Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

**VICTOR HUGO CAMILO**

# CRIMES CIBERNÉTICOS E INVASÃO DE PRIVACIDADE À LUZ DA LEI CAROLINA DIECKMANN

**Assis/SP**
**2020**

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

**VICTOR HUGO CAMILO**

# CRIMES CIBERNÉTICOS E INVASÃO DE PRIVACIDADE À LUZ DA LEI CAROLINA DIECKMANN

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação.

**Orientando: Victor Hugo Camilo**
**Orientador Gisele Spera Maximo**

**Assis/SP**
**2020**

FICHA CATALOGRÁFICA

C183c CAMILO, Victor Hugo.
Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann /Victor Hugo Camilo

44p.

Trabalho de conclusão de curso (Direito). – Fundação Educacional do Município de Assis – FEMA
Orientadora: Me. Gisele Spera Maximo
1. Crime cibernético 2. Lei 12/373/2012 3. Direito Digital

CDD: 341.55251
Biblioteca da FEMA

# CRIMES CIBERNÉTICOS E INVASÃO DE PRIVACIDADE À LUZ DA LEI CAROLINA DIECKMANN

**VICTOR HUGO CAMILO**

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

**Orientador:** _____
Gisele Spera Maximo

**Examinador:** _____
Luiz Antonio Ramalho Zanoti

**Assis/SP**
**2020**

# DEDICATÓRIA

Dedico este trabalho em primeiro lugar a Deus, que meu deu saúde e forças para superar todos os momentos difíceis em que me deparei ao longo da graduação, ao meu pai Valdir Camilo e minha mãe Neide Lúcia Rosa Camilo, minha irmã e namorada, por serem essenciais na minha vida e a toda minha família e amigos por me incentivarem a ser uma pessoa melhor e não desistir dos meus sonhos.

# AGRADECIMENTOS

Agradeço à toda minha família, amigos, professores, namorada e pessoas que ajudaram na realização desse trabalho. Sou imensamente grato pela paciência e incentivo. Obrigado pela incansável dedicação e confiança. Sou grato principalmente à Gisele Spera Maximo, que foi a minha orientadora e contribuiu muito com a realização dessa pesquisa.

*"Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível."* (Charles Chaplin)

# RESUMO

O objetivo do presente trabalho é focar na atuação do Estado e suas consequências no combate às práticas criminosas por meio da internet. O principal fator para a escolha deste tema foi a crescente em relação aos números de práticas deste delito nos últimos anos, por conta de que as novas tecnologias vêm tendo um aumento no que tange aos consumidores, o que consequentemente abre margem para novas infrações. Nesse sentido, será realizado primeiramente um estudo extenso no que tange à Carolina Dieckmann, com a lei 12.737/2012, discorrer sobre este tema e trazer possíveis sistematizações. Após, será realizado um estudo sobre o *cyberbullying*, retratando quais são os principais motivos para surgirem tanta frequência. E por fim, comentar a respeito do Direito Digital que é um ramo muito jovem e nosso país. Tudo isso será amparado em pesquisa jurisprudencial e análise estatística e bibliográfica pertinente ao ramo, tanto em artigos científicos quanto em livros de doutrina.

**Palavras-chave:** Crime cibernético; Lei Carolina Dieckmann (Lei º 12.737/2012); Marco Civil da Internet (Lei nº 12.965/2014); Direito Digital

# ABSTRACT

This paper aims to focus on State procedure and its consequences on the combat against internet crimes. The main factor to choose this subject was the recent years growing on internet crimes, meanwhile new technologies boost new consumers who are exposed to those new criminals. In this way, we start our work doing an extense look on Carolina Dieckmann's Law (12.737/12), discoursing about this subject and the possibility of new systematizations. After, we'll study *cyberbullying*, trying to see the reasons of why it happens so often. Finally, we'll talk about Digital Law, a new branch on Brazilian's Law. All of it will be supported by jurisprudential works, statistics and scientific papers and books who attend this area.

**Keywords:** Cybercrime; Carolina Dieckmann's Law (Lei º 12.737/2012); Civil Framework of the Internet (Lei nº 12.965/2014); Digital Law

# SUMÁRIO

# INTRODUÇÃO

O intuito desta monografia é analisar os chamados crimes cibernéticos. O principal motivo que se fundou na escolha do tema foi a evolução dos números nos últimos anos a respeito deste tipo de crime, isso porque o número de novas tecnologias vem crescendo conforme os anos passam.

O presente trabalho visará realizar um estudo estrito de como que a atualidade vem lidando com essa situação, bem como o ordenamento jurídico brasileiro está regulando a matéria, apontando as qualidades e as falhas.

Como há de se saber, estudos e pesquisas sobre este tema são muito dificultosos por se tratar de uma matéria consideravelmente recente em nosso país. Contudo, é possível verificar uma necessidade em se aprofundar no estudo dessa temática, isto por haver diversas lacunas em nossas legislações que (não) regulam este tipo de matéria.

Com isso, há curiosidade de sabermos como é a estrutura dos órgãos encarregados de fazerem tais investigações, como os agentes se especializam para resolver determinados casos. E por se tratar de matéria recente em nosso país, sabemos que não há uma grande experiência nesses casos, logo, não há uma capacitação profissional ou estruturação, em razão das circunstâncias financeiras que o Estado oferece aos seus encarregados.

A estratégia utilizada para a criação dos textos partiu-se de fontes indiretas, isso porque o trabalho visou abordar de forma geral o que tange aos crimes cibernéticos, para então se atentar às legislações que tutelam esse crime e avançar explorando como ocorre a parte da investigação

A estrutura da presente pesquisa se inicia, primeiramente, na análise fática do acontecimento que houve com Ana Carolina Dieckmann, no ano de 2012. Será relatado como o Marco Civil da Internet tutela os dados pessoais dos usuários.

Em seguida, trataremos do *cyberbullying*, um dos grandes males advindos da globalização e do desenvolvimento tecnológico. Um problema que não se esgota em território nacional, mas que, além disso, se acentua em todo o globo terrestre.

Por último, iremos tratar da área do direito digital e de como esta tem crescido e se desenvolvido para atenuar os problemas causados pelas práticas ilícitas feitas no âmbito digital. Trataremos também da interdisciplinaridade presente no ramo do direito digital e como esse tem cada vez mais ganhado autonomia dentro do ordenamento jurídico brasileiro.

Com os três pontos levantados, será possível tecer alguns aspectos a título de considerações finais.

# 1. CAPÍTULO I – A LEI CAROLINA DIECKMANN E O CRIME DIGITAL

## 1.1. A ORIGEM DA LEI 12.737/2012 – "LEI CAROLINA DIECKMANN''

A lei 12.737/2012 foi elaborada em atenção à necessidade evidenciada pela sociedade de um tratamento especifico acerca do crime virtual, caracterizado este pela invasão de aparelhos eletrônicos para a obtenção de dados particulares de terceiros.

A referida legislação recebeu o nome da atriz Carolina Dieckmann, pois sua origem se deu por conta da exposição de 36 fotos íntimas da atriz - sem o seu consentimento - na internet, em maio de 2012. Ainda, antes da divulgação, o criminoso, denominado apenas de *hacker*, tentou extorqui-la no montante de dez mil reais em troca da não publicação de suas fotos.

Na oportunidade, a polícia identificou quatro suspeitos de terem roubado as fotos do computador da atriz. Contudo, como ainda não havia tipificação para tal conduta no Código Penal, os acusados foram indiciados por furto, extorsão qualificada e difamação.

Na época, a Polícia Civil averiguou a hipótese de as imagens terem sido copiadas de uma máquina fotográfica que, em momento anterior, havia sido levada para conserto. Entretanto tal hipótese caiu por terra, pois se apurou que a caixa de e-mail pertencente à atriz havia sido violada por ação de hackers.

Inconformada com a penalidade mínima cominada ao delito praticado pelos hackers, pois considerava uma afronta para sua dignidade, à sua imagem e à sua condição de pessoa humana, Carolina Dieckmann abraçou a causa, se socorreu nos meios de comunicação e conseguiu representatividade no poder legislativo, o que culminou na criação e promulgação de lei especifica para tratar do crime cibernético, cedendo o próprio nome que hoje está vinculada com a nova lei.

Na oportunidade, a referida legislação derivou do Projeto de Lei n. 2.793/11 – apresentado no Congresso como apenas uma proposta - onde já corria o PL n. 84/99, ambas com disposições para tratar de infrações cometidas através de tecnologias e da informática.

Entretanto, pela grande pertinência de suas peculiaridades, o Projeto de Lei n. 2.793/11 em comparação aos demais projetos similares, teve uma rápida aprovação dentro das casas legislativas. Sendo assim, por se tratar de fotos íntimas vazadas e pela grande repercussão que houve na época, tiveram a discricionariedade de agilizar todos os meios necessários para promover a promulgação da então Lei nº 12.737/2012.

## 1.2. DA VIGÊNCIA DA LEI 12.737/2012

A referida lei entrou em vigência na data de 2 de abril de 2012, sendo conhecida popularmente como Lei Carolina Dieckmann. Esta legislação trouxe uma inovação dentro dos textos do Código Penal, pois enfatiza a criação de um novo tipo penal, no que tange aos crimes virtuais próprios, que se caracteriza pela invasão de dispositivo informático alheio, tipificando-se no artigo 154-A do CP.

Segundo a doutrina, o ato de copiar dados ou informações pessoais sem o consentimento destas, até então, não gozava de previsão legal dentro do sistema penal brasileiro. Com isso, como havia uma falta de meios, as autoridades se utilizavam de recursos alternativos, como por exemplo o crime de furto, previsto no art. 155 do CP, para atribuir responsabilidade ao criminoso.

À vista disso, com a Lei n. 12.737/2012, já em vigência, ocorreu uma nova ótica, mais específica, quanto à invasão de dispositivos, possibilitando, desta maneira, que haja processos sem a proibição da analogia *in malam partem*[2] e até mesmo que não fira o princípio da legalidade.

Ela entrou em vigência com o intuito de tutelar todos os crimes virtuais que envolvam dados pessoais vazados. Os indivíduos que praticarem os crimes previstos na Lei 12.737/2012 serão punidos com pena mínima de 03 meses e máxima de 02 anos de reclusão, mais multa, como dispõe os artigos 154-A e 154-B. É oportuno dizer que, dependendo das circunstâncias, a pena poderá ser ainda maior. Se o mesmo crime for praticado contra integrantes de cargos públicos, a lei prevê um aumento de pena de um a dois terços.

---

[2] A analogia *in malam partem* é aquela que traz algum tipo de maleficia ao réu dentro do processo.

Em contrapartida, muitos doutrinadores e especialistas em crimes virtuais não são favoráveis à lei, pois dizem haver muita polêmica acerca do assunto e alguns acreditam que a punição é desproporcional ao ato praticado, sendo que, em caso de o agente cometedor do crime não ostentar antecedentes criminais, é possível que ele tenha um benefício que a própria lei impõe, que é a inversão da pena e doação de cestas básicas, o que implica dizer que poderá haver a execução do instituto *Sursis*[3].

Como há de se perceber restou uma lacuna nesta lei, pois o sujeito ao cometer o delito poderá ser beneficiado por essa brecha existente.

## 1.3. DAS ALTERAÇÕES NO CÓDIGO PENAL EM DECORRÊNCIA DA LEI 12.737/12

Foram acrescentados ao Código Penal, por meio da referida lei, os artigos 154-A e 154-B, bem como a alteração dos artigos 266 e 289.

O artigo 154-A prevê o crime de invasão de dispositivo informático, seja ele por meio de uma conectividade de internet ou não, do qual o criminoso se utiliza da vulnerabilidade da violação de segurança da tecnologia com o objetivo de obtenção, adulteração ou até mesmo destruição de dados pessoais lá constantes.

A pena cominada ao ato praticado presente no *caput,* bem como de quem comercializa algum tipo de programa para permitir a prática da referida conduta, é de 03 meses a 01 ano de detenção, e multa. Além disso, se esta obtenção causar um prejuízo de cunho econômico à vítima, a pena poderá ser aumentada de 1/6 a 1/3.

Vale lembrar que, se a conduta for praticada para a obtenção de conteúdo de comunicações privadas, informações sigilosas de empresas ou industriais, a pena é ainda mais grave, sendo de 06 meses a 02 anos de reclusão, e multa.

A lei também prevê algumas situações quando o delito for praticado contra cargo público específico, como por exemplo, Presidente da República,

[3] Sursis é uma suspensão condicional da pena, aplicada à execução da pena privativa de liberdade não superior a dois anos, podendo ser suspensa, por dois a quatro anos, desde que o condenado não seja reincidente em crime doloso e não seja indicada ou cabível a substituição por penas restritivas de direitos.

governadores, prefeitos, dentre outros que se encontram previstos no parágrafo 5º. Nestes casos, a pena poderá ser aumentada de até 1/3 a 1/2.

O artigo 154-B estipula que a Ação Penal adequada para as condutas expostas no artigo anterior é somente por meio de representação do ofendido, ou seja, somente haverá denuncia se houver o consentimento e autorização da vítima que teve seu dispositivo violado. Porém, se o crime for praticado contra a Administração Pública, seja ela direta ou indireta, quaisquer que sejam os poderes, da União, Estados, Distrito Federal ou Municípios, a Ação Penal se procederá mediante ação pública incondicionada.

É oportuno observar que este novo crime é distinto em relação ao tipo penal constante no artigo 154 e dos demais tipos penais comuns. No caso, a elementar é a "violação indevida de mecanismo de segurança'', portanto, é possível afirmar que somente será enquadrado o crime previsto no artigo 154-B quando o autor da conduta se utilizar de sua habilidade para burlar a proteção do sistema operacional informático. Porém, caso o dispositivo se encontre sem a proteção devida, não há de se falar em punição ao agente pois no caso não houve a chamada "violação de segurança''.

Ademais, as informações ditas acima precisam chegar nos cibernautas para que eles possam se proteger ao máximo, se utilizando de programas antivírus, senhas mais complexas em redes sociais, além de evitarem de acessar sites/links deixados pelos *crackers*[4]*,* que acabam fazendo com que o próprio usuário seja o responsável pela passagem desse criminoso pelo sistema operacional da máquina.

Insta dizer que no artigo 298 do Código Penal houve um acréscimo de dois parágrafos, o primeiro prevê ao tipo penal a interrupção do serviço telemático ou informação de utilidade pública e o segundo permite a possibilidade da aplicação em dobro nos casos de calamidade pública.

Ainda, o supracitado artigo teve adicionado em sua capitulação jurídica um parágrafo único. Nele, diz que o cartão de crédito ou débito é caracterizado como uma tipificação do crime de falsificação de documento particular.

---

[4] Cracker é o termo usado para designar o indivíduo que pratica a quebra (ou *cracking*) de um sistema de segurança de forma ilegal.

> Falsificação de documento particular
>
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> Falsificação de cartão
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a Documento particular o cartão de crédito ou débito. (BRASIL, 1940)

Apesar disso, segundo a doutrina, tal acréscimo ocorreu em decorrência do aumento de número de fraudes bancárias envolvendo clonagens de cartões. Vale esclarecer ainda que muitos estudiosos do direito entendem que a adição deste parágrafo único do artigo 298 do Código Penal deixou de aproveitar a oportunidade de adicionar também outros documentos, sejam eles físicos ou digitais, como por exemplo o Certificado Digital[5].

Muito embora ainda haja entendimentos conflitantes de estudiosos da área, ainda é preciso ter uma análise de doutrinas e jurisprudências para firmar os instrumentos introduzidos, modo pelo qual não se tenha nenhuma brecha em que o infrator pode eventualmente se valer e acabar saindo beneficiado de tal conduta. Trata-se um assunto delicado, pois o mundo tecnológico se atualiza constantemente e, por conta disto, torna-se dificultoso sanar tais vícios legais.

Por conta disso, após dois anos, veio o surgimento da Lei nº 12.965/14, também conhecida como o Marco Civil da Internet, que foi elaborada com a contribuição da sociedade civil juntamente com o Poder Público.

## 1.4. LEI AZEREDO (LEI 12.735/2012)

No ano de 1999, surgiu o chamado projeto da Lei Azeredo (PL 84/99), que teve sua criação derivada do ex-deputado federal Luiz Piauhylino, cujo objetivo era encarregar-se dos crimes cibernéticos, difusão de vírus, eventos para derrubar sites, pornografia infantil bem como os próprios hackers de computador.

[5] Certificado Digital é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, e por ele pode se fazer transações online com garantia de autenticidade e com toda proteção das informações trocadas.

Dentro desse projeto foi incluso, por exemplo, o crime de estelionato eletrônico. O PL tramitou por treze anos nas casas do Congresso Nacional. Em 2008 se encaminhou, aprovado na Câmara, até o Senado Federal. Na casa do Senado, o Senador Eduardo Azeredo modificou o texto, dando mais potência e abrangência à previsão anterior

Contudo, esse projeto guardava inúmeros pontos polêmicos, como por exemplo o fato de guardar o histórico acessado pela pessoa por até três anos, que poderia acabar implicando um certo controle da privacidade e liberdade do usuário. Diante disso, a Lei Azeredo chegou até a ser alcunhada de ‘’ AI-5 Digital’’[5], pelo fato de a lei afrontar a liberdade e privacidade como já foi dito acima. Todavia, ela foi totalmente alterada, sendo que, dos seus 23 artigos, 17 foram removidos. Assim sendo, a lei passou a cobrir crimes como traição por transferência de dados ao inimigo e falsificação de cartões de crédito ou débito.

Em vista disso, podemos afirmar que inicialmente essa lei foi criada com o intuito de tutelar os crimes cibernéticos e por fim, ela deixou de zelar por invasões de computadores, tampouco pelo compartilhamento de informações sigilosas de pessoas.

Contudo, após o exaurimento dos artigos, o artigo 4º da Lei Azeredo teve grande importância para a criação de centros policiais especializados em investigações de crimes cibernéticos.

No entanto, é pertinente ressaltar que grande parte dos Estados de nossa Federação não possuem uma boa estrutura, por falta de capacitação dos profissionais ou até mesmo por um baixo desdobramento de orçamento aos centros especializados.

Na era dos avanços tecnológicos, é evidente que os centros especializados contribuem de forma significativa na resolução de acontecimentos de difícil elucidação, como por exemplo, homicídios ou ataques a instituições bancárias. Porém, há de se fazer uma releitura da Lei Azeredo para que os centros especializados possam fazer investigações somente em crimes

[5] O AI-5 é entendido como o marco que inaugurou o período mais sombrio da ditadura e que concluiu uma transição que instaurou de fato um período ditatorial no Brasil.

próprios, que são aqueles delitos que necessariamente precisam ser praticados mediante o uso de uma máquina, pois o nível de complexidade nesses casos é maior, doravante deixando com que os demais casos fiquem para o atendimento das demais delegacias.

## 1.5. MARCO CIVIL DA INTERNET – (LEI 12.965/2014)

A lei 12.965/14 é conhecida como Marco Civil da Internet, e tem por principal objetivo ser uma *Carta Magna* nos assuntos inerentes ao meio digital, tendo em vista que ela visa tutelar todos os direitos e deveres daqueles que tem contato com a rede mundial de computadores, smartphones ou tablets. Melhor dizendo, todo aparelho que pode ter a conectividade com a internet.

O Marco Civil da Internet foi qualificado de forma divergente por tratar de diversos setores da sociedade civil para ensejar a criação da referida lei, com a colaboração da democracia, por meio de consultas públicas disponibilizadas pelo caminho da internet. Foi uma junção de parceria entre a Secretaria de Assuntos Legislativos do Ministério da Justiça e o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, além da sociedade como um todo.

Para que se chegasse ao final com o projeto e com o texto pronto, foram realizados diversos seminários, videoconferências e audiências. Desta forma, ressalta-se o cunho da democracia, onde, criou-se um meio de comunicação entre o Estado e a sociedade civil, que pôde opinar de forma mais direta.

No ano de 2014, foi promulgada a Lei de nº 12.965. Esta lei foi criada com o intuito de tutelar a internet, dando mais segurança aos dados pessoais bem como estabelecer regras, direitos e deveres no âmbito virtual. Depois de diversas sugestões por meio de sites e audiências públicas, foi ratificado pela até então presidente da República, Dilma Rousseff, em 23 de abril de 2014.

A lei 12.965/2014 é constituída por trinta e dois artigos, subdivididos em cinco capítulos: Disposições preliminares; Dos direitos e garantias dos usuários; Da provisão de conexão e aplicações da Internet; Da atuação do poder público; e Disposições Finais.

O primeiro capítulo é mais genérico, pois busca comentar a respeito de conceitos, princípios, direitos e deveres para se utilizar a internet no Brasil. Outro

ponto importante que é descrito no primeiro capítulo trata da liberdade pessoal, que se baseia nos usos e costumes.

O segundo capítulo determina os direitos e garantias dos usuários, dos quais eles têm em sua vida particular bem como na sua vida profissional, referentes aos termos de políticas e termos de uso dos sites, redes sociais e sites de compras.

O terceiro capítulo traz medidas a respeito dos provedores de conexão e de aplicação de internet. É oportuno compreender que dentro deste capítulo é possível encontrar a neutralidade da rede no que diz à responsabilidade do encarregado pela transmissão, comunicação e roteamento de dados.

O quarto capítulo expõe a maneira de atuação do Poder Público, isto é, determina diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios no que tange à internet no Brasil.

Por fim, o quinto capítulo, já de forma conclusiva, trata sobre a liberdade de escolha do usuário na utilização de programa de computador, sobre a defesa de interesses e dos direitos estabelecidos nesta lei entre outros.

> Art. 3º **-** 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;
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014)

O princípio da liberdade de expressão garante que todas as pessoas tenham igual direito de difundir informações e opiniões na rede. Para isso, os conteúdos publicados só podem ser retirados com autorização do autor ou com ordem judicial e os provedores de acesso e de serviços não podem ser responsabilizados pelo que os usuários publicam.

O princípio da proteção da privacidade determina que provedores e sites não possam usar dados dos usuários com fins comerciais, mas que devem guardar esses dados por pelo menos seis meses. Esse princípio também obriga empresas estrangeiras a submeterem-se às leis brasileiras de segurança à informação, ainda que os centros de armazenamentos de dados (datacenters) estejam fisicamente fora do país.

Ainda, o princípio da preservação e garantia da neutralidade da rede impede que provedores de conexão de rede cobrem valores diferentes dos usuários em função do que acessam. Isso significa que a empresa não pode oferecer um pacote barato para prover acesso a e-mail e redes sociais e outro caro para acesso à plenitude da Internet. Com a rede neutra, os provedores só podem cobrar pela velocidade de conexão; todos os sites têm mesma velocidade e o usuário navega por qual quiser.

Dentre os princípios e direitos apontados acima, é cabível dizer que o Marco Civil da Internet, no entanto, é muito mais principiológico do que regulamentador, doravante na maior parte de seus dispositivos apenas reconhece direitos fundamentais já previstos na Constituição Federal de 1988 ou em tratados internacionais nos quais o Brasil é pertencente. O que fica evidente é dizer que o principal intuito do legislador foi de reforçar a proteção de tais direitos no ambiente virtual e buscar uma maior comodidade por parte dos utilizadores da internet.

Por fim, o Marco Civil da Internet (MCI) aponta como sujeitos de direitos e deveres os usuários da internet, no qual se equiparam a consumidores para todos os fins, conforme assegurado pelo Código de Defesa do Consumidor, tendo como objetivo garantir o direito à informação, honra objetiva, proteção contra práticas abusivas, etc. Além do mais, outros consumidores garantidos pela legislação seriam os provedores de conexão e de acesso à internet, estejam eles no Brasil ou no exterior.

Ademais, Leite e Lemos dissertam em seu livro Marco Civil da Internet (Atlas, 2014)

> Com isso, o resultado final do Marco Civil foi uma lei tecnicamente sólida, abrangente e ambiciosa. Mais do que isso, seu texto foi saudado por especialistas de vários países como um dos mais avançados e “pró-inovação” que se poderiam conceber naquele momento. Com isso, o Marco Civil despertou grande interesse internacional. E grande expectativa com relação ao Brasil: nosso país passou a correr o bom risco de aprovar uma das leis mais avançadas para a internet.
>
> Por tudo isso, é possível afirmar, que o Marco Civil tenha sido um dos projetos de lei mais amplamente debatidos no país em múltiplas mídias, tendo inaugurado uma nova metodologia de construção legislativa que pode informar uma grande medida os caminhos da democracia em uma sociedade cada vez mais digital. (p. 6-7)

À vista disso, foi um grande passo não só para o Brasil, mas para o mundo. É notório que o Marco Civil da Internet se tornou uma legislação sem muitas complicações para haver um entendimento sobre sua essência. Essa legislação que também é conhecida como a “Constituição Federal da internet’’ veio para assegurar direitos fundamentais básicos ao utilizar a ferramenta da internet.

## 1.6. A PROTEÇÃO DA DIGNIDADE DA PESSOA HUMANA E O MARCO CIVIL DA INTERNET

É possível afirmar que o princípio da dignidade da pessoa humana é um norteador jurídico que tem por escopo assegurar a todo ser humano, pelo simples fato de ser humano, o valor intrínseco da pessoa às condições mínimas indispensáveis para uma existência e uma vida digna.

O Ministro do Supremo Tribunal Federal, Luís Roberto Barroso (apud Rocha, 2014) salienta a respeito deste princípio o seguinte pensamento:

> (...) a começar por sua origem e evolução até chegar à compreensão atual, assentada no pressuposto de que cada ser humano possui um valor intrínseco e desfruta de uma posição especial no universo, passando pelos marcos religiosos e filosóficos, aportando no marco histórico decisivo para o delineamento hodierno da dignidade humana, que foram as atrocidades cometidas pelos regimes totalitários (nazismo e fascismo) e a reação que eles provocaram após a Segunda Grande Guerra, com o despertar dos povos e nações para o sentimento de que a proteção dos direitos da pessoa humana há de ser objeto de preocupação internacional. Desse modo, a dignidade humana incorporou-se ao discurso político dos vitoriosos como alicerce a resguardar a paz mundial e a estabilidade das relações internacionais. Em seguida, é transportada para discurso jurídico, com

> sua inserção nas Declarações de Direitos e nos diversos textos constitucionais do pós-guerra. (p. 345)

O Marco Civil da Internet aponta como uma das principais garantias a proteção da dignidade, a inviolabilidade de dados pessoais e a proteção à privacidade e à intimidade do usuário, conforme é assegurado pela Carta Magna em seu disposto do artigo 5º, X da CF/88.

Portanto, os dados pessoais de um determinado usuário somente podem ser concedidos mediante o seu próprio consentimento ou por ordem judicial, o que implica no fim de questões controvertidas como a diminuição de armazenamento de dados na internet.

O Marco Civil da Internet, ao ser elaborado, teve uma grande preocupação no que diz respeito à privacidade dos usuários, tendo em vista que um dos problemas enfrentados pelo usuário é decorrente à comercialização de dados pessoais.

Pelo texto taxativo do Marco Civil da Internet (MCI), os provedores de internet não são responsáveis pelos dados vazados no mundo virtual. Em controvérsia, há juízes que punem, por exemplo, sites como *Facebook* e *Google* por páginas criadas por usuários detentores de contas em seus sites, mas há outros magistrados que punem apenas os cometedores responsáveis pelo conteúdo. Porém, em concordância com a nova legislação, as empresas somente serão punidas quando houver danos a terceiros caso não respeitem decisões judicias que definam a remoção de tais publicações ofensivas.

## 1.7. AS RELAÇÕES DO MARCO CIVIL DA INTERNET COM AS DEMAIS LEGISLAÇÕES BRASILEIRAS

Como já indicado nesta obra, o Marco Civil da Internet sobreveio de diálogos, onde a sociedade teve a oportunidade de participar na elaboração da lei 12.965/2014. Com isso, evidentemente, foram introduzidos diversos direitos fundamentais garantidos pela Constituição Federal de 1988 e documentos internacionais.

Assim, a estrutura da referida lei vai adiante, nela é possível encontrar diversos princípios que regem o uso da internet, englobando o Código Civil de 2002 no que tange aos direitos da personalidade, e também o Código de Defesa do Consumidor (Lei nº 8.078/90). Pode se falar também em diálogo com o Estatuto da Criança e do Adolescente, pois segundo um estudo mostrado pelo Comitê Gestor da Internet (CGI.br)[6], a faixa etária predominante da internet é de crianças de 09 anos até adolescentes de 17 anos. Além do mais, encontra-se incluso no Marco Civil a lei de Direitos Autorais (Lei nº 9.610/99), Lei do Sistema Brasileiro de Defesa da Concorrência (Lei nº 12.529/11), Lei de Ação Civil Pública (7.347/85), Lei do *Habeas Data* (9.507/97), o Código de Processo Civil e por fim, os Códigos Penal e de Processo Penal.

Contudo, podemos notar que a lei do Marco Civil da Internet foi criada para tutelar todos os âmbitos possíveis que possam ser violados, de forma que não haja nenhuma brecha em que o criminoso possa se valer e sair beneficiado da conduta típica.

[6] O Estudo se encontra disponível no seguinte link: <https://www.cgi.br/noticia/releases/cresce-numero-de-criancas-e-adolescentes-que-buscam-noticias-na-internet-aponta-cetic-br/> Acesso em: jul.2020

# 2. CAPÍTULO II - ASPECTOS HISTÓRICOS DO *CYBERBULLYING*

O surgimento do *cyberbullying* se deu a partir momento em que as redes sociais tomaram uma maior proporção nos meios digitais, e como consequência, o crime veio a aumentar.

A internet começou a ser um problema quando a tecnologia passou a interferir nas relações humanas de uma forma socialmente desagradável, possibilitando até a ocorrência e a perpetração de alguns delitos. E a partir disso, se viu a necessidade de uma tutela jurisdicional para as ações realizadas no meio virtual, mas que sejam dotadas de características de ações realizadas no "mundo real" ou que nele surte efeitos (Fiorillo  Conte, 2016, P. 16).

Deu-se início ao *cyberbullying* em sites de relacionamentos como por exemplo Orkut, Facebook, etc. Nesse crime, o praticante tem a vantagem de cometer e atingir a pessoa desejada, a qual prejudica psicologicamente e ainda sai com o benefício do anonimato, o que acaba dificultando na punição.

Schreiber e Antunes (2015) conceituam o surgimento do *cyberbullying* da seguinte forma:

> Dentro desse cenário, sobre a influência do rápido desenvolvimento das tecnologias de comunicação e suas implantações no meio social, esse tipo de violência passou a se estender para fora do ambiente escolar, através das redes sociais e aparelhos de comunicação digital. Um dos pioneiros a falar sobre esse tipo de violência é Belsey (2004), denominando-o de cyberbullying, que é o uso de informações e de tecnologias de comunicação - como e-mail, celular, aparelhos e programas de envio de mensagens instantâneas e sites pessoais - Universidade Católica do Salvador | Anais da 22ª Semana de Mobilização Científica- SEMOC | 2019 com o objetivo de difamar ou apoiar de forma deliberada comportamentos, seja de indivíduo ou grupo, que firam de alguma forma outros tantos (p. 111).

Portanto, podemos dizer que o *bullying* é uma situação que acontece no decorrer dos anos, diferentemente do *cyberbullying* que somente veio aparecer após as redes sociais serem inauguradas na internet.

## 2.1. O *CYBERBULLYING* E A LEI Nº 13.185/15

Estamos vivendo na denominada era digital, na qual todo mundo tem uma estreita relação com a tecnologia, recebendo e enviando diversas informações.

Com o fácil acesso à internet, possibilita-se que pessoas façam tarefas rotineiras por meio destes aparelhos que vieram para ajudar a vida do ser humano, porém, abre-se espaço para a criminalidade virtual. Infelizmente, muitas pessoas que têm acesso à internet não possuem discernimento de certas atitudes que podem ou não serem cometidas na internet e os criminosos se aproveitam dessa vulnerabilidade. É nesse contexto que surge o *cyberbullying*, ou seja, a prática comum de uma versão tecnológica já conhecida por nós, o *bullying*.

O *cyberbullying* é uma prática extremamente recente da internet, além de ser bastante comum, pois, como se sabe, a internet também é um espaço de grandes violências. A priori, comentaremos a definição de *cyberbullying*, que pode ser entendido como a prática de violência que acontece principalmente pela rede mundial de computadores. Mas é oportuno dizer que esta definição é genérica, porque é contido dois conceitos em um único que juntos formam esta ideia.

O primeiro deles é o conceito de *bullying*, que significa intimidar ou amedrontar determinada pessoa, o que acontece com mais frequência nos ambientes escolares, inclusive, esse termo já foi utilizado em nosso país para caracterizar não atos reais, mas sim atos que atingem o psicológico da pessoa. Por outro lado, o segundo conceito, de *Cyber*, traz a ideia de espaço virtual e internet, deste modo, está ligado ao mundo das redes sociais.

Tendo os dois conceitos definidos, fica evidente que haver a junção de ambos se traduz na prática de violências que acontecem pelo mundo virtual, ou seja, o canal de espaço para que o infrator possa chegar até o resultado desejado, é a internet.

Como há de se saber, a lei 13.185/15 tem um viés administrativo e não punitivo. Ela busca indicar como utilizar nas escolas os métodos de prevenção ao *bullying*, podendo algumas sistematizações serem utilizadas por analogia nos casos do *cyberbullying*.

## 2.2. CARACTERÍSTICA DO FENÔMENO DO *CYBERBULLYING*

A expressão *bullying* advém do inglês e significa tirano, brigão ou até mesmo valentão, e é utilizado para empregar a alguém determinados atos que tem por viés intimidar ou amedrontar a pessoa, atingindo, então, a sua saúde psicológica. Este fenômeno já é antigo em nosso país e costuma ocorrer com frequência em ambientes escolares, isso porque crianças e adolescentes não possuem noção de suas condutas, e o que elas podem ocasionar.

As condutas do *bullying* presencial foram potencializadas com o *cyberbullying*. Diversos elementos fizeram com que os sujeitos que praticavam tais condutas na vida real passassem a se utilizar do meio virtual. O praticante do *cyberbullying* é um agressor diferenciado, porque se utiliza de uma forma dissimulada de agressão verbal ou escrita. E possui em comum com suas vítimas algumas características consistentes como passar muito tempo na Internet e utilizá-la para estabelecer relacionamentos (FIORILLO e CONTE, 2016, p.260). Neste caso, não precisa ser maior ou mais forte do que as vítimas, como é característica peculiar do *bullying* presencial. Com isto, a força física da pessoa se tornou algo irrelevante para concretizar o *cyberbullying*, que necessita apenas da conectividade com as tecnologias de informação, além de garantir o anonimato ao infrator, sendo certeiro que os ataques atingirão a pessoa.

O anonimato é um atributo a mais para que o praticante tenha vontade de continuar ou até mesmo dizer coisas que presencialmente não teria coragem. Desta forma, o praticante ignora todas as repercussões que seus atos poderão surtir, até mesmo porque o agressor não recebe uma resposta imediata da vítima, fazendo com que se estimule ainda mais a ideia de continuar atingindo a vulnerabilidade da vítima.

A Associação Brasileira Multiprofissional de Proteção à Infância e à Adolescência define *bullying* com as seguintes ações: colocar apelidos, ofender, zoar, gozar, encarnar, sacanear, humilhar, fazer sofrer, discriminar, excluir, isolar, dentre outras condutas. No que diz respeito ao *cyberbullying*, a ação praticada busca atingir o foro subjetivo da pessoa e, consequentemente, o seu psicológico, por meio de mensagens falsas publicadas em páginas de redes sociais ou o compartilhamento de informações. Assim, o *cyberbullying* engloba

todo e qualquer tipo de agressões, assédios, coações, constrangimentos que façam a pessoa passar ou condutas similares, todas realizadas mediante o uso das tecnologias de comunicação e informação (TCI).

O *cyberbullying* pode ser subdividido em diversas espécies, como por exemplo o *flaming*, que consiste no envio de mensagens vulgares ou que mostram hostilidade em relação a uma pessoa determinada. A mensagem pode ser enviada tanto em grupos online quanto diretamente para a própria pessoa. As mensagens são chamadas de *flames* (traduzindo do inglês significa *chamas*) e servem para provocar a vítima, tirá-la do sério. Já os que enviam as mensagens são denominados de *flamers* ou *trolls*. Dependendo da mensagem, é possível enquadrar a conduta do criminoso no crime contra a honra objetiva da pessoa.

Uma outra modalidade de *cyberbullying* é o chamado *cyberstalking*, onde, a conduta é perseguir a pessoa online. Conforme leciona Damásio E. de Jesus:

> *Stalking* é uma forma de violência na qual o sujeito ativo invade a esfera de privacidade da vítima, repetindo incessantemente a mesma ação por maneiras e atos variados, empregando táticas e meios diversos: ligações nos telefones celular, residencial ou comercial, mensagens amorosas, telegramas, ramalhetes de flores, presentes não solicitados, assinaturas de revistas indesejáveis, recados em faixas afixadas nas proximidades da residência da vítima, permanência na saída da escola ou do trabalho, espera de sua passagem por determinado lugar, frequência no mesmo local de lazer, em supermercados etc. (2008)[7]

Contudo, o *stalker* visa dominar psicologicamente a vítima através desta perseguição online, fazendo com que a mesma se sinta pressionada.

Na situação do *cyberbullying,* acaba acarretando um maior dano em comparação ao *bullying* presencial, isto porque sabe-se que o mundo virtual é muito abrangente e sem fronteiras. À vista disso, a informação falsa publicada em uma rede social poderá fazer com que a prática chegue ao mundo inteiro em questão de horas, talvez menos.

---

[7] Trata-se de artigo publicado online, disponível em: << https://jus.com.br/artigos/10846/stalking#:~:text=Stalking%20%C3%A9%20uma%20forma%20de,%2C%20telegramas%2C%20ramalhetes%20de%20flores%2C>> Acesso em jul.2020

É importante salientar que a principal característica do *cyberbullying* se faz através dos processos de intimidação pelas redes sociais. Um exemplo claro disto seriam as criações de perfis fakes, caracterizando-se o crime de falsificação ideológica que se encontra previsto no artigo 299 do Código Penal.

> Falsidade ideológica
>
> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
>
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular.
>
> Parágrafo único - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte. (BRASIL, 1940)

Se formos comparar a fiscalização que havia antigamente em relação aos pais sobre os filhos com a de hoje, iremos perceber que atualmente os pais deixaram de se importar um pouco na questão sobre o que o filho faz na internet. Com isso, o menor de idade tem uma determinada autonomia em tudo que está fazendo, o que muitas das vezes abre a oportunidade de o mesmo vir a cometer esses crimes virtuais e os pais nem sequer ficam sabendo.

Geralmente esses *fakes*[8] são criados por jovens estudantes para atacarem outros jovens estudantes. Isso demonstra que em muitos casos o autor da violência e também a vítima são jovens. Eles criam contas *fakes* normalmente para zombar de alguém, divulgar fotos íntimas, ameaçar, falar coisas de baixo calão direcionadas a uma pessoa determinada, entre outras ações. Fica evidente que elas se utilizam do mundo virtual para se expressar, coisa que se fosse presencialmente, em muitos casos, não teriam coragem de fazer.

[8] Fake é uma palavra da língua inglesa que significa falso ou falsificação. Pode ser uma pessoa, um objeto ou qualquer ato que não seja autêntico. No âmbito da tecnologia, o perfil fake se constitui na criação de um perfil falso na internet, onde uma pessoa se passa por outra. Com as redes sociais, o termo passou a ser muito utilizado para designar uma conta na internet ou o perfil em uma rede social de alguém que pretende ocultar a verdadeira identidade.

## 2.3. O ORDENAMENTO JURÍDICO E A LEI DE *CYBERBULLYING*

O tratamento do *cyberbullying* no Brasil deixa um pouco a desejar, pois não traz resultados positivos na maioria dos casos e é necessário encontrar novos mecanismos para diminuir o alto índice desses delitos para combater ou pelo menos diminuir suas ocorrências.

Como dito anteriormente, não existem ferramentas eficazes para se ter êxito no combate e, por conta disso, por haver lacunas em nosso ordenamento jurídico, fica evidenciado que o fenômeno ocorre por não haver tratamento positivo.

A Constituição Federal, em seu artigo 1º, coloca como um dos fundamentos da República Federativa do Brasil a dignidade da pessoa humana. Segundo o princípio da reserva legal, explana que não tem crime sem lei prévia que o defina e faz correlação em que não há crime sem ofensa ao bem jurídico protegido por lei. Logo, se formos pensar, no *cyberbullying* há uma ofensa a um bem jurídico positivado que é a dignidade da pessoa humana, mesmo que seja de forma indireta.

A esfera deste crime está relacionada com o já mencionado princípio pelo fato de que o principal destinatário do Código Penal é o cidadão. Logo, os direitos sociais mínimos devem ser respeitados.

A Lei nº 13.185, de 6 de novembro de 2015, sancionada pela até então presidente Dilma Rousseff, definiu o Programa de Combate à Intimidação Sistemática (*Bullying*), e em seu parágrafo único da já dita lei explica o que se entende por intimidade sistemática:

> Parágrafo único. Há intimidação sistemática na rede mundial de computadores (cyberbullying), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial. (BRASIL, 2015)

Porém, esta é uma lei de pouca aplicabilidade, haja vista que a sua aplicação não proíbe a prática do *cyberbullying* conforme será comprovado a seguir.

Como há de se saber, a pratica de *bullying* e *cyberbullying* nos Estados Unidos da América acontecem com bastante frequência e em 1999 houve um massacre, tendo como causa o *bullying*, no Instituto Columbine, do estado do Colorado. Esse estado norte-americano possuía leis anti-*bullying* e aplicava programas de prevenção na escola envolvida (FIORILLO e CONTE, 2016, p. 271).

Contudo, tais leis do programa de prevenção são vistas como violação ao direito civil. Na lei, há sim a tentativa de prevenção, mas a punição fica inerte, logo, tais leis são irrelevantes.

No âmbito cível, é possível fazer-se a aplicação da analogia na ausência de uma legislação especifica, então, cabe ao magistrado operar com as demais ferramentas que lhe estão disponíveis. Porém, o problema está na esfera criminal, pois segundo o princípio da legalidade não é possível fazer a aplicação da analogia *in mallam partem*, pois o réu poderia sair prejudicado e a conduta praticada pelo mesmo deve-se enquadrar perfeitamente à descrição típica.

Sendo assim, na esfera criminal o que se utilizaria não seria a analogia, por proibição, mas sim, seria necessário que houvesse uma norma regulamentando os praticantes de *cyberbullying*.

Logo, a maneira em que o crime de *cyberbullying* é tratado em nosso ordenamento jurídico brasileiro é ineficaz por conta da falta de ferramentas e mecanismos para fazer o combate, e se torna imprescindível que tipifiquem o *cyberbullying* como crime.

## 2.4. MÉTODOS PARA COMBATER O *CYBERBULLYING*

Como já abordado neste trabalho, o ordenamento jurídico brasileiro é ineficaz no que tange ao crime de *cyberbullying*. Portanto, como haverá um combate de êxito nesse crime se nem mesmo os códigos estão preparados? Com isso, como uma maneira de efetiva diminuição da sua ocorrência ou até

mesmo o fim, é primordial que o *cyberbullying* seja enfrentado de uma outra forma, mais detalhadamente, ser tipificado como crime.

A Lei nº 13.185/15, sem sombra de dúvida foi um grande avanço jurídico em relação ao *cyberbullying*, muito embora haja lacunas a serem preenchidas. Os praticantes desse crime, cientes dessas brechas deixadas pelo legislador, acabam cometendo o crime pelo simples fato de saberem que não haverá punição, e a cada dia que passa, o percentual de vítimas aumenta.

O ordenamento jurídico brasileiro precisa levar como base os modelos utilizados por outros países. Por exemplo, em Cingapura, há um conjunto de leis direcionadas apenas às práticas antissociais como o *cyberbullying*, não direcionando apenas esse fenômeno aos meios escolares, mas também para as demais áreas, por exemplo, os locais de trabalho.

Essa tipificação conferiria ao *cyberbullying* a seriedade e a atenção compatíveis com o potencial ofensivo que o fenômeno merece. Contudo, a tipificação penal do *cyberbullying* como crime não deve ser entendida como a solução para o problema, mas sim para amenizá-lo, intimidando um maior crescimento dessa violência (FRANÇA, 2014). À vista disso, é preciso que o direito tipifique delitos como o *cyberbullying* com o intuito de promover segurança, proteção e o mais essencial, a privacidade das pessoas para que elas não sejam prejudicadas.

Muito embora não haja um método certo para impedir o *cyberbullying*, existem outros meios para combate-lo. É preciso incentivar a vítima, que na maioria das vezes são os jovens, a levar a prática desse crime ao conhecimento dos pais e professores. Uma outra forma seria salvar no próprio computador ou celular todas e quaisquer provas que vieram do *cyberbullying*. Muitas dessas provas poderão ser utilizadas para identificar e até mesmo punir.

Os colégios, em especial, precisam disciplinar duramente no que diz respeito ao *cyberbullying*. Esse crime é extremamente perigoso e nocivo, e jamais poderá ser aceitado. Assim sendo, houveram inúmeros casos em que as vítimas tiraram a própria vida por conta de serem humilhados, expostos e agredidos pelo *cyberbullying*.

Nesses casos, pais e educadores necessariamente precisam estar presentes para auxilia-los a fim de proteger crianças e adolescentes dessa prática covarde. Ademais, caso uma pessoa esteja sendo vítima de *cyberbullying*, a orientação é de buscar uma delegacia e registrar um boletim de ocorrência, e em havendo suspeito, indica-lo. Também poderá se ingressar com uma ação judicial contra o provedor de serviço, para que se possa rastrear dados do responsável pelo conteúdo enviado.

Segundo a advogada especialista em crimes virtuais, Gisele Truzzi, descoberto o suspeito, caberá ação judicial na esfera cível, com indenização, e ação judicial na esfera criminal, para punição do agressor. “Existe também a possibilidade de exclusão do conteúdo, por meio de notificação extrajudicial aos sites que hospedam o conteúdo ofensivo” (TRUZZI, 2007), explicou.

## 2.5. POSSIBILIDADE DE AÇÃO PENAL POR C*YBERBULLYING* SEM PROVAS

Como há de se notar, todo e qualquer operador do Direito sabe que em qualquer caso judicial são imprescindíveis as provas processuais, isso para comprovar se tal fato é verdadeiro ou falso, além de levar o convencimento do magistrado sobre os atos ditos pelas partes em juízo. No caso de *cyberbullying* não é diferente, é necessário provas para saber onde o tipo penal se encaixa, *bullying* ou *cyberbullying*.

Segundo pesquisas feitas no site do Jus Brasil, grande parte das provas advém de provas testemunhais, mas por outro lado, se for possível as provas documentais têm grande valor para formar o convencimento do Juiz. Porém, no crime de *cyberbullying*, é complicado de conseguir provas documentais, isto porque nesse tipo de delito há muitos *hackers* que com grande facilidade podem deletar, por exemplo, aquela conversa que indicaria a autoria e a materialidade ou até mesmo a omissão por lado da vítima, que deixa de tirar um *printscreen* da tela que provaria o ato de agressão.

De acordo com uma notícia postada no G1, no ano de 2011, salienta que ‘’Ata notarial é emitido por cartórios de notas e pouco conhecido, mas muito útil. O tabelião registra exatamente o que está acontecendo em uma reunião, condomínio, página na internet.’’ Ademais, a pessoa se direciona até um cartório

e fará um breve relato dos fatos para o tabelião. De acordo com o artigo 411, I, do Código de Processo Civil (CPC): “Considera-se autêntico o documento quando: I - o tabelião reconhecer a firma do signatário”

À vista disso, a ata notarial está prevista legalmente dentro do CPC, admitindo tal documento como prova processual. Para haver a expedição desse documento hoje, está avaliado em torno de R$ 466,87 reais pela primeira folha e com adição de outras páginas é acrescido mais R$ 235,75 reais.

Como um processo é muito complexo, para o Juiz dar seu veredito final, as provas são as responsáveis por clarear e auxiliar o magistrado em uma futura decisão. As provas virtuais necessitam um pouco mais de cautela em relação às provas físicas, isso porque as mesmas podem ser facilmente adulteradas ou falsificadas.

Em não havendo provas documentais não quer dizer que o caso está totalmente perdido, basta procurar outros meios de prova para comprovar, como por exemplo as provas orais para que se tenha um impulsionamento do processo.

As provas judiciais são importantes para comprovarem a veracidade dos fatos ditos em juízo pelas partes, para que não fique nenhuma dúvida em relação ao caso. Uma prova pode desmentir uma testemunha ou o autor da ação, por conta disso, para que tenha uma melhor comprovação dos fatos descritos nos autos, é necessário escutar as testemunhas e produzir o máximo de provas.

Em consulta ao site Jus.com.br, foi publicado um artigo cuja autoria é de Rogério Tadeu Romano, onde, ele expõe a respeito das provas indiretas que se distinguem das provas diretas. Um meio de prova indireta seria a forma de presunções sobre um fato que ocorreu com a utilização do raciocínio lógico e consistente. Desta forma, assim salienta Romano:

> A presunção é a conclusão do silogismo, construído sobre uma premissa maior: a lei baseada na experiência. A presunção pode ser absoluta, que não admite uma prova em contrário e relativa, que a admite. É a presunção legal quando expressa em lei, e de fato, quando cabe ao juiz fazer o raciocínio lógico que a ela conduz a sua inteligência. (2013)

Desse modo, poderá o magistrado se utilizar desse raciocínio, sem a necessidade de uma prova física. Uma vez que advinda do raciocínio lógico será onde a prova terá seu valor. Conforme o artigo 370 do CPC de 2015, onde se estipula que “Caberá ao juiz, de ofício ou a requerimento da parte, determinar as provas necessárias ao julgamento do mérito “

Portanto, o Juiz, de oficio, poderá dizer quais e quantas provas serão produzidas para o processo, sejam elas por requerimento das partes pedindo a produção de provas necessárias ou de oficio do magistrado.

# 3. CAPÍTULO III - DIREITO DIGITAL COMO RESPOSTA ÀS NECESSIDADES SOCIAIS E LEGAIS NA ERA DIGITAL

A globalização da economia e da sociedade obrigou uma postura diferenciada do Direito, ampliando o pensamento jurídico de forma a abranger as relações interpessoais que são realizadas no mundo digital, surgindo daí a expressão Direito Digital.

Assim, o Direito Digital é uma junção entre o Direito e a ciência da computação, integrando conjuntos de normas, aplicações, conhecimentos e relações advindas do ambiente digital.

E como consequência desta interação e comunicação entre o meio virtual e as questões inerentes do convívio em sociedade, nasceu a necessidade de garantir a proteção jurídica de informações pessoais, informações financeiras e profissionais dos cidadãos.

Segundo Novo, se define o Direito Digital da seguinte forma:

> O Direito Digital é o resultado da relação entre a ciência do Direito e a Ciência da Computação sempre empregando novas tecnologias. Trata-se do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital.
>
> Essa nova ramificação jurídica corresponde ao conjunto de normas que visam tutelar as relações humanas e as violações comportamentais em ambientes digitais. Isto é, se com o uso da tecnologia, as pessoas

> enviam e recebem informações, realizam negócios, emitem opiniões etc., devem existir regras e princípios que orientem a conduta nesse meio. (NOVO, Posição 354)

Para os operadores do Direito, a tecnologia foi capaz de viabilizar ferramentas nas quais o profissional tem a possibilidade de simplificar e aperfeiçoar suas tarefas. Todavia, a tecnologia abriu portas para a prática de crimes, como, por exemplo, a violação de direito autoral. Com isso, autores se juntam para conseguir descobrir a autoria e a materialidade do delito.

Assim, o Direito Digital aborda todos os princípios fundamentais e institutos jurídicos que são aplicados até hoje. Para estudiosos da área, muito se diz que o Direito Digital está se tornando um ramo do Direito, porém é certo saber que o Direito Digital não possui autonomia cientifica pelo fato de não possuir institutos, fins, objeto e princípios próprios, levando em consideração que as demais áreas do Direito possuem todos esses pressupostos. À vista disso, não se pode afirmar que o Direito Digital se trata de uma nova área do Direito em si, mas sim de uma nova perspectiva, a qual pode ser compreendida como uma forma de influenciar a relação entre pessoas físicas e pessoas jurídicas em razão da grande utilização da tecnologia e por consequência acaba afetando o Direito de cada um desses sujeitos.

Neste cenário atual, o Direito deve seguir no mesmo sentido, acompanhando novas necessidades decorrentes das novas tecnologias que vão surgindo, isso para estabelecer regramentos que tenham a capacidade de normatizar todas as repercussões oriundas das novas tecnologias em todos os âmbitos do Direito.

O Direito Digital deixou de ser entendido como uma disciplina fechada, que visava apenas a esfera da tecnologia ou ambiente digital e passou também a regulamentar o Direito como um todo, passou-se a englobar todas as disciplinas do Direito, como, por exemplo, o Direito civil, criminal, contratual, tributário, autoral, constitucional, trabalhista, etc.

Assim, considerando a necessidade de solucionar os conflitos que começaram a surgir no âmbito digital, foi necessária a criação do Direito Digital,

ou seja, um regramento consubstanciado em matéria específica de enfrentamento das violações de direitos.

## 3.1. DIREITO DIGITAL E SUAS LEGISLAÇÕES

A normatização das relações jurídicas no ambiente digital ainda é muito precária e tímida se formos comparar com o grande volume de integração das pessoas na nova realidade das tecnologias. Por haver um grande crescimento de pessoas se utilizando dos aparelhos, a criminalidade também ganha bastante espaço e, por conta disso, dificulta ainda mais a criação de legislações para tutelar a pratica desses delitos.

No entanto, outras nações vêm tentando aos poucos buscar formas de legislar a respeito desse assunto, mas acabam encontrando um empecilho, que é a grande velocidade das mudanças no meio.

Conforme já explanado nos capítulos anteriores, já temos no Brasil, algumas leis que regulamentam os crimes virtuais. Além da adaptação das leis do mundo em nosso país, as principais normas cridas pelo Congresso Nacional foram:

- A lei dos crimes informáticos que também é conhecida por Lei Carolina Dieckmann (Lei 12.737/2012), na qual estabelece que certas condutas praticadas mediante uma tecnologia afim de invadir o dispositivo informático para a obtenção, destruição ou modificação de dados pessoais de certa pessoa;
- O Marco Civil da internet (12.965/2014), que é responsável por fixar regras básicas do uso da internet no Brasil além de determinar o mundo da internet é regulamentado pelo Direito Civil, consumidor, comercial, entre outros;
- O Código de Processo Civil de 2015 regulamenta o assunto, porém em escala menor, ou seja, cria normas para o desenvolvimento do processo judicial eletrônico;
- E por fim, a lei de acesso à informação (12.527/2011), que estabelece que as prestações de contas dos entes públicos com o

> uso da tecnologia da informação, ou seja, deixar público toda e qualquer despesa pública para consulta de qualquer um.

Assim sendo, podemos notar quão precária é a nossa legislação quando o assunto tratado é o crime informático. A legislação nacional ainda demanda de uma especialidade e maior profundidade no que diz respeito a esse assunto, até porque em muitos casos a legislação antiga não tem capacidade de proteger o cidadão, que tem um prejuízo pela prática desse crime.

Um dos desafios do meio digital nos dias atuais se faz pela insegurança jurídica. Tal falta de normatização sobrecarrega o sistema, por assim dizer, de forma que o operador do direito muitas vezes se encontra em difícil situação para resolver a demanda proposta pela sociedade.

Uma outra característica que faz com que haja uma dificuldade para a criação de boas normas seria a velocidade das mudanças tecnológicas. Muitas pessoas que têm um aparelho telefônico hoje em dia não tem um bom conhecimento de quais atos podem ou não serem praticados na internet, e em vista disso, as tecnologias conforme os anos passam acabam ficando ainda mais complexas. Logo, mesmo com o empenho dos legisladores sempre existe uma lacuna que acaba acarretando em incerteza sobre as normas que regulam o ambiente digital.

## 3.2. DESAFIOS DO DIREITO DIGITAL

Como já abordado nesse trabalho, o Direito Digital ainda é um ramo do Direito considerado novo e, por conta disso, há uma carência de normas para regulamentar a área. Em vista disso, o direito digital denota uma série de desafios a serem abatidos, para se ter uma boa aplicação das regras e regimentos legais aos casos concretos com êxito. E para se chegar a um bom resultado, é necessário ter normas regulando a área além do operador do Direito ter uma boa capacidade de interpretação e raciocínio lógico.

Portanto, ter conhecimento de técnicas sobre programação, estar por dentro das regras dos cibercrimes e segurança da informação é um diferencial para vencer os desafios que a esfera apresenta. Afinal de contas, ter

conhecimento sobre esse tipo de informações colabora com a aplicação da lei ao caso concreto e a adequação das demais normas.

Para tanto, alguns órgãos reguladores manifestaram a ideia de que uma normatização ágil pode trazer mais desafios do que soluções, haja vista que quando se trata de tecnologias sabemos que o desenvolvimento é muito constante, logo, nem sempre criar novas normas pode ser a melhor solução.

Todavia, conforme a sociedade apresenta novas ocorrências de vazamentos de dados pessoais, clonagem de cartões, fraudes envolvendo negócios digitais ou até mesmo outros crimes envolvendo a tecnologia, o direito tenta suprir com alternativas distintas para se ter a resolução dos casos, complementando as lacunas deixadas pelas leis.

No entanto, sabe-se que o sistema jurídico tem suas dificuldades para a criação de novas leis que não deixem brechas, consequentemente, produzir normas que acompanhem todos os avanços e a velocidade da criação de novas tecnologias é, de fato, impossível. O correto seria que os profissionais da área se especializassem ainda mais para que com o conhecimento consigam ter resultados favoráveis. E para que isso aconteça, o operador do direito deve ser interessado na área tecnológica, se manter sempre informado sobre as novas tecnologias e informações a respeito do tema.

O profissional do direito digital deve pensar além para conseguir soluções rápidas para a manutenção da segurança jurídica, é imprescindível esse profissional para defender vítimas de crimes digitais, apurar a autoria e materialidade do crime. Além de defender, os responsáveis também têm o dever de conscientizar as pessoas de todos os riscos do mundo digital, colaborando para uma sociedade mais segura e evoluída.

Somente a título de esclarecimento sobre a necessidade premente de um regramento específico que determine minimamente os limites de atuação na era digital, podemos citar o caso atual que tem sido divulgado nas mídias televisivas acerca do assunto da *fake news,* no qual o atual presidente Jair Messias Bolsonaro manifestou-se a respeito da criação de lei que combateria notícias falsas publicadas na web. Por conseguinte, o presidente diz que a lei poderia

infringir ou até mesmo limitar a liberdade de expressão que é um direito fundamental previsto expressamente em nossa Constituição Federal.

Bolsonaro salientou que um regramento mais rigoroso no mundo das redes sociais poderia obstar a livre manifestação de opiniões e caso alguém se sentisse prejudicado, deveria se socorrer do Poder Judiciário. Em um encontro realizado em frente ao Palácio da Alvorada, Jair Messias Bolsonaro disse:

> Vocês sabem que a liberdade de expressão é essencial se você quer falar em democracia. O Congresso está discutindo aqui, já passou no Senado, está na Câmara, seria a lei das fake news. Acho que é mais uma maneira de botar limites na liberdade de expressão.
>
> Você nunca vai saber qual o limite. Vai virar um terreno onde você vai perder a liberdade. Você não vai mais poder se manifestar sobre nada. E [foi] essa liberdade de expressão, essas mídias sociais, que me botou aqui na Presidência[9] (2020)

Com base nisso, ao analisar o artigo XIX da Declaração Universal dos Direitos Humanos fica evidente que se trata de um direito fundamental. O supracitado artigo estipula da seguinte forma:

> Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão (1948)

A Constituição Federal em seu inciso IV do artigo 5º traz a garantia da liberdade de pensamento, expressão e manifestação do seguinte modo “IV - é livre a manifestação do pensamento, sendo vedado o anonimato”

E continua no inciso IX, que assegura os seguintes direitos: “IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”

---

[9] Parte da entrevista pode ser conferida no seguinte link. <https://agenciabrasil.ebc.com.br/politica/noticia/2020-07/bolsonaro-diz-que-projeto-de-fake-news-limita-liberdade-de-expressao>

O princípio da liberdade de expressão é assegurado pela Constituição Federal para impedir com que os poderes do Estado não oprimam tal direito. É garantia assegurada a qualquer indivíduo de se manifestar, opinar ou criar ideias de todos os tipos de assunto. Por esse motivo, é importante que haja democracia e uma sociedade civil participativa e informada das informações atuais para que possa contribuir de modo positivo à vida pública.

É oportuno dizer que, por mais que seja um direito que assegura a livre manifestação e formação de opiniões, a liberdade de expressão não é um direito absoluto, logo, determinadas manifestações poderão incumbir em crimes como a calúnia, difamação e injúria, o que é capaz originar um processo futuro.

Por esse motivo, existe um jargão no qual se expressa da seguinte forma “O seu direito termina quando começa o direito do outro’’, isto por conta de que, se uma pessoa tem o direito de liberdade de expressão, as demais pessoas possuem a dignidade da pessoa humana, à imagem, à honra e o direito à vida privada. Destarte, exposto isso, fica evidente que a liberdade de expressão é sim imprescindível e fundamental para todo ser humano, porém, não pode ser utilizada de pretexto para o cometimento de crimes e práticas ilícitas.

No Brasil, há um histórico que vem crescendo em relação aos meios de comunicação onde todos possuem uma relação com esses aparelhos, estamos vivendo em um mundo cada vez mais impessoal, onde as pessoas utilizam as redes sociais para se expressar da forma que pensam sobre determinado assunto, acreditando a rigor que estão protegidas atrás de seus aparelhos. Contudo, neles, vem integrada a liberdade de expressão, que permite se expressar livremente no meio ambiente virtual.

Portanto, se formos analisar que no ano de 2012 houve um crime nacionalmente conhecido e que passou a receber o nome da atriz global Carolina Dieckmann e originou a criação da lei 12.737/2012, e no ano de 2020 ainda há especulações e proliferação no que diz respeito a fake news, podemos notar que os crimes virtuais ainda não possuem um regramento severo, não há controle. Em vista disso, o STF tem interpretado normas infraconstitucionais em relação aos atos ilícitos praticados em meio ao mundo virtual.

# CONSIDERAÇÕES FINAIS

Durante este trabalho, pode-se concluir que a lei 12.737/2012 foi um grande avanço para a nossa legislação no que tange a invasão de aparelhos eletrônicos para a obtenção de dados particulares de terceiros. Em vista disso, por se tratar de dados pessoais vazados, o Projeto de Lei n. 2.793/11 em comparação aos demais projetos, teve uma rápida aprovação dentro das casas legislativas.

Portanto, até que a referida lei entrasse em vigência, não havia nenhuma tipificação penal em nossos códigos que tutelavam dados pessoais vazados, com isso, foi uma inovação dentro dos textos do Código Penal, tipificando o dispositivo informático como crime.

À vista disso, a Lei n. 12.965/2014 surgiu com o intuito de cessar alguns crimes praticados mediante a internet, e fazer com que o meio ambiente virtual seja um marco mais amplo e seguro para todos os usuários da rede, bem como para todos os tipos de sites.

Aproveitando-se da segurança e privacidade concedida pelo Marco Civil da Internet, podemos dizer que, por mais que a internet seja uma ferramenta imprescindível para muitos usuários, era evidente que a legislação brasileira estava precisando de uma regulamentação para garantir que os dados pessoais não fossem vazados no ambiente virtual, e que os responsáveis fossem culpados pelos atos ilícitos cometidos.

O *Cyberbullying*, por sua vez, agregou dois conceitos para a sua formação, onde, deixou de ser aquele *bullying* presencial que era usado somente em ambientes escolares e passou-se a ser introduzido ao meio virtual.

O crime de *cyberbullying* é composto por uma agressão indireta, e que com esse estudo podemos observar que pode ser cometido de diversas formas se valendo da utilização de uma conexão com a internet.

Por fim, mas não menos importante, o Direito Digital. Por conta da globalização da sociedade, obrigou-se o direito a ter uma postura diferente, um pensamento que abrangesse as relações no mundo virtual, dando, então, a nomenclatura de Direito Digital.

O Direito Digital é considerado uma relação que incumbe a ciência do Direito e a ciência da computação. Nele vem integrado normas, aplicações, conhecimentos e relações jurídicas. É contido também o importantíssimo princípio da liberdade de expressão, o qual é assegurado por nossa Constituição Federal como direito basilar.

# REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO, Loraynne. **A cada minuto, 54 pessoas são vítimas de crimes virtuais no país**. Edição do Brasil. Belo Horizonte, 2017. Disponível em: <<http://edicaodobrasil.com.br/2017/08/03/cada-minuto-54-pessoas-sao-vitimas-de-crimes-virtuais-no-pais/>>

ÁVILA, Humberto. **Teoria dos Princípios: da definição à aplicação dos princípios jurídicos**. 15 ed. São Paulo: Malheiros, 2014.

BAUMANN, Z. **O mal-estar da Pós-Modernidade**. Rio de Janeiro: Jorge Zahar, 1998

BRASIL. **Constituição Federal.** Brasília: Planalto, 1988.

BRASIL. **Código de Processo Civil.** Brasília: Planalto, 2015

BRASIL. **Código Penal.** Rio de Janeiro: Catete, 1940

BRASIL. **Lei n. 12.737 – Lei Carolina Dieckmann**. Brasília: Planalto, 2012

BRASIL. **Lei n. 12.735 – Lei Azeredo.** Brasília: Planalto, 2012

BRASIL. **Lei n. 12.965 – Marco Civil da Internet.** Brasília: Planalto, 2014

BRASIL. **Lei 13.185 – Lei do Programa de Combate à Intimidação Sistemática.** Brasília: Planalto, 2015

BRITO, Ana. **Documento pouco conhecido pode ser usado como prova na Justiça.** Portal G1. 2011. Disponível em: <<https://g1.globo.com/jornal-hoje/noticia/2011/05/documento-pouco-conhecido-pode-ser-usado-como-prova-na-justica.html>>

CÂMARA DOS DEPUTADOS. **Legislação atual já pune cyberbullying e cyberstalking, diz advogada à CPI: Fonte: Agência Câmara de Notícias.** 2016. Disponível em: https://www.camara.leg.br/noticias/482215-legislacao/atual/jápune-cyberbulying-e-cyberstalking-diz-advogada-a-cpi/.

CAPEZ, Fernando. **Curso de direito penal**. 17 ed. São Paulo: Saraiva, 2012. Vol. 1, parte geral: (arts. 1º a 120).

CAPEZ, Fernando; PRADO, Stela. **Código Penal Comentado**. 7. ed. São Paulo: Saraiva, 2016.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Portal Âmbito Jurídico. 2012. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529 https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>

CGI. **Faixa etária das pessoas que utilizam a internet.** 2018. Disponível em: <<https://www.cgi.br/noticia/releases/cresce-numero-de-criancas-e-adolescentes-que-buscam-noticias-na-internet-aponta-cetic-br/>>

DICIONARIO DIREITO. **O que são Crimes Virtuais?** Portal Dicionário Direito. Disponível em: <https://dicionariodireito.com.br/crimes-virtuais>

FIORILLI, C.A.P; CONTE, P.C. **Crimes no meio ambiente digital e a sociedade da informação**. São Paulo: Saraiva, 2ª ed. 2016

FRANÇA, Amlyn Thayanne Santos. **Aspectos gerais sobre o bullying e sua tipificação penal no ordenamento jurídico brasileiro**. Boletim Jurídico, 2014. Disponível em: << https://www.boletimjuridico.com.br/artigos/direito-penal/2991/aspectos-gerais-bullying-tipificacao-penal-ordenamento-juridico-brasileiro>>

JESUS, Damásio E. de. **Stalking.** Portal Jus. 2008. Disponível em: <<https://jus.com.br/artigos/10846/stalking>>

KERR, Vera Kaiser Sanches. **A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet.** São Paulo: USP, 2011. Dissertação de Mestrado.

LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo. Editora Atlas S.A. 2014.

MELO, Karine. **Bolsonaro diz que projeto de fake news limita liberdade de expressão.** Agência Brasil. 2020. Disponível em: <<https://agenciabrasil.ebc.com.br/politica/noticia/2020-07/bolsonaro-diz-que-projeto-de-fake-news-limita-liberdade-de-expressão>>

NETO, M.F.; SANTOS, J. E.L; GIMENES, V.E. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, 1ª ed. 2012

NOVA ESCOLA. **O que fazer para evitar o bullying?** Portal Nova Escola Online. 2016. Disponível em: <https://novaescola.org.br/conteudo/282/o-que-fazer-para-evitar -o-bullying.>

NOVO, Benigno Núñez. **Direito Digital [ebook].** Amazon, s/d.

ONU. **Declaração Universal dos Direitos Humanos.** Genebra, 1948. Disponível em: <<https://nacoesunidas.org/direitoshumanos/declaracao/>>.

ROCHA, F. L. X. *A dignidade da pessoa humana no direito constitucional contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial, de Luís Roberto Barroso*. In **Revista Controle - Doutrina e Artigos**, v. 12, n. 2, p. 341-345, 25 nov. 2016.

ROMANO, Rogério Tadeu. **Dos sistemas sobre a apreciação da prova**. Portal Jus. 2013. Disponível em: <https://jus.com.br/artigos/23713/dos-sistemas-sobre-a-apreciacao-da-prova/2>

SCHREIBER, Fernando Cesar de Castro e ANTUNES, Maria Cristina. *Cyberbullying: do virtual ao psicológico*. **Bol. - Acad. Paul. Psicol. [online]**. 2015, vol.35, n.88, pp. 109-125.

TRUZZI, Gisele; DAOUN, Alexandre. *Crimes informáticos: o direito penal na era da informação*. In **International Conference on Forensic Computer Science and Cyber Law.** Brasília: UnB, 2007. Disponível em: <http://www.icofcs.org/2007/ICoFCS2007-pp17.pdf>.

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