**FACULDADE UNIFAMETRO MARACANAÚ**

**CURSO DE DIREITO**

**ANA JAMILA SOUSA FURTADO**

**THAYS SOARES BARBOSA**

# CRIMES VIRTUAIS NO BRASIL E A INVESTIGAÇÃO CRIMINAL

**MARACANAÚ – CE**

**2023**

**ANA JAMILA SOUSA FURTADO**

**THAYS SOARES BARBOSA**

# CRIMES VIRTUAIS NO BRASIL E A INVESTIGAÇÃO CRIMINAL

Artigo TCC apresentado ao curso de Direito da Faculdade Unifametro Maracanaú como requisito para a obtenção do grau de bacharel, sob a orientação do Prof. Me. Ismael Alves Lopes.

**MARACANAÚ – CE**

**2023**

ANA JAMILA SOUSA FURTADO
THAYS SOARES BARBOSA

# CRIMES VIRTUAIS NO BRASIL

Artigo de TCC apresentado no dia 18 de dezembro de 2023 ao Curso de Direito da Faculdade Unifametro Maracanaú, como requisito para obtenção do título em Bacharel em Direito, tendo sido aprovados pela banca examinadora composta pelos professores abaixo:

Maracanaú, 18 de dezembro de 2023.

**BANCA EXAMINADORA**

_____
Prof. Me. Ismael Alves Lopes
Orientador

_____
Profª. Me. Janaína da Silva Rabelo
Membro

_____
Profª. Me. Sylvana Rodrigues de Farias
Membro

# CRIMES VIRTUAIS NO BRASIL

Ana Jamila Sousa Furtado[1]
Thays Soares Barbosa[2]
Prof. Me. Ismael Alves Lopes[3]

## RESUMO

O presente estudo aborda a problemática dos crimes virtuais no Brasil, uma questão emergente devido ao crescente uso da Internet como plataforma de comunicação. Com a digitalização de inúmeros serviços, indivíduos se encontram vulneráveis à exposição de dados pessoais, o que potencializa o risco de tais informações serem acessadas por agentes mal-intencionados. A dificuldade em definir e classificar os crimes virtuais reside na sua natureza diversa e em constante evolução, desafiando assim os marcos legais existentes. Este trabalho tem como objetivo principal elucidar as condições necessárias para a condução de investigações policiais eficazes frente a esses delitos, bem como identificar os tipos de crimes mais recorrentes, as legislações aplicáveis e os recursos disponíveis aos profissionais da área. A metodologia adotada é de caráter descritivo, fundamentada em doutrinas, legislações vigentes e artigos científicos pertinentes ao tema. Como resultado, espera-se oferecer um panorama detalhado sobre o estado atual dos crimes virtuais no país, contribuindo assim para um melhor entendimento e preparo dos envolvidos na prevenção e combate a essas infrações. As conclusões apontam para a necessidade de uma constante atualização dos profissionais de segurança e do aparato legal, visando acompanhar a dinâmica dos crimes cibernéticos e garantir a proteção efetiva dos usuários da Internet.

**Palavras-chave:** crimes virtuais; legislação brasileira; segurança cibernética; investigação policial; proteção de dados.

[1] Graduanda do curso de Direito da Faculdade Unifametro Maracanaú.
[2] Graduanda do curso de Direito da Faculdade Unifametro Maracanaú.
[3] Professor do curso de Direito pela Faculdade Unifametro de Maracanaú.

## 1 INTRODUÇÃO

A internet, essa vasta rede que conecta o mundo, tem revolucionado a forma como interagimos e realizamos nossas atividades diárias. Com a evolução tecnológica, as distâncias entre as pessoas diminuíram, e uma miríade de oportunidades surgiu. Estamos conectados 24 horas por dia, e a maioria das nossas tarefas pode ser realizada na “palma da mão”, através da internet.

No entanto, essa evolução trouxe consigo o ônus da exposição nas redes sociais. Informações pessoais estão cada vez mais acessíveis, e os criminosos encontraram nesse meio um novo campo para suas ações nefastas. A investigação desses crimes cibernéticos apresenta desafios significativos, como identificar a origem da ação, o autor e o alcance do dano causado. Essas são questões cruciais que nossa polícia enfrenta ao tentar solucionar cada caso.

Diante desse cenário, emergem questionamentos pertinentes: Como os crimes se manifestam no ciberespaço? O ordenamento jurídico penal atual dispõe de normativas adequadas para proteger os bens jurídicos afetados pela cibercriminalidade? E o aparato policial, está preparado e qualificado para lidar com os crimes virtuais?

Atualmente, a sociedade está em alerta. Embora existam delegacias especializadas, muitos dos profissionais que nelas atuam não são especialistas em informática e carecem de conhecimento e ferramentas para combater a cibercriminalidade. A seleção desses profissionais, geralmente feita 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 evidentes. A internet, apesar de ser uma ferramenta transformadora, também tem sido associada ao crescimento dos crimes virtuais. Surge, portanto, a demanda por normas eficazes que possam punir os criminosos e diminuir a incidência desses delitos.

O objetivo deste artigo é analisar a tutela penal dos crimes virtuais, refletir sobre os desafios jurídicos impostos por essa nova manifestação da criminalidade, examinar as leis vigentes, 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 EVOLUÇÕES DA TECNOLOGIA E OS CRIMES VIRTUAIS

O mundo atual exige um acompanhamento cuidadoso das mudanças sociais por meio de leis, especialmente no campo em constante evolução da tecnologia da informação. Acontece que essa evolução abriu caminho para novas conquistas, assim como para novas ilegalidades. É nesse sentido que o objetivo da lei é criar barreiras sólidas contra os crimes virtuais. Atualmente, muitos brasileiros vivem e dependem de seus dispositivos digitais, armazenando ali dados e informações relacionadas à sua vida profissional e pessoal. Essas informações estão intimamente relacionadas aos seus proprietários (pessoas físicas, jurídicas, instituições bancárias, etc.) causando interesses para os criminosos. Segundo Coriolano Almeida Camargo e Cleórbete Santos, (Camargo; Santos, 2018, p.34):

> Os crimes mais comuns são cometidos contra o sistema financeiro, os crimes de phishing, que são furtos mediante fraude. Uma pessoa recebe uma mensagem falsa, via internet, ela clica no arquivo malicioso e importa um vírus para dentro da máquina. Por exemplo: 'você está sendo notificado porque a Polícia Federal está lhe investigando. Para saber mais detalhes sobre o processo, clique aqui: No momento em que você clica você importa o arquivo malicioso para dentro da sua máquina, ele vai fazer uma varredura, vai encontrar seus dados bancários e com esses dados ele vai retirar valores da sua conta corrente. Os criminosos descobriram que é muito melhor atacar o correntista, que é o polo mais fraco, do que atacar o polo mais forte, que é o banco. Então, é um crime que utiliza a boa fé, a distração do cliente, não é como o estelionato, em que você entrega espontaneamente as coisas. No furto mediante fraude, a distinção é que a pessoa usa sua distração, você pensa estar clicando em uma mensagem verdadeira - nesse momento é cometida a fraude e, depois, o furto. O furto mediante fraude, dentro do rol de crimes eletrônicos, já está tipificado, ou seja, não precisa de uma legislação para tipificar o furto mediante fraude, mas precisamos de uma legislação para tipificar outros delitos, por exemplo, invasões em portais, em sites, em bancos de dados. Existe uma corrente de juristas que entende que quando você congestiona um serviço público, já existe uma previsão penal por prejudicar o serviço de utilidade pública. Agora, se você prejudicar o serviço de utilidade pública pela internet, talvez você venha a acarretar um dano maior à sociedade. No caso, o delito poderia ser tipificado com uma pena talvez maior, porque as consequências para a sociedade também são mais nefastas. Tudo o que acontece no mundo virtual tem propagação nociva mais rápida, tanto para o bem como para o mal. A informação falsa circula mais rápido, e a verdadeira também, pelos meios eletrônicos.

É sabido que as atribuições da polícia judiciária foram descritas no artigo 144 da Constituição Federal Brasileira de 1988. A polícia é um órgão de direito público e criado para manter a paz e a segurança pública na sociedade. Desta forma, a

polícia tem duas funções, uma administrativa e outra judicial. Portanto, este tipo de ação é preventiva e repressiva, visando restringir, regular e fiscalizar os direitos e interesses dos cidadãos, e é uma instituição de direito público que visa manter a paz e a segurança pública na sociedade.

O artigo 144, parágrafo 4º, da Constituição Federal de 1988 estabelece que a Polícia Civil seja responsável e liderada por chefes de polícia, respeitando o trabalho com Polícia Federal e Militar, funções de polícia judiciária e investigações criminais. Sendo assim, as investigações policiais são importantes e determinarão a eficácia das investigações criminais. O cibercrime, em particular, traz particularidade à investigação. A polícia, tão claramente precisa usar recursos adequados, às vezes pode ser um obstáculo para elucidar esses crimes.

Outro ponto a ser discutido seria o destacado por Rocha (2013) no trecho transcrito abaixo:

> Estudiosos sobre o tema ainda afirmam que uma alteração no Código Penal não é conditio *sine qua non* para que se possa combater e coibir de forma eficaz os cibercrimes. O professor de Direito Penal da Faculdade Federal de Minas Gerais e Mestre em Ciências Penais pela UFMG Túlio Lima Vianna assevera que o nosso ordenamento não necessita de lei regulamentadoras e sim, um aparato técnico e específico nas investigações forenses por parte das polícias quanto a estes delitose uma ação conjunta entre os diversos entes que corporificam o Poder Judiciário e o Ministério Público. (Rocha, 2013, p.8).

Podemos pensar na Internet como a “mãe de todas” as redes porque conecta todos os computadores ao redor do mundo. Originou-se na década de 1960. A Internet chegou ao Brasil em 1992, conectando inicialmente grandes universidades. Na época, era usado apenas para troca de e-mails. Em 1995, a Internet começou a ser utilizada comercialmente no país. No mesmo ano, foi criado o Conselho Governador da Internet no Brasil (CGI.br), responsável por garantir a qualidade técnica da Internet do país e divulgar os serviços prestados.

A Internet mudou a forma como as pessoas compartilham informações. No passado, o acesso à Internet era lento e caro, o que limitava a sua utilização. Com o advento das redes de banda larga, 3G, 4G e 5G e a queda dos preços, cada vez mais pessoas têm acesso à internet. Essa mudança permite que as pessoas acessem uma variedade de informações de forma rápida e eficiente. Elas podem se comunicar com pessoas de todo o mundo, assistir vídeos, ouvir música, ler

notícias e fazer compras online.

Nesta esteira, Marcelo Crespo aduz:

> 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 constituíram como nervos da sociedade, que cada vez mais depende dos computadores e das intranets (redes internas de cada corporação). (Crespo, 2011, p. 368).

A evolução tecnológica tem levado a sociedade a uma nova era, a sociedade da informação. Nesse contexto, os sistemas de defesa passaram a depender cada vez mais da informática. Isso ocorre porque a internet, por um lado, trouxe importantes avanços no compartilhamento de informações, mas, por outro, também trouxe grandes ameaçasdevido ao seu uso indevido.

## 2.1 A INTERNET NO DIREITO

A relação entre Direito e Informática vem se tornando cada vez mais estreita. Com o avanço da tecnologia, novas formas de crime e de violação de direitos surgem a todo o momento. Por isso, é necessário que o Direito se adeque às novas realidades, para garantir a justiça e a segurança da sociedade. Alguns especialistas defendem a criação de um novo ramo do Direito para tratar especificamente das questões relacionadas à Informática. Essa nova área do Direito seria responsável por regulamentar o uso das tecnologias e punir os crimes cometidos por meio delas. Independentemente de se criar um novo ramo do Direito ou não, é fundamental que o Direito tradicional se atualize para acompanhar as mudanças tecnológicas. O Direito deve ser capaz de proteger os direitos dos cidadãos, mesmo quando esses direitos são violados por meio da tecnologia.

Nesse sentido, esclarece Miguel Reale “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).

Segundo Pinheiro (2016, p. 77), o Direito Digital nada mais é do que o aperfeiçoamento do próprio Direito, pois, além de englobar seus princípios fundamentais, ainda fornece novas ideias e perspectivas ao pensamento jurídico

como um todo (Direito Civil, Autoral, Econômico, Penal, Tributário, etc.). O Direito Digital deve ser aprofundado para fornecer novas ferramentas aptas para satisfazer seus anseios.

Sobre estes anseios, Patrícia Pinheiro aduz:

> [...] 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 estraté gicas, dos processos contra hackers e muito mais. (Pinheiro, 2016, p. 77).

Na visão de Crespo (2011, p. 543), considerando o Direito Penal e sua relação com a informática, também se faz necessário debater sobre quesitos como harmonização internacional, lugar do crime, spam, estelionato, acesso a sistemas, legítima defesa, vírus, engenharia social, entre outros.

Essas novas ameaças que até então não eram conhecidas pelo Direito vieram a ocasionar conflitos. Tais ameaças apresentam eventos nos quais a vítima é a coletividade em geral, e não os bens jurídicos clássicos, tais como a vida e o patrimônio, sendo o mesmo caso de atentados à ordem econômica e o meio ambiente, que são bens jurídicos supraindividuais, na qual sua propriedade pertence à coletividade. Ou seja, ao mesmo passo que a internet foi de suma importância para o desenvolvimento econômico, também é incumbida por estipular novos contratos sociais que constituíram novos conflitos em uma nova área criminal. (Brito, 2013, p. 185).

Para Pinheiro (2016, p. 78), não existe e nem deve ser criado o “Direito da Internet”, visto que ao longo da historia houve outros veículos de comunicação que vieram a ter relevância jurídica, como a televisão, o telefone, o rádio, etc. Existem peculiaridades na internet que devem ser incorporadas pelas diferentes áreas do Direito, porém sem necessidade de um Direito específico. A evolução tecnológica é sempre mais rápida que a legislativa, por isso os princípios devem se sobressair em relação às 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. No entanto, elas também trouxeram um lado sombrio, que é o aumento da criminalidade virtual. Com o avanço

da tecnologia, novas formas de crime surgem a todo o momento. Crimes como o cyberbullying, o roubo de dados e o terrorismo digital são cada vez mais comuns. Esses crimes são cometidos por pessoas de má índole que querem prejudicar outras pessoas ou a sociedade como um todo.

É importante estar ciente do lado sombrio da tecnologia para se proteger. É preciso tomar medidas para se proteger de crimes virtuais, como usar senhas fortes, instalar antivírus e softwares de segurança, e não abrir e-mails ou arquivos suspeitos.

## 3 LEGISLAÇÕES PENAIS NO ÂMBITO DIGITAL

É útil que, como afirmado anteriormente, sobre a questão principal da investigação policial, estará relacionado ao desenvolvimento tecnológico, que exigem profissionais e especialização da área, também leva em consideração a existência de proteção penal excessiva. Até o ano de 2012 a legislação pátria era omissa quanto à tipificação dos delitos que ocorriam por utilização do meio internet. Em obediência ao previsto no artigo 5º, XXXIX, Constituição Federal de 1988, o princípio da legalidade, os delitos assim cometidos não poderiam ser repreendidos, se não devidamente tipificados em Lei. Em razão da imprevisão de regramentos específicos, a disseminação de tais condutos foi rápida e diversificada. A lacuna deixada pelo rastro da internet instalou discussões acerca da necessidade de o ordenamento jurídico atentar as novas condutas realizadas pelos meios informáticos. Tal debate acalorou-se com a repercussão do episódio ocorrido com uma figura pública, a atriz Carolina Diekmann, em que esta teve vazado por meio de invasão do seu computador fotos intima.

A falta de leis específicas para crimes virtuais no Brasil é um desafio antigo, pois o Código Penal é de 1940, quando a internet ainda não existia. Além disso, o direito deve proteger os bens mais importantes da sociedade, mas interferir o mínimo possível na vida dos cidadãos. Por isso, foi difícil criar leis que tipificassem crimes virtuais sem ferir esses princípios. Os crimes virtuais são uma ameaça crescente à sociedade, mas o Brasil enfrenta desafios para combatê-los. A aprovação de leis específicas para crimes virtuais é um passo importante para enfrentar esse desafio. (Milagre, 2016, p. 47).

A aprovação de leis específicas para crimes virtuais era inevitável, pois o ambiente digital é um espaço de constante troca de informações, de todas as esferas da sociedade.Desde conversas cotidianas até transações financeiras, tudo é realizado por meio da redeinformática.

Ainda de acordo com Milagre (2016, p. 48), mesmo com tais fatos, havia certa reprovação no que tange a uma legislação informática específica, e foi necessário que uma pessoa pública famosa fosse constrangida com suposto crime virtual para que finalizassem uma demanda que estava há mais de dez anos no Congresso Nacional. O suposto crime aconteceu com a atriz Carolina Dieckmann, e a Lei n.° 12.737/2012, que leva seu nome, foi sancionada em novembro desse mesmo ano. Os crimes virtuais não se limitam aos bens jurídicos tradicionais, como o patrimônio e a vida. Os criminosos também visam os sistemas, as informações e outros bens que são exclusivos do ambiente digital. Por isso, é necessária uma legislação específica para esses crimes.

Segundo Brito (2013, p. 780) expõem, os crimes virtuais são pluriofensivos, pois da mesma maneira que precisam de resguardo de bens jurídicos tradicionais, concomitantemente precisam de resguardos que advém da sociedade da informação.Ou seja, não é certo atrelar somente o meio pelo qual se comete a ação, tendo que se criar em torno da pretensão dainformação como bem a ser amparado.

## 3.1 O CÓDIGO PENAL

O texto altera o Código Penal para aumentar as penas por invasão de aparelho, furto qualificado e apropriação indébita que ocorram em meio digital, conectado ou não à Internet.

O crime de invasão de dispositivo, bem como alteração ou destruição de dados e instalação de vírus (malware) para obtenção ilícita, passa a ser punido com pena de prisão de 1 a 4 anos e multa, sendo o motivo agravado em um terço. Perda econômica, então aumentou para dois terços. Penas anteriores previam apenas três meses a um ano de detenção. Dois a cinco anos de prisão e multa por obter "comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais ou controle remoto não autorizado de equipamentos

comprometidos". Antes de a lei ser alterada, a multa era de seis meses a dois anos.

Sendo assim, a própria Lei n.º 12.735/2012 expressa em seu artigo 4º 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.° 12.737/12)

A Lei n.° 12.737/12, sancionada neste mesmo ano, teve seu nome associado à atriz Carolina Dieckmann, devido ao fato do escândalo ocorrido após a atriz ter seu dispositivo invadido e os criminosos terem divulgado fotos íntimas na internet.

Na oportunidade, os criminosos acessaram sua conta de e-mail e conseguiram visualizar as imagens. Após conseguirem as imagens, começaram a chantageá-la para que pagasse certa quantia em dinheiro para que não tivesse sua intimidade exposta. Por não ter legislação específica na época, os criminosos foram condenados por extorsão, furto e difamação, porém ficaram isentos da invasão do dispositivo, por não haver tipificação à época. Por tal fato ter sido extensamente difundido na mídia, ocasionou-se uma pressão muito forte para que alguma legislação surgisse no que tange os delitos informáticos, e foi assim que aprovou o PL n.° 35/2012, originado pelo PL n.° 2.793/2011. Foi a primeira lei do ordenamento jurídico brasileiro a tratar dos crimes cometidosatravés da internet. Especificamente o dispositivo 154-A do Código Penal Brasileiro, o qual tipifica a conduta de:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidasem lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constituicrime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dadosou informações obtidos.

> § 5º Aumenta-se a pena 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; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipalou do Distrito Federa. (Brasil, 1940, online)

Os principais objetos jurídicos a serem tutelados no artigo 154-A são: a segurança dos aparelhos eletrônicos, a privacidade e a liberdade individual do indivíduo. Além disso,só há crime se a conduta incidir em dispositivo alheio. É crime comum e pode ser praticado por qualquer cidadão. A vítima pode ser qualquer pessoa, tanto física quanto jurídica. Para que seja consumado, não basta invadir o dispositivo alheio, é preciso obter, alterar ou excluir os dados sem o consentimento do seu titular, ou buscar obter vantagem ilícita (favores sexuais, dinheiro, etc.). A ação penal é pública condicionada à representação, a não ser quando envolver a administração pública. Nesse caso, a ação será pública incondicionada, conforme o artigo 154- B do Código Penal (Masson, 2015, p. 277):

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se 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 Municípiosou contra empresas concessionárias de serviços públicos.

Caso o delito seja consumado, pode ser que ocorra a agravação da pena caso a conduta esteja tipificada nas causas de aumento, de acordo com os parágrafos 2º e 4º, ecaso verifique-se um crime mais grave incide no parágrafo 3º do artigo 154-A do CP.

Tal lei também tratou de tipificar um dos delitos mais cometidos na internet, que é a indisponibilização dos serviços por meio de ataques de negação de serviços. Tais ataques tiram a própria internet do ar para que os usuários legítimos não consigam se conectar à rede. Aqui não é uma invasão do sistema, mas sim uma sobrecarga nos servidores. A Lei n.° 12.737/12 complementou o artigo 266 do Código Penal, pois este não tratava dos ataques que abarcam asinterrupções.

> Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena – detenção, de 1 (um) a 3 (três) anos, e multa.
> § 1° Incorre na mesma pena quem interrompe serviço telemá tico ou de

> informa- ção de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2° Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamida- de pública.

Além do mais, a Lei Carolina Dieckmann complementou a redação do artigo 298 do Código Penal, que trata da falsificação ou alteração de documento particular, equiparandodocumento particular a cartões, tanto de débito quanto de crédito.

> Art.298. Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro.
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o carta de crédito ou débito.

Resumem os seguintes autores:

> A Lei 12.737/12 introduziu no ordenamento jurídico 3 tipificações penais no Código Penal: o artigo 154- A que versa sobre a invasão de dispositivo informático alheio, o artigo 266, §1º e 2º que fala sobre a interrupção ou perturbação de serviço telefônico, telegráfico, informático, telemático ou de informação de utilidade pública, artigo 298,§ único, que tipifica falsificação de cartão de crédito ou débito (Maues, Duarte, Carvalho, 2018, p.173).
> A nova Lei ainda alterou a redação do artigo 266 do Código Penal, que acrescentou ao crime de “interrupção ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento”, o parágrafo 1° que dispõe que incorrerá na mesma pena aquele que interrompe serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar- lhe o restabelecimento, bem como também acrescentou ao artigo 298 o parágrafo único, o qual dispõe que para fins de falsificação ou alteração, equiparasse o documento particular o cartão de crédito (Harakemiv; Vieira; 2014, p. 425)

A aprovação da Lei n.° 12.737/2012, que tipifica o crime de invasão de dispositivo informático, foi um passo importante para a proteção da privacidade no ambiente digital. No entanto, a lei apresenta algumas lacunas e inconsistências que podem comprometer sua eficácia. Um exemplo é a necessidade de violação de mecanismo de segurança para a configuração do crime. Isso significa que, se uma pessoa obtém ou exclui informações pessoais de um dispositivo eletrônico com o consentimento do proprietário, não será responsabilizada penalmente.

Essa lacuna é preocupante, pois permite que criminosos acessem dados pessoais sem serem punidos. Além disso, a definição de "mecanismo de segurança" é bastante ampla, o que pode gerar interpretações divergentes. Outro problema da lei é que ela não considera a falta de conhecimento dos usuários sobre segurança digital. Muitas pessoas não sabem que precisam usar senhas fortes,

instalar antivírus e outros softwares de segurança. Isso pode dificultar a aplicação da lei, pois os usuários podem argumentar que não tinham conhecimento de que estavam violando a lei.

Em suma, a Lei n.° 12.737/2012 é um avanço importante, mas ainda precisa ser aperfeiçoada para garantir a sua eficácia. A lei é enfraquecida por permitir que os criminosos invadam dispositivos alheios sem serem punidos. Isso ocorre porque a lei não considera todas as formas de invasão, como aquelas que não violam mecanismos de segurança. Como resultado, a lei não cumpre seu objetivo de proteger a privacidade e a segurança dos usuários.

Tanto é que, na visão de Luis Flávio Gomes, além de a lei permitir múltiplas interpretações, a mesma não é eficaz quanto sua função preventiva:

> De qualquer modo, houve intenção de se suprir uma lacuna no Brasil. O relator do projeto, deputado Paulo Teixeira, procurou fazer o melhor texto, mas todo conjunto de palavras permitem mil interpretações. Numa rápida olhada assinalei 104 conceitos dados pela lei, todos dependentes de interpretação. As penas são baixas (em regra, até dois anos), logo, a chance de prescrição é muito grande. Por todos esses motivos, nãoconfio na eficácia preventiva dessa lei. (Gomes, 2013).

## 3.3 MARCO CIVIL DA INTERNET (LEI N.° 12.965/2014)

A chegada da internet trouxe uma nova realidade para a sociedade, e o direito penal precisou se adaptar para lidar com os crimes praticados no ambiente digital. Esses crimes, principalmente quando a vítima é uma pessoa ou ente público, têm grande repercussão social, e por isso são motivo de preocupação da sociedade e dos profissionais do direito. A partir dessa preocupação, começaram-se a discutir quais são os direitos e deveres dos usuários da internet. O objetivo é definir o que é permitido e o que é proibido no ambiente digital. (Marcacini, 2016, p. 727).

O Marco Civil ocorreu com A Lei n.° 12.965/2014, promulgada em 2014, conhecida como Marco Civil da Internet, surgiu para regulamentar os direitos e obrigações dos internautas. O Marco Civil tornou-se uma ferramenta essencial para proteger os dados dos internautas, garantindo que os usuários só possam acessar informações e conteúdos privados em sites e redes sociais por ordem judicial. A lei também regulamenta a possibilidade de retirar do ar conteúdos, sejam eles, ofensivos, violentos ou pornográficos. Além da pornografia de vingança que pode ser retirada do ar por meio de solicitação da vítima diretamente ao site que

hospeda o conteúdo, outros casos exigem ordem judicial e avaliação para serem retirados da web.

É importante ressaltar que o Marco Civil da Internet não dispõe de tipos penais. A lei visa regular a utilização da internet no país através de seus princípios, e tambémdireciona as instruções para que o Estado possa atuar.

A Lei n.° 12.965/14 tem seus pilares elencados em seu artigo 3º:

> Art. 3 A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I- garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II- proteção da privacidade;
> III- proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V- preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de 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 conflitem com os demais princípios estabelecidos nesta Lei.

A neutralidade da rede garante que todos os usuários da internet tenham acesso a qualquer tipo de conteúdo, independentemente do provedor ou do plano de assinatura contratado. Isso significa que os provedores não podem cobrar taxas extras 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 elas não podem cobrar mais pelos serviços mais populares. Já os defensores da neutralidade da rede afirmam que ela é essencial para garantir a liberdade de expressão e o acesso à informação, independentementeda classe social. (Santino, 2014)

A lei garante a privacidade dos usuários da internet. Os provedores devem armazenar os dados de conexão por um ano em um ambiente seguro. Eles só podem compartilhar esses dados com terceiros com uma ordem judicial. As informações que os usuários compartilham na internet não podem ser usadas para outros fins que não sejam aqueles para os quais foram originalmente coletadas. Isso porque esses dados podem ser facilmente armazenados e vendidos para outras finalidades.

A lei também garante que os provedores não têm responsabilidade alguma sobre o que seus usuários postam ou fazem em ambiente virtual, a fim de coibir a censuracaso estes fossem corresponsáveis. Quem postar conteúdo ofensivo carece do direito ao contraditório, a não ser que o teor das postagens fira algum tipo penal, como pornografia infantil, racismo, etc. (Amaral, 2016).

Antigamente, era difícil para uma pessoa comum se comunicar com um grande público. Para isso, era preciso ter acesso a equipamentos caros e sofisticados, como gráficas, rádios e TVs. Com a internet, isso mudou. Qualquer pessoa com um celular simples e barato pode se expressar para o mundo todo. Por isso, é importante que existam leis que garantam o direito à liberdade de expressão na internet. O Marco Civil da Internet é uma importante conquista para a democracia e a liberdade de expressão no Brasil. A lei garante que todos os usuários da internet tenham acesso às informações e possam se expressar livremente, sem censura ou discriminação.

## 3.4 PROJETOS DE LEI

Como o tema é relativamente novo, é necessário atualizar a legislação para preencher as lacunas existentes. Nesse sentido, há alguns projetos de lei interessantes em tramitação, que veremos a seguir. Projetos de lei buscam proteger mulheres e usuários da internet. Três projetos de lei em tramitação no Congresso Nacional buscam proteger mulheres e usuários da internet.

Invasão de privacidade feminina como violência doméstica. O PL n.° 5555/2013, do deputado federal João Arruda (PSD-PR), identifica a invasão da privacidade feminina como um tipo de violência doméstica e familiar. O projeto altera a Lei Maria da Penha e tipifica a exposição pública da intimidade da mulher, como pornografia de vingança ou *revenge porn*. O projeto foi aprovado pela Câmara dos Deputados sem objeções e agora segue para o Senado Federal. Se aprovado, será sancionado pelo presidente da República.

Conteúdos que incitam o suicídio. O PL n.° 6989/2017, também do deputado federal João Arruda, altera o artigo 12 do Marco Civil da Internet para introduzir mecanismo de exclusão de conteúdos que incitam o suicídio.

De acordo com o deputado, “a liberdade de expressão é a regra, mas a

proteção da vida humana é uma exceção pela qual vale a pena estabelecer um regramento protetor mais incisivo".

Agravante genérica para crimes cometidos na internet. O PL n.° 154/2019, do deputado federal José Nelto (Podemos-GO), altera o Código Penal, estabelecendo o cometimento de crimes mediante ou contra dispositivos eletrônicos, que podem ou não estar conectados à internet, como agravante genérica no referido código. A proposta visa aumentar a punição para crimes cometidos na internet, como cyberbullying, crimes deódio e crimes contra a honra.

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) surge para regulamentar à coleta e o tratamento de dados pessoais, alterando os artigos 7º e 16 do Marco Civil da Internet. Em outras palavras, a LGPD visa proteger a captura, armazenamento e compartilhamento de dados pessoais coletados por sites e empresas online na tentativa de criar um ambiente digital mais seguro.

A mais recente legislação sobre crimes cibernéticos é a Lei n.º 14.155/2021, derivada da Lei n.º 4.554/2020 (PL) aprovada pelo Senado no ano passado.

## 4 CRIMES VIRTUAIS

O crime virtual, também conhecido como crime cibernético, crime tecnológico, crime informático, crime informático ou crime de informação, é um comportamento prejudicial cometido através de dispositivos eletrónicos ou contra sistemas informáticos. Podem ter como alvo indivíduos, empresas ou instituições públicas. No Brasil, os crimes virtuais mais comuns são: fraudes, roubo de dados e ataques cibernéticos. Outros crimes virtuais que podem ser cometidos incluem pornografia infantil, discriminação racial ou religiosa, apoio ao crime ou terrorismo.

Como conceitua Tarcísio Teixeira, "[...] crime de informática é aquele que, quando praticado, utiliza-se de meios informáticos como instrumento de alcance ao resultado pretendido, e também aquele praticado contra os sistemas e meios informáticos." (Teixeira,2018, p. 505-506).

Tais más condutas podem ser divididas em "crimes cibernéticos" e "condutas prejudiciais atípicas". "Comportamento lesivo atípico" refere-se ao comportamento que causa dano à vítima, mas não possui classificação criminal e o autor não pode

ser punido dentro da categoria criminal. O "crime cibernético" pode ser "evidente" (inadequado) ou "totalmente cibercrime" (legítimo). "Aberto" refere-se ao conteúdo que pode ser enviado com ou sem computador e é apenas um meio de aplicação. Portanto, há uma distinção entre crimes “somente cibernéticos” porque eles só podem ser cometidos através de um computador ou outro dispositivo eletrônico com acesso à Internet.

Os crimes cibernéticos abertos podem ser divididos em três tipos: crimes puros, comuns e mistos. Crimes puros: são aqueles que ocorrem exclusivamente no ambiente virtual, utilizando dispositivos eletrônicos. Exemplos: invasão de dispositivo informático, furto de dados, pornografia infantil. Crimes comuns: são aqueles que podem ocorrer tanto no ambiente virtual quanto no ambiente físico. Exemplos: estelionato, ameaça, difamação. Crimes mistos: são aqueles que utilizam o ambiente virtual como meio para a prática de um crime que também pode ser cometido no ambiente físico. Exemplos: fraude eletrônica, chantagem, tráfico de drogas.

Os crimes puros são os mais difíceis de investigar e punir porque os criminosos podem cometer crimes anonimamente e são difíceis de identificar. Os crimes comuns são mais fáceis de investigar e punir porque os criminosos podem ser identificados e localizados no ambiente físico. Os crimes híbridos são uma combinação dos dois primeiros tipos. Podem ser mais difíceis de investigar e punir porque os criminosos podem operar anonimamente em ambientes virtuais, enquanto a identificação é difícil em ambientes físicos.

Um estudo recente realizado pela SaferNet Brasil juntamente com o Ministério Público Federal (MPF) constatou que ao menos 366 (trezentos e sessenta e seis) crimes cibernéticos são registrados diariamente apenas no Brasil. A maior recorrência refere-se à pornografia infantil, seguido de 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 frequentes. Isso ocorre por dois motivos principais: Falsa sensação de anonimato: Os criminosos acreditam que podem agir impunemente na internet, pois não são facilmente identificados. Falta de cuidado dos usuários: Muitas pessoas não têm consciência dos riscos de inserir

seus dados pessoais na internet.

A falsa sensação de anonimato é um problema real. A internet é um ambiente anônimo para muitos usuários, o que facilita a prática de crimes. Os criminosos podemse esconder atrás de perfis falsos e cometer crimes sem serem identificados.

A falta de cuidado dos usuários também é um fator importante para o aumento dos crimes virtuais. Muitas pessoas não têm consciência dos riscos de inserir seus dados pessoais na internet. Elas podem fornecer dados como nome, endereço, número de telefone e cartão de crédito em sites e aplicativos que não são confiáveis.

## 4.1 PORNOGRÁFIA INFANTIL

Moisés Cassanti cita:

> Consiste em produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da web, e-mails, newsgroups, salas de bate-papo (chat), ou qualquer outra forma. Compreende, ainda, o uso da internet com a finalidade de aliciar crianças ou adolescentes para realizarem atividades sexuais ou para se exporem de forma pornográfica. (Cassanti, 2014, p. 40).

O crime de pornografia infantil efetuado através da internet aponta algumas características próprias, pois isenta o contato físico entre os envolvidos, bastando capturas fotos da criança ou do adolescente, dando-lhe conotação pornográfica para queo crime esteja consumado. Pode ocorrer também o contato em ambiente virtual entre vitima e abusador, e quando a vitima se nega a fazer o que o abusador manda, geralmente é ameaçada de que terá seu conteúdo divulgado, e, por medo, acabafazendo o que o abusador quer (Silva; Veronese, 2009).

Não podemos confundir pedofilia com pornografia infantil. A pornografia infantil está prevista no Estatuto da Criança e do Adolescente (ECA), Lei n.° 8.069, e a pedofilia é uma doença em que a pessoa sente atração por crianças. A pedofilia torna o criminoso inimputável ou semi-inimputável, e a internet é um meio dos portadores dessa doença satisfazerem digitalmente suas vontades. Na pornografia infantil, os donos dos sites recebem dinheiro dos usuários em troca de vídeos e imagens. Já na pedofilia, as redes são visitadas e alimentadas por pedófilos. Por fim, o acervo é compartilhado diretamente via e-mail ou outras formas. (Teixeira, 2018, p. 513-514).

Não podemos confundir pedofilia com pornografia infantil. A pornografia infantil é regida pelo Estatuto da Criança e do Adolescente (ECA), Lei n.° 8.069, pedofilia é um transtorno no qual uma pessoa sente atração por crianças. A pedofilia torna os criminosos inimputável ou semi-inimputável, e a internet é uma forma de as pessoas com o transtorno realizarem seus desejos digitalmente. Na pornografia infantil, os proprietários de sites coletam dinheiro dos usuários por meio de vídeos e imagens. Na pedofilia, a Internet é acessada e alimentada por pedófilos. Por fim, o acervo é compartilhado diretamente via e-mail ou outras formas. (Teixeira, 2018, p. 513-514).

A Lei n.° 11.829/2008 incluiu o artigo 241-A no 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.
> § 1° Nas mesmas penas incorre quem:
> 4.1.1. – assegura os meios ou serviços para o armazenamento das fotografias,cenas ou imagens de que trata o caput deste artigo;
> 4.1.2. – assegura, por qualquer meio, o acesso por rede de computadores àsfotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2° As condutas tipificadas nos incisos I e II do
> § 1° deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito deque trata o caput deste artigo.

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

## 4.2 CRIMES CONTRA A HONRA

A internet é um espaço de grande diversidade de opiniões, o que é positivo. No entanto, é importante lembrar que comentários ofensivos podem gerar responsabilização. A liberdade de expressão é um direito fundamental, mas não deveser confundida com o direito de ofender. Comentários ofensivos podem causar

danos psicológicos, morais e até financeiros às vítimas. Por isso, é importante refletir antes de publicar qualquer comentário na internet. Lembre-se de que suas palavras podem ter consequências.

Guilherme Nucci conceitua honra: “É a faculdade de apreciação ou o senso que se faz acerca da autoridade moral de uma pessoa, consistente na sua honestidade, no seu bom comportamento, na sua respeitabilidade no seio social, na sua correção moral; enfim, na sua postura calcada nos bons costumes.” (Nucci, 2018, p. 211).

Existem três tipos de crimes contra a honra: Calúnia, difamação e injúria, todos previstos no Código Penal Brasileiro:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime. Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação.
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.

De acordo com Campanhola (2018), se a difamação ocorrer por e-mail, cada pessoa que receber e compartilhar o e-mail poderá ser acusada de ser coautora. No caso de difamação, é necessária retratação pública se houver arrependimento. Um insulto é uma acusação de comportamento ofensivo à imagem de outra pessoa. Também é bastante comum o crime de racismo, que tem previsão legal 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 reclusão de 1 a 3 anos e multa. Porém, se for praticado 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 alguém engana outra pessoa para obter algum tipo de vantagem, como dinheiro, bens ou serviços. O crime de estelionato se diferencia de outros crimes por sua base no engano. O estelionatário induz a vítima a erro, fazendo-a acreditar em algo que não é verdade. Por isso, o estelionato é um crime que causa grande prejuízo às vítimas, tanto material quanto moral.

Para que seja configurado o estelionato, é necessário o emprego de método fraudulento, induzir ao erro a vítima, e obrigatoriamente deve haver o duplo

resultado, que é a vantagem ilícita do agente e o prejuízo alheio associado à fraude que este provocou (Delmanto, 2016, p. 622).

No meio digital, o golpe pode começar com a criação de um site enganoso que oferece prováveis benefícios às vítimas, tais como links patrocinados, comunicados pelo *whatsapp*, posts no Facebook, na maioria das vezes se passando por alguma empresa.A partir daí, o estelionatário contata as vitimas e dá inicio ao golpe, fazendo transparecer que aquele será um ótimo negócio e uma oportunidade única. Após conseguirem o dinheiro das vítimas o golpista some, e só aí que estes vão perceber que tudo não passava de um golpe (Bernal, 2019).

Outra maneira bastante usual que caracteriza o estelionato na internet é através da invasão da caixa de e-mails das vítimas, em especial as que sempre costumam utilizar o *internet banking*. Nesse episódio, o estelionatário consegue clonar a página de um bancoe fazer com que o usuário insira sua senha imaginando que está em um ambiente seguro, pois o site é idêntico ao que ele está acostumado (Inellas, 2009).

## 4.4 INVASÃO DE PRIVACIDADE

A privacidade é um direito fundamental que garante às pessoas o direito de serem deixadas em paz, sem que suas informações pessoais sejam divulgadas sem o seu consentimento. Na sociedade contemporânea, a internet tornou mais fácil a coleta e a disseminação de informações pessoais. Isso pode levar à violação da privacidade das pessoas, com consequências negativas para sua vida pessoal e profissional. Por isso, é importante que as pessoas estejam cientes dos riscos à sua privacidade na internet e tomem medidas para protegê-la, é um quesito de extrema importância, sendo considerado um direito fundamental, e sua violação é vedada pelo artigo 5º, inciso X da Constituição Federal de 1998:

> Art. 5° Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito àvida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas,assegurado o direito a indenização pelo dano material ou moral decorrente de suaviolação;

O crime de invasão de privacidade na internet é cometido quando alguém

acessa informações ou dados pessoais de outra pessoa sem o seu consentimento. Esse crime pode ser cometido de diversas formas, como por meio de senhas roubadas, vírus ou softwares maliciosos. As consequências desse crime podem ser graves, como prejuízos financeiros, danos morais e até mesmo a prisão.

De acordo com Sydow (2015, p. 115), grande parcela dos sistemas operacionais que são difundidos no mercado apresentam “bugs”, que são erros de programação. Esses erros podem ocasionar algumas brechas no sistema que podem levar intrusos a acessarinformações de outrem que podem ser utilizadas para qualquer finalidade. Não obstante, além disso, criminosos também podem induzir as vítimas a instalarem programas que infectam seus dispositivos e abrem portas de entrada para que estes possam adentrar no sistema.

Tais condutas estão tipificadas no artigo 154-A do Código Penal, através da Lei n.º 12.737/2012:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - detenção, de 3 (três) mesesa 1 (um) ano, e multa.

Mesmo que haja o consentimento do dono do dispositivo para que determinada pessoapossa acessar seu aparelho, tal pessoa pode acabar divulgando informações sem autorização para terceiros.

Um fato que merece destaque, pois acontece frequentemente em nossa sociedade atual, principalmente com as mulheres, é a *revenge porn*, ou pornografia da vingança, que ocorre quando suas intimidades sexuais, enviadas aos parceiros românticos, são impropriamente publicadas em sites, redes sociais e aplicativos como o Whatsapp e Messenger sem seu consentimento. E uma vez que esses arquivos vão parar na internet, é muito difícil retirá-los, pois são compartilhados rapidamente e o controle de sua divulgação é dificultado, constituindodanos de árdua reparação.

É claro que o *revenge porn* acontecia antes da existência dos aplicativos e das redes sociais, porém tal ato ganhou dimensões imensuráveis devido à rapidez com que são compartilhados tais conteúdos, somados à difícil remoção dos mesmos uma vez queeles caemna rede.

Como bem ressalva Paulo José da Costa Jr:

> [...] para que se pudesse falar de intrusão, seria necessário que existisse, anteriormente, um momento de ilicitude, o que não se configura. O extraneus foi trazido para a vida privada pelo seu legítimo titular, que dela podia livremente dispor. Não houve, pois, invasão. Adquiriu o terceiro legitimamente os segredos que lhe foram confiados. Sem fraude, sem captação irregular. No momento ulterior, abusou da confiança depositada, divulgando as intimidades reveladas. Faz-se mister distinguir ambas as hipóteses. Numa, a intimidade é agredida, porque violada. Noutra, a intimidade é lesada, porque divulgada. (Costa Jr, 2007, p.26).

No primeiro caso, a obtenção dos arquivos não é legítima. No segundo caso, apesar da obtenção legítima das informações, sua exposição é ilícita. Sendo assim, no primeiro caso, a ofensa atua de dentro para fora, e, no segundo, de fora para dentro.

Conquanto temos a preservação da intimidade por meios digitais (artigo 154-A, que tipifica o crime de invasão de dispositivo informático), agora também temos amparo penal por propagação indevida da intimidade, mesmo que diretamente confiados. O que antes era considerado como injúria (ofendendo a dignidade) ou difamação (acusando de fato ofensivo à reputação), hoje está tipificado no Artigo 218-C do Código Penal, através da Lei n.° 13.718/18:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: (Incluído pela Lei nº 13.718, de 2018)
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.(Incluído pela Lei nº 13.718, de 2018)
> Aumento de pena (Incluído pela Lei nº 13.718, de 2018)
> § 1 A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação. (Incluído pela Lei nº 13.718, de 2018). (Brasil, 1940, online)

Além da coleta de dados pessoais nas redes sociais, existe outro tipo de captação de dados que invade a privacidade dos usuários da rede. Portais, provedores de e-mail e outras empresas coletam informações sobre os interesses, atividades e hábitos dos usuários na internet para enviar anúncios personalizados. É comum ver propagandas de produtos que pesquisamos recentemente ou até de coisas que falamos perto de nossos smartphones.

De acordo com Teixeira (2018, p. 86), a privacidade é invadida facilmente

como consequência da descontrolada captação de dados, que podem ser comercializados com base no perfil dos usuários, criando a possibilidade de destiná-los incontáveis mensagens e propagandas, sem levar em consideração os danos causados aos internautas, deixando claras as consequências jurídicas causadas por esse fato. A ocorrência de episódios recentes, como vazamentos de dados e uso indevido de informações pessoais, gera incertezas jurídicas sobre o uso da internet e a proteção dos dados dos usuários.

## 4.5 A NECESSIDADE DE CAPACITAÇÃO DOS PROFISSIONAIS CONTRA OS CRIMES VIRTUAIS

Sendo assim, a própria Lei n.º 12.735/2012 expressa em seu artigo 4º 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”. Pois bem, a melhora da prestação do serviço à sociedade vai além da melhora dos recursos estatais, de infraestrutura: é necessário o investimento em conhecimento especializado na área, inclusive de profissionais na área de informática, na prática, pois não basta o somente a esfera penal. Anteriormente as tipificações já se tornavam difíceis às investigações, e na atualidade, a dificuldade continua na destreza que a área requer. É certo que pela evolução da prática e crimes virtuais e o próprio desenvolvimento das investigações tem-se como principal consideração a necessidade de capacitação dos profissionais. Ainda, aponta-se que esse envolvimento pode ser alcançado através da cooperação institucional através do intercâmbio de informações de investigação e de soluções de tecnologia da informação (Silva, 2006).

Desse modo, entende-se que a principal demanda apontada frente ao combate dos crimes virtuais é a vasta necessidade de aperfeiçoamento incessante dos policiais civis que trabalham diretamente com a investigação criminal. Verifica-se ainda que a adoção de medidas como a identificação do prosseguimento a tomar nesses casos já vem sendo discutida na doutrina, o que torna o enfrentamento a essas condutas mais eficazes. Dentre essas medidas, destaca-se o trabalho feito pela polícia junto aos fornecedores de internet, que ajudam para solução destes

crimes. Vale ressaltar, a necessidade de cooperação entre as polícias estaduais e federais, e também a necessidade de troca de informações entre as polícias internacionais, de modo a existir as qualificações. Sendo assim, esta é a apresentação do cenário atual da investigação destes crimes e algumas alternativas a escassez do aparato estatal e profissionais que atuam nesta área.

Os autores Maues, Duarte e Cardoso (2018) fazem uma observação além da necessidade de especialização policial, conforme explicitado abaixo:

> Ou seja, delegacias de polícias precisam ser especializadas em crimes cibernéticos, os juízes devem se atualizarem nas jurisprudências e doutrinas que envolvem delitos informáticos e os advogados, públicos ou privados, devem acompanhar a evolução do Direito Digital para que possa haver uma melhora no funcionamento da Justiça no Brasil (Maues, Duarte, Cardoso, 2018, p.178).

Portanto, com o número de crimes cada vez maior aplicado através da internet, se faz necessário a especialização dos profissionais nessas áreas, no Brasil já tem delegacias para tratar sobre estes crimes, um exemplo, seria a Delegacia de Repressão aos Crimes Cibernéticos, localizada na cidade de Fortaleza no Ceará. Porém não temos profissionais especialiados na área de tecnologia, como os cargos são preenchidos ateves de concurso público, se faz necessário só nivel médio e superior, sendo assim seria importante a formação e especialização na área da tecnologia.

## 5 CONSIDERAÇÕES FINAIS

A regulação da internet no Brasil é um tema complexo e multifacetado. Apesar da existência de leis voltadas para essa área, a eficácia dessas regulamentações é questionável. A estrutura atual não consegue abranger adequadamente os diversos aspectos envolvidos na internet, que incluem não apenas questões técnicas, mas também aspectos econômicos, sociais e políticos.

As empresas privadas e os órgãos públicos, que são os principais responsáveis pela segurança das informações no ambiente virtual, muitas vezes não possuem a tecnologia ou o conhecimento necessário para garantir essa segurança. Isso é evidenciado pelos vários casos de vazamento de dados que ocorreram no país, demonstrando a vulnerabilidade das informações no ambiente virtual.

Além disso, as leis existentes não são suficientes para proteger os usuários

da internet de ameaças imprevisíveis ou novas. As leis geralmente são criadas para atender a casos específicos, que já aconteceram. Isso significa que elas não conseguem prever ou lidar com novas situações que surgem com a constante evolução da tecnologia.

O Direito, por sua natureza, tem dificuldade em acompanhar a rápida evolução da tecnologia. Isso torna difícil tipificar crimes que ainda não foram praticados. Como resultado, os usuários da internet continuam navegando sob constantes ameaças.

Em suma, a regulação da internet no Brasil é um desafio que exige um esforço conjunto de várias partes interessadas. É necessária a capacitação dos profissionais de investigação criminal, para que possam lidar com a rápida evolução da tecnologia e as constantes ameaças enfrentadas pelos usuários da internet. Além disso, é crucial melhorar a estrutura tecnológica das empresas e órgãos públicos, para garantir a segurança das informações no ambiente virtual. Esses são passos essenciais para garantir 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 out. 2023.

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 out. 2023.

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,**

**direitos e deveres 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 da União, 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-Lei nº 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 out. 2023.

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 out. 2023.

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. E-book. Disponível em: https://ler.amazon.com.br/?asin=B076C1914R. Acesso em: 10 out. 2023.

GOMES, Luis Flavio. **Lei "Carolina Dickman" e sua (in)eficácia.** Jusbrasil, 2013. Disponível em: https://professorlfg.jusbrasil.com.br/artigos/121931292/lei-carolina-dickman-e-sua-in- eficacia. Acesso em: 20 out. 2023.

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. 2023.