 a 5 anos e multa.

4.3 Estelionato

O estelionato é um crime que ocorre quando uma pessoa engana outra para obter vantagem, como dinheiro, bens ou serviços. Esse crime se distingue de outros por seu fundamento no engano. O estelionatário induz a vítima ao erro, fazendo-a acreditar em algo falso. Dessa forma, o estelionato causa grandes prejuízos materiais e morais às vítimas.

Para que o estelionato seja configurado, é necessário usar métodos fraudulentos para induzir a vítima ao erro, e deve haver o duplo resultado: a vantagem ilícita do criminoso e o prejuízo à vítima causado pela fraude (Delmanto, 2016, p. 622).

No meio digital, um golpe pode começar com a criação de um site falso que promete benefícios às vítimas, como links patrocinados, mensagens pelo WhatsApp ou posts no Facebook, geralmente fingindo ser uma empresa legítima. O estelionatário, então, contata as vítimas e apresenta o golpe como uma oportunidade única e vantajosa. Após obter o dinheiro, o golpista desaparece, e as vítimas percebem que foram enganadas (Bernal, 2019).

Outra prática comum de estelionato na internet envolve a invasão de caixas de e-mails, especialmente de usuários que frequentemente utilizam internet banking. O estelionatário pode clonar a página de um banco e fazer com que o usuário insira sua

senha, acreditando estar em um ambiente seguro, já que o site é idêntico ao original (Inellas, 2009).

4.5 A necessidade de capacitação dos profissionais contra os crimes virtuais

A Lei n.º 12.735/2012, em seu artigo 4º, estabelece que "os órgãos da polícia judiciária devem criar, conforme regulamentação, setores e equipes especializadas no combate aos crimes praticados em redes de computadores, dispositivos de comunicação ou sistemas informatizados". Para melhorar o serviço prestado à sociedade, é necessário não apenas aprimorar os recursos estatais e a infraestrutura, mas também investir em conhecimento especializado, incluindo a capacitação de profissionais da área de informática. A atuação no campo da segurança cibernética requer mais do que a aplicação das normas penais; é essencial ter profissionais bem treinados e informados.

A evolução dos crimes virtuais e das técnicas investigativas revela a necessidade contínua de capacitação para os profissionais da área. A colaboração institucional, incluindo o intercâmbio de informações e soluções tecnológicas, é fundamental para enfrentar esses desafios (Silva, 2006).

A principal demanda no combate aos crimes virtuais é a formação contínua dos policiais civis envolvidos na investigação criminal. A discussão doutrinária sobre medidas a serem adotadas para a identificação e solução desses casos já está em andamento, o que pode tornar a abordagem desses crimes mais eficiente. Destaca-se a importância da cooperação entre as polícias estaduais e federais, bem como a troca de informações com agências internacionais, para garantir qualificações adequadas.

Maues, Duarte e Cardoso (2018) ressaltam a importância da especialização em diversas áreas do sistema de justiça:

> Delegacias devem se especializar em crimes cibernéticos, juízes precisam atualizar-se sobre jurisprudências e doutrinas relacionadas aos delitos informáticos, e advogados, tanto públicos quanto privados, devem acompanhar a evolução do Direito Digital para melhorar o funcionamento da Justiça no Brasil" (Maues, Duarte, Cardoso, 2018, p. 178).

Dado o aumento dos crimes cometidos via internet, a especialização dos profissionais é crucial. No Brasil, já existem delegacias dedicadas a esses crimes, como a Delegacia de Repressão aos Crimes Cibernéticos em Fortaleza, Ceará. Contudo,

ainda há uma carência de profissionais com formação específica em tecnologia. Como os cargos são preenchidos por meio de concursos que exigem apenas nível médio e superior, a formação e especialização em tecnologia se tornam essenciais para lidar adequadamente com os desafios da cibersegurança.

CONSIDERAÇÕES FINAIS

A regulação da internet no Brasil apresenta uma complexidade considerável e abrange múltiplas dimensões. Embora existam legislações específicas para essa área, a efetividade dessas regulamentações é frequentemente questionada. A estrutura vigente não é suficiente para cobrir de forma adequada todos os aspectos da internet, que incluem não apenas questões técnicas, mas também dimensões econômicas, sociais e políticas.

Empresas privadas e órgãos públicos, responsáveis pela segurança das informações no ambiente digital, muitas vezes carecem da tecnologia e do conhecimento necessários para garantir essa proteção. Isso se torna evidente pelos inúmeros casos de vazamento de dados ocorridos no país, evidenciando a vulnerabilidade das informações no ambiente virtual.

Além disso, as leis atuais não conseguem proteger os usuários da internet contra ameaças imprevisíveis ou emergentes. Geralmente, as legislações são formuladas para responder a incidentes específicos já ocorridos, o que as torna incapazes de antecipar ou lidar com novas situações que surgem com a constante evolução tecnológica.

O Direito, por sua própria natureza, enfrenta desafios para acompanhar a rápida evolução da tecnologia, o que dificulta a tipificação de crimes que ainda não foram cometidos. Como resultado, os usuários da internet permanecem expostos a ameaças constantes.

Em síntese, a regulação da internet no Brasil é um desafio que demanda um esforço colaborativo entre diversas partes interessadas. É crucial a capacitação contínua dos profissionais de investigação criminal para que possam enfrentar a rápida evolução tecnológica e as constantes ameaças. Adicionalmente, é fundamental melhorar a infraestrutura tecnológica das empresas e órgãos públicos para garantir a

segurança das informações no ambiente digital. Esses são passos essenciais para assegurar uma navegação segura e eficaz na internet.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988.

Brasília, DF: Presidência da República, 1988. BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceitoderaça ou de cor. Brasília, DF: Presidência da República, 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 30 mar. 2024.

BRASIL. Lei nº 11.829, de 25 de novembro de 2008. Altera a Lei no 8.069, de 13 de julho de1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil [...]. Brasília, DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm.Acesso em: 15 mar. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, 28 direitos edeveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Brasília, 2021. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais(LGPD). Diário Oficial da União, Brasília, 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco civil da internet. Diário Oficial daUnião, Brasília, 2014.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012.Tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, 2012.

BRASIL. Código de Processo Penal Brasileiro: promulgado em 03 de outubro de 1941. Decreto-Leinº 3.689 de 1941.

BRASIL. Código Penal: promulgado em 7 de dezembro de 1940. Lei Nº 12.735, de 30 de novembro de 2012. BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: senado, 1988.

BRENE, Cleyson; LEPORE, Paulo. Manual do Delegado de Polícia Civil: Teoria e Prática.Salvador: Editora Juspodvim, 2017. ROCHA, Carolina Borges (2013). A

evolução criminológica do Direito Penal: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.

BRITO, Auriney. Direito penal informático. São Paulo: Saraiva, 2013. E-book. Disponível em: https://ler.amazon.com.br/?asin=B076C12MP9. Acesso em: 20 mar. 2024.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. Rio de Janeiro: Brasport, 2014. E-book. Disponível em: https://ler.amazon.com.br/?asin=B00ZQ0OP6E. Acesso em: 10 mar. 2024.

CAMARGO, Coriolano Almeida; SANTOS, Cleórbete. Direito Digital. 1. ed. São Paulo: Lumen Juris, 2018.

COSTA JR, Paulo José da. O Direito de Estar Só: tutela penal da intimidade. 4. ed. São Paulo: Editora Revista dos Tribunais, 2007.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011. Ebook. Disponível em: https://ler.amazon.com.br/?asin=B076C1914R. Acesso em: 10 mar. 2024.

GOMES, Luis Flavio. Lei "Carolina Dickman" e sua (in)eficácia. Jusbrasil, 2013. Disponívelem:https://professorlfg.jusbrasil.com.br/artigos/121931292/lei-carolina-dickman-e-sua-in-eficacia. Acesso em: 20 mar. 2024.

HARAKEMIW, Rafael Antônio; VIEIRA, Tiago Vidal. Crimes Cibernéticos. Anais do 2º Simpósio Sustentabilidade e Contemporaneidade nas Ciências Sociais, 2014.

MAUES, Gustavo Brandão Koury et al. Crimes virtuais: Uma análise sobre a adequação da legislação penal brasileira. Revista Cientificada FASETE, 2018.

QUINTINO, Eudes. A nova lei Carolina Dieckmann. Jusbrasil, 2013.

SANTOS, C.A.A.C. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico, 2009.

SILVA, Paulo Quintiliano. Crimes cibernéticos e seus efeitos internacionais. 2006. Disponível em: http://icofcs.org/2006/ICoFCS2006- pp02.pdf. Acesso em: 30 mai. 2024