UNIVERSIDADE PRESBITERIANA MACKENZIE

GABRIEL AUGUSTO GONÇALVES LAZZARINI

CRIMES VIRTUAIS: UMA ANÁLISE SOBRE A CARÊNCIA DE LEIS PARA COMBATER SUAS ESPECIFICIDADES

São Paulo

2020

GABRIEL AUGUSTO GONÇALVES LAZZARINI

CRIMES VIRTUAIS: UMA ANÁLISE SOBRE A CARÊNCIA DE LEIS PARA COMBATER SUAS ESPECIFICIDADES

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

ORIENTADORA: THAMARA DUARTE CUNHA MEDEIROS

São Paulo

2020

GABRIEL AUGUSTO GONÇALVES LAZZARINI

CRIMES VIRTUAIS: UMA ANÁLISE SOBRE A CARÊNCIA DE LEIS PARA COMBATER SUAS ESPECIFICIDADES

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovado em:

BANCA EXAMINADORA

Examinadora: Renata da Rocha

Examinadora: Márcia Cristina de Souza Alvim

CRIMES VIRTUAIS: UMA ANÁLISE SOBRE A CARÊNCIA DE LEIS PARA COMBATER SUAS ESPECIFICIDADES

Gabriel Augusto Gonçalves Lazzarini

RESUMO

Este artigo propõe-se a fazer uma rápida análise sobre o advento da internet e como o Direito Digital brasileiro está lidando com os crimes que são praticados por meio desta, além de apresentar os desafios que a legislação precisa superar. Com a internet sendo introduzida à realidade de cada vez mais pessoas, deparamo-nos com novos meios de ataques a bens jurídicos, como por exemplo furto e roubo de dados pessoais e nesse sentido há a necessidade de impedir tais práticas ilícitas, o que somente será viável com a criação de leis mais especificas, como por exemplo a Lei Carolina Dieckmann (Lei n. 12.737/12) e o Marco Civil da Internet (Lei n. 12.965/14), que foram concebidas através de grande pressão midiática, porém ainda não são o bastante para proteger os cidadãos dos cibercriminosos.

PALAVRAS-CHAVE: Direito Digital, crimes virtuais, internet.

ABSTRACT

This article proposes to make a quick analysis about the advent of the internet and how the Brazilian Digital Law is dealing with the crimes that are practiced through it, besides presenting the challenges that the legislation needs to overcome. With the internet being introduced to the reality of more and more people, we are faced with new ways of obtaining legal assets, such as theft and steal of personal data and in that sense there is a need to prevent such illegal practices, which is only feasible with the creation of more specific laws, such as the Carolina Dieckmann Law (Law 12.737/12) and the Marco Civil da Internet (Law 12.965/14), which were conceived through great media pressure, but are still not enough for protect citizens from cybercriminals.

KEYWORDS: Digital Law, virtual crimes, internet.

1 INTRODUÇÃO

A internet veio para revolucionar a forma como a sociedade estabelece suas relações. Ela está presente diariamente no cotidiano de milhões de pessoas, o que faz com que muita informação seja trocada através dela. Em muitos casos, as relações sociais se dão mais através da internet do que pessoalmente, visto que ela é um importante pilar da globalização de um

modo geral, fazendo com que as pessoas possam se conectar em tempo real em qualquer parte do mundo que estejam.

É inegável que a internet trouxe inúmeros benefícios que facilitaram nossa vida. Porém, juntamente com isso, muitos novos tipos de delitos surgiram, e o Direito está tendo que se reinventar para conseguir acompanhar essas mudanças que rapidamente acontecem, e cada dia mais aparecem novas formas de obter vantagem ilícita em decorrência de seu uso, os chamados crimes virtuais.

Diante disso, surgem algumas questões. Como os crimes se manifestam no ciberespaço? O ordenamento jurídico penal já dispõe de normativas para tutelar os bens jurídicos no âmbito da cibercriminalidade?

Quanto mais cresce o número de pessoas que tem acesso à internet, maior é a incidência de crimes virtuais. Diante dessa realidade, surge um anseio para que normas eficazes sejam criadas a fim de que se diminua esse tipo de crime e que os criminosos sejam devidamente punidos.

Isto posto, o presente artigo tem como objetivo fazer uma análise dissertativo-analítica sobre a tutela penal dos crimes virtuais , bem como uma reflexão sobre os desafios jurídicos que sugerem essa nova manifestação da criminalidade, a partir de uma pesquisa bibliográfica em livros, doutrinas, leis, artigos científicos, jornais e publicações disponíveis na biblioteca online do Mackenzie e também no ambiente acadêmico virtual.

2 A INTERNET NO BRASIL

Podemos considerar que a internet é a mãe de todas as redes, pois conecta todos os computadores ao redor do mundo. Ela teve sua origem na década de 1960. O governo americano, para conseguir sincronizar seus computadores, criou a ARPANET (*Advamced Research Projects Agency*), para que não houvesse apenas um centro de comando caso algum ataque nuclear viesse a atacá-los durante a Guerra Fria (GOUVÊA, 1997, p. 36).

Inicialmente, o experimento foi testado pela ARPA nas universidades, e conseguiram interligar o Stanford Institute, a Universidade da Califórnia e a Universidade de Utah. Passada a Guerra Fria, a ARPANET, considerada a precursora da internet, começou a ser disseminada tanto no meio acadêmico quanto no meio científico. Já no ano de 1987 foi permitido o início seu uso comercial (KUMMER, 2017).

Já no Brasil, a internet foi implementada no ano de 1992, e, inicialmente, conectou as principais universidades, porém era utilizada apenas para a troca de e-mails. Entretanto, em

1995, iniciou-se seu uso comercial no país. Ainda neste ano, foi criado o Comitê Gestor da Internet no Brasil (CGI.br), cujo propósito era propiciar a qualidade técnica da internet no Brasil e difundir os serviços que estavam sendo ofertados (WENDT; JORGE, 2017).

Hoje em dia a internet mudou completamente o modo como a troca de informação é compartilhada. Deixou de existir a Internet discada para dar lugar à Banda Larga e às redes 3G e 4G a custos significativamente inferiores, o que possibilitou que grande parte da população atualmente tenha acesso à rede (KUMMER, 2017).

Segundo pesquisa realizada pela TIC Domicílios 2019, feita pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), a cada quatro brasileiros, três tem acesso à internet, o que corresponde a 134 milhões de pessoas. Dentre os dispositivos de acesso, 99% dos usuários conseguem navegar através de smartphones. Apesar de predominarem os smartphones, outras maneiras de acessar a internet são através de computadores (42%), Televisões (37%) e consoles de videogames (9%). Desses usuários, 90% afirmam utilizar a internet diariamente (VALENTE, 2020).

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).

Ou seja, toda essa evolução tecnológica nos fez caminhar a passos largos para o que podemos chamar de sociedade da informação. Porém, da mesma forma, os sistemas de defesa passaram a depender muito mais da informática, visto que, apesar da internet ter trazido ao mundo importantes evoluções acerca do compartilhamento de informações, ao mesmo passo trouxe grandes ameaças devido ao seu uso indevido.

2.1 O DIREITO E A INTERNET

O Direito e a Informática estão cada vez mais correlacionados, havendo até quem defenda que deve ser criado um novo ramo do Direito para discutir tais questões. Uma vez que o Direito trata dos princípios e normas que regem a sociedade visando que esta consiga viver em harmonia, este tem o dever de punir os cidadãos que se utilizam práticas ilegais. Então o Direito deve se adequar a todas as novidades que aparecem no meio social.

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 estratégicas, 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 houveram 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.

Podemos concluir que as revoluções tecnológicas não ofereceram apenas benefícios para a sociedade, pois quanto mais aumenta e evolui o vasto mundo digital, mais surgem novos crimes e pessoas de má índole querendo prejudicar algo ou alguém de alguma forma.

3 CRIMES VIRTUAIS

Crimes virtuais, cybercrimes, crimes tecnológicos, crimes informáticos, crimes de computador, infocrimes, são apenas algumas das várias denominações que podem ser utilizadas para as condutas lesivas que podem ser praticadas através de dispositivos eletrônicos ou contra sistemas de informática.

Como bem 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).

De acordo com Wendt e Jorge (2017, p. 31), tais condutas indevidas podem ser classificadas em "crimes cibernéticos" e "ações prejudiciais atípicas". "Ações prejudiciais atípicas" são condutas que geram prejuízo para a vítima porém não há tipificação penal, não podendo punir o autor no âmbito criminal. Já os "crimes cibernéticos" podem ser "abertos" (impróprios) ou "exclusivamente cibernéticos" (próprios). "Abertos" são os que podem ser cometidos com ou sem a utilização do computador, sendo este apenas um meio para sua execução. Destarte, os crimes "exclusivamente cibernéticos" se distinguem pois exclusivamente só poderão ser realizados mediante o uso de computadores ou outros dispositivos eletrônicos com acesso à internet.

Dentre os crimes cibernéticos abertos, ainda podemos diferenciar os crimes puros, comuns e mistos. Os "puros" acontecem apenas em ambiente virtual através de dispositivos próprios. Os "comuns" logram êxito tanto no meio digital quanto fora dele. Já os crimes "mistos" usufruem do meio digital como sua maneira de execução, visando obter bem jurídico ou vantagem econômica (BITTENCOURT, 2019, p. 10).

Figura 1 – Condutas indevidas praticadas por computador

CONDUTAS INDEVIDAS PRATICADAS POR COMPUTADOR		
AÇÕES PREJUDICIAIS ATÍPICAS	**CRIMES CIBERNÉTICOS ABERTOS**	**CRIMES EXCLUSIVAMENTE CIBERNÉTICOS**
✓ Invasão de computador sem o fim de obter, adulterar ou excluir dados e informações. ✓ Difusão de *phishing scam*	✓ Crimes contra a honra ✓ Ameaça ✓ Pornografia infantil ✓ Estelionato ✓ Furto mediante fraude ✓ Racismo ✓ Apologia ao crime ✓ Falsa identidade ✓ Concorrência desleal ✓ Tráfico de drogas	✓ Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. ✓ Interceptação telemática ilegal ✓ Pornografia infantil por meio de sistema de informática ✓ Corrupção de menores em sala de bate papo ✓ Crimes contra a urna eletrônica

Fonte: Wendt; Jorge, 2017, p. 33

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).

Os crimes virtuais estão aumentando ano após ano. Isso se dá pela falsa sensação de anonimato por parte dos criminosos, que encontram na rede um ambiente solícito à prática de crimes, e também pela falta de cuidado dos usuários, que muitas vezes não sabem onde estão inserindo seus dados, o que favorece práticas criminosas.

3.1 PORNOGRAFIA INFANTIL

De acordo com Moisés Cassanti:

> *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 que o 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, acaba fazendo 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).

Cumpre destacar que 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.*
> *§ 1o Nas mesmas penas incorre quem:*
> *I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;*
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

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 Direitos da Criança, adotada pela Assembleia Geral das Nações Unidas, o que implica a incidência do inciso V do art. 109 da Constituição Federal.

3.2 CRIMES CONTRA A HONRA

Todas as pessoas têm o direito de expressar suas opiniões, ainda mais na internet, ambiente amplamente democrático. Com tamanha liberdade, é um local que reúne diversos pontos de vista sobre os mais variados assuntos. Porém, apesar de muitos usuários acharem que podem falar tudo o que quiserem sem pensar nas consequências, caso faça algum comentário ofensivo, será responsabilizado.

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), caso a calúnia aconteça através de um e-mail, todos que receberem e compartilharem podem ser acusadas de coautoria. No caso da difamação, compete retratação pública caso haja arrependimento. E a injúria é a acusação de ato ofensivo à imagem de outrem.

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.

3.3 ESTELIONATO

O crime de estelionato se caracteriza quando o agente visa enganar alguém com uma história fictícia para obter algum tipo de vantagem ilícita perante a vítima à qual o estelionatário iludiu. A principal diferença do estelionato em relação aos outros crimes é que este se dá por meio do engano, induzindo ou mantendo a vítima em erro.

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 banco e 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).

3.4 INVASÃO DE PRIVACIDADE

A privacidade é um quesito de extrema importância, sendo considerada um direito fundamental, e sua violação é vedada pelo artigo 5º, inciso X da Constituição Federal de 1998. Porém, no contexto da sociedade contemporânea, ancorada na liberdade e transparência da informação por meio da internet, esta garantia constitucional está em constante vulnerabilidade.

> *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 à vida, 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 sua violação;*

O crime de invasão de privacidade no âmbito da internet constitui-se no caso de o agente adentrar o aparelho informático de alguém, que pode ou não estar ligado na rede, através da violação da segurança deste, com o objetivo ou não de obter, adulterar ou excluir informações e dados sem o consentimento expresso ou tácito do proprietário do aparelho ou implantar meios para auferir vantagem ilegal.

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 acessar informações 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 nº 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) meses a 1 (um) ano, e multa.

Contudo, por vezes, mesmo que haja o consentimento do dono do dispositivo para que determinada pessoa possa 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, constituindo danos 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 que eles caem na 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)

Também temos mais um tipo diferente de captação de dados que invadem a privacidade dos usuários da rede. Muitos portais, provedores de e-mails e adjacentes captam informações pessoais dos usuários através de quais conteúdos este está buscando, quais seus gostos, hobbys, atividades e tudo o que a pessoa faz na internet, para que possam enviar anúncios personalizados para estes. Não é incomum aparecer uma propaganda de algo que pesquisamos anteriormente, e até de algo 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 claro as consequências jurídicas causadas por esse fato.

Todos esses episódios, até certo ponto recentes, geram uma insegurança jurídica acerca do uso da internet e a garantia dos dados pessoais de seus usuários.

4 LEGISLAÇÕES PENAIS NO ÂMBITO DIGITAL

Um dos maiores desafios para o Brasil no âmbito dos crimes virtuais, sempre foi trata-los com um Código Penal muito antigo, dos tempos do rádio. Levando em conta que o direito deve operar apenas para defender os bens mais importantes e indispensáveis da sociedade e interferir o menos possível na vida dos cidadãos, não foi nada fácil sancionar leis que tipificassem crimes virtuais. Neste diapasão, considerando o amparo destinado aos bens jurídicos clássicos, também precisávamos de amparo perante os delitos praticados em meios digitais (MILAGRE, 2016, p. 47).

Não se pode negar que uma legislação nesse sentido se fazia necessária, visto que em ambiente digital milhares de informações são trocadas por segundo, e de todas as esferas da sociedade, desde as mais abrangentes até as mais específicas. Desde uma simples conversa em aplicativos de mensagens instantâneas até transações bancárias e financeiras para qualquer lugar do mundo, tudo isso por meio da rede informática.

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 Dieckman, e a Lei n. 12.737/2012, que leva seu nome, foi sancionada em novembro desse mesmo ano.

Ao estudarmos os crimes que se dão por meio digital, podemos refletir que estes podem ferir outros bens jurídicos que não os tradicionais. Os criminosos hoje em dia não visam somente bens jurídicos já tutelados como o patrimônio, a vida e etc., mas também os sistemas, as informações e tudo que envolve o ambiente virtual. Daí a necessidade de legislação específica.

Segundo Brito (2013, p. 780) expõe, 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 da informação como bem a ser amparado.

4.1 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 aprovaram o PL n. 35/2012., originado pelo PL n. 2.793/2011. Foi a primeira lei do ordenamento jurídico brasileiro a tratar dos crimes cometidos através da internet.

> *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 definidas em 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 constitui crime 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 dados ou 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, municipal ou do Distrito Federal.*

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 Municípios ou 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, e caso verifique-se um crime mais grave, incide no parágrafo 3º do artigo 154-A do CP.

> *§ 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 definidas em 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 constitui crime 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 dados ou 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, municipal ou do Distrito Federal.*

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 as interrupções.

> *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.*
> *§ 1o Incorre na mesma pena quem interrompe serviço telemático ou de informa- ção de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.*
> *§ 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade 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, equiparando documento 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 cartão de crédito ou débito.*

A chegada dessa lei, ainda que tardia a equivocada, mostrou a aflição do Estado em amparar as muitas transformações advindas da tecnologia, fazendo-se de suma importância a apuração de parâmetros que buscam proteger a liberdade individual das pessoas. Porém, parece que essa lei trouxe mudanças muito específicas, visando criminalizar um fato isolado, deixando claro a correria em promulgá-la devido ao forte apelo social.

Senão vejamos, caso uma pessoa peça emprestado o dispositivo eletrônico de outra, e essa consinta, caso a pessoa que pediu emprestado obtenha ou exclua informações pessoais, fotos, vídeos ou qualquer outra coisa, não poderá incidir no crime previsto no artigo 154-A, isto porque sua redação deixa claro que deve haver a violação do mecanismo de segurança para que se caracterize o crime, e, no caso em comento, o acesso às informações se deu com o consentimento da vítima. Além do mais, quais seriam esses mecanismos de segurança?

Muitas são as críticas em relação à eficácia da lei devido as várias lacunas que estão presentes nela. O principal ponto é essa necessidade de haver mecanismo de segurança. Sabemos que grande parte das pessoas que usufruem da internet nem imaginam que precisam usar mecanismos de segurança, como antivírus ou senhas, ou talvez não tenham condições financeiras de contratar tais serviços, fazendo com que a lei não seja válida para toda a população. Além disso, temos o fato de existir um enorme volume de termos possíveis em seu texto, permitindo distintas compreensões, o que facilita a defesa do infrator.

O que enfraquece a lei é que existem diversas maneiras dos criminosos invadirem os dispositivos alheios sem que haja punição para tal, fazendo com que esta não cumpra o principal objetivo de sua criação.

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, não confio na eficácia preventiva dessa lei. (GOMES, 2013).

4.2 MARCO CIVIL DA INTERNET (LEI N. 12.965/2014)

Desde a chegada da internet para sua utilização em sociedade, até sua posição consolidada de fenômeno que mudaria para sempre o cotidiano das pessoas, a principal preocupação jurídica que se concebeu no país era como tal novidade se encaixaria no âmbito do direito penal. Os crimes que são praticados através da internet têm muita repercussão social, principalmente quando a vítima é uma pessoa ou ente público. Então, desde o início, a criminalidade virtual sempre foi o maior receio da sociedade, e, consequentemente, um objeto de atenção aos profissionais do direito penal e dos legisladores. A partir dessa temática, começou-se a discutir quais os direitos e deveres consequentes ao uso da internet para definir o que se pode ou não fazer na web (MARCACINI, 2016, p. 727).

O Marco Civil da Internet, que também ficou conhecido como a “Constituição da Internet”, foi criado para preencher essa lacuna do Direito brasileiro no que tange o uso da internet. Para que o projeto de lei fosse criado, o Ministério da Justiça contou com a colaboração de diferentes setores do corpo social, e também com a participação direta dos civis, tudo para que se pudesse chegar em um consenso que abrange a maior parte possível dos interessados. Referida lei veio para determinar os rumos a serem seguidos no que tange o uso da rede no Brasil (O QUE É O MARCO CIVIL [...], 2014).

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 também direciona 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.*

O princípio da neutralidade da rede define que na internet não se pode ter “pedágios”, o que quer dizer que nenhum provedor pode estabelecer obstáculos no acesso a qualquer tipo de conteúdo com intenções financeiras. Ou seja, não podem criar um plano que cobre um valor x apenas para utilizar, por exemplo, o e-mail, e restringir o acesso a outros tipos de conteúdo como o Youtube ou a Netflix. As empresas provedoras sustentam que tal neutralidade extingue as possibilidades de serem criados pacotes mais baratos. Em contrapartida, os defensores aduzem que, caso não fosse aprovada a medida, esta seria objeto de exclusão social, impedindo o acesso dos menos favorecidos a todos os tipos de conteúdo (SANTINO, 2014)

Em se tratando da privacidade dos usuários, a lei aduz que os dados das conexões devem ser resguardados pelo período de um ano pelos provedores em ambiente seguro. Além disso, estes só serão obrigados a prover as informações dos utilizadores através de ordem judicial. A lei também garante que as informações que os usuários colocaram na rede não devem ser usadas para outros fins que não seja sua usabilidade inicial pretendida, visto que esses dados podem ser armazenados e vendidos muito rapidamente para outros fins.

No mais, 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 censura caso 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).

Há poucas décadas era muito difícil uma pessoa normal conseguir atingir um público maior do que os indivíduos ao seu redor, isso porque precisava de uma gráfica de jornais ou por meios das ondas de rádio e televisão, todos inacessíveis para grande parte da população. Com a revolução digital, as pessoas conseguiram essa proeza, pois conseguem expressar sua opinião para o mundo inteiro através de qualquer simples e barato smartphone. Por isso se fazia necessária uma lei que assegurasse tais direitos.

Enfim, o Marco Civil representa importantes avanços positivando as relações que se dão através da internet, garantindo a democracia, a liberdade de expressão e todos os demais institutos por ela resguardados.

4.3 PROJETOS DE LEI EM ANDAMENTO

Por se tratar de um tema relativamente novo, precisamos também de novas reformas normativas a fim de que esta lacuna seja preenchida. E, nesse sentido, temos alguns interessantes projetos de lei em tramitação, conforme veremos a seguir.

O PL n. 5555/2013, cujo autor é o Deputado Federal João Arruda, visa identificar a invasão da privacidade feminina como um tipo de violência doméstica e familiar. O mesmo projeto altera a Lei Maria da Penha e tipifica a exposição pública da intimidade da mulher, elaborando métodos para reprovar comportamentos ofensivos contra estas na rede. O projeto foi recentemente aprovado sem objeções, agora deve ser votado no Senado e sancionado pelo presidente.

O PL n. 6989/2017, também de autoria do Deputado Federal João Arruda, visa alterar 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”.

O PL n. 154/2019, de autoria do Deputado Federal José Nelto, visa alterar 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.

5 CONCLUSÃO

Não obstante às legislações discutidas, com as normas que temos hoje, o país ainda não tem estrutura para regularizar a utilização da internet de forma eficaz. Temos muitos pontos abrangidos neste tema, como o econômico, social e político.

É sabido que a grande maioria, senão todas as empresas privadas e também os órgãos públicos, não tem tecnologia e nem conhecimento o bastante para assegurar a segurança no mundo virtual sequer de seus próprios servidores, quiçá das informações compartilhadas na internet de modo geral.

Em várias das situações apresentadas pudemos confirmar alguns dos fatos que atestam tal afirmação. No entanto, há mais um ponto que deve ser discutido, que é a carência de leis que possam assegurar ameaças imprevisíveis e também novas ameaças que podem chegar no Brasil.

O máximo que fizemos até hoje foi legislar sobre matérias que aconteceram em fatos (nem tanto) isolados, que classificaram como crime ações especificas, como por exemplo a Lei Carolina Dieckmann, que versa sobre a invasão de dispositivos eletrônicos, entre outras leis.

O Direito não consegue acompanhar a dinâmica da criminalidade, pois temos um protocolo a se cumprir que é distinto das transformações que ocorrem no âmbito da sociedade da informação. E, levando em consideração que as tecnologias se desenvolvem e crescem muito rápido, torna-se praticamente impossível tipificar alguns delitos que ainda não foram praticados.

Sendo assim, não tendo respaldo legal, inviabiliza um comportamento eficiente frente aos acontecimentos. Como por exemplo quando um novo vírus é lançado ou alguma forma de ludibriar as pessoas digitalmente é inventada, fazendo com que continuemos navegando sob frequentes ameaças.

6 REFERÊNCIAS

AMARAL, Amilcar do. O Marco Civil da Internet. *Pereira da Costa Advogados*, 12 set. 2016. Disponível em: https://pereiradacostaadvogados.com.br/artigos/32/o-marco-civil-da-internet. Acesso em: 20 out. 2020.

BERNAL, Ana. Crimes contra a honra na internet. *Jornal Estado de Minas*, 15 nov. 2019. Disponível em: https://www.em.com.br/app/noticia/direito-e-justica/2019/11/15/interna_direito_e_justica,1101173/crimes-contra-a-honra-na-internet.shtml. Acesso em: 15 out. 2020.

BITTENCOURT, Luís. *Crimes no universo digital*: sobre os crimes praticados na internet. Porto Alegre: [*s. n.*], 2019. *E-book.* Disponível em: https://ler.amazon.com.br/?asin=B08C3VR53C. Acesso em: 20 out. 2020.

BRASIL. *Código Penal*. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-lei/Del2848compilado.htm. Acesso em: 13 out. 2020.

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 preconceito de raça 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. 2020.

BRASIL. *Lei nº 11.829, de 25 de novembro de 2008*. Altera a Lei no 8.069, de 13 de julho de 1990 - 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. 2020.

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.

BRITO, Auriney *Direito penal informático*. São Paulo: Saraiva, 2013. *E-book.* Disponível em: https://ler.amazon.com.br/?asin=B076C12MP9. Acesso em: 20 out. 2020.

CAMPANHOLA, Nadine Finoti. Crimes Virtuais Contra a Honra. C*onteúdo Jurídico*, 17 abr. 2018. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/51558/crimes-virtuais-contra-a-honra. Acesso em: 30 out. 2020.

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. 2020.

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. 2020.

CRIMES cibernéticos disparam e expõem fragilidade tecnológica no Brasil. *Jornal Estado de Minas*, 04 ago. 2019. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crimes-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 30 out. 2020.

DELMANTO, Celso *et al*. *Código Penal Comentado*. 9. ed. rev., atual e ampl. São Paulo: Saraiva, 2016. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502634633/cfi/0. Acesso em: 10 out. 2020.

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. 2020.

GOUVÊA, Sandra. *O Direito Na Era Digital*: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. Disponível em: https://books.google.com.br/books?id=3vzmW3DtAuQC&printsec=frontcover&dq=inauthor:%22Sandra+Gouv%C3%AAa%22&hl=pt-BR&sa=X&ved=2ahUKEwilwPP9nbDsAhUSHbkGHZegCaUQ6AEwAHoECAAQAg#v=onepage&q&f=false. Acesso em: 30 out. 2020.

INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*. 2. ed. atual. e ampl. São Paulo: Juarez de Oliveira, 2009.

JESUS, Damasio de; MILAGRE, José Antonio. *Manual de Crimes Informáticos* – São Paulo: Saraiva, 2016. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627253/cfi/4!/4/4@0.00:14.3. Acesso em: 15 out. 2020.

KUMMER, Fabiano R. *Direito Penal na Sociedade da Informação*. Paraná: Edição do autor, 2017. *E-book*. Disponível em: https://ler.amazon.com.br/?asin=B07478RC4M. Acesso em: 30 out. 2020.

MARCACINI, Augusto Tavares Rosa. *Aspectos Fundamentais do Marco Civil da Internet*: Lei nº 12.965/2014. São Paulo: Edição do autor, 2016. Disponível em: https://ler.amazon.com.br/?asin=B06W9HZW7H. Acesso em: 20 out. 2020.

MASSON, Cleber. *Direito Penal Esquematizado*. 7. ed. rev, atual. e ampl. São Paulo: Método, 2015. v. 2. Disponível em: https://2014direitounic.files.wordpress.com/2016/02/cleber-masson-direito-penal-esquematizado-vol-2-20152.pdf. Acesso em: 20 out. 2020.

NUCCI, Guilherme de Souza. *Curso de Direito Penal*: parte especial: arts. 121 a 212 do Código Penal. 3. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2018. *E-book*, v. 2. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530982973/cfi/6/4!/4/2@0:0. Acesso em: 15 out. 2020.

O QUE é o Marco Civil da Internet?. *Pensando o Direito*, 23 abr. 2014. Disponível em: http://pensando.mj.gov.br/2014/04/23/o-que-e-o-marco-civil-da-internet/. Acesso em: 30 out. 2020.

PINHEIRO, Patricia Peck. *Direito Digital*. 6. ed. rev., ampl. e atual. São Paulo: Saraiva, 2016. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502635647/cfi/17!/4/4@0.00:0.00. Acesso em: 10 out. 2020.

REALE, Miguel. *Lições Preliminares de Direito*. 27. ed. rev. e atual. ajustada ao novo Código Civil. São Paulo: Saraiva, 2004.

SANTINO, Renato. Saiba o que é a "neutralidade da rede" defendida no Marco Civil. *Olhar Digital*, 25 mar. 2014. Disponível em: https://olhardigital.com.br/noticia/41035/41035. Acesso em: 25 out. 2020.

SYDOW, Spencer Toth. *Crimes Informáticos e Suas Vítimas* –2. ed. São Paulo: Saraiva, 2015. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502229495/cfi/0. Acesso em: 10 out. 2020.

SILVA, Rosane Leal da; VERONESE, Josiane Rose Petry. Os crimes sexuais contra crianças e adolescentes no ambiente virtual. *Âmbito Jurídico*, 01 nov. 2009. Disponível em: https://ambitojuridico.com.br/edicoes/revista-69/os-crimes-sexuais-contra-criancas-e-adolescentes-no-ambiente-virtual/. Acesso em: 15 out. 2020.

TEIXEIRA, Tarcísio. *Curso de Direito e Processo Eletrônico*: doutrina, jurisprudência e prática. 4. ed. atual. e ampl. São Paulo: Saraiva Educação, 2018. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553172740/cfi/505!/4/4@0.00:65.0. Acesso em: 10 out. 2020.

VALENTE, Jonas. Brasil tem 134 milhões de usuários de internet, aponta pesquisa, *Agência Brasil*, 26 maio 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa. Acesso em: 15 out. 2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos*: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2017. *E-book*, p. 21. Disponível em: https://ler.amazon.com.br/?asin=B01N9JNPLQ. Acesso em: 20 out. 2020.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Gabriel Augusto Gonçalves Lazzarini

Aluno(a), regularmente matriculado(a), no Curso de Direito, na disciplina do TCC da 10ª etapa, matrícula nº 31632467, Período Noturno, Turma S ,

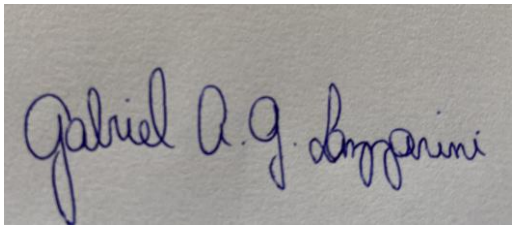
tendo realizado o TCC com o título: Crimes Virtuais: Uma análise sobre a carência de leis para combater suas especificidades.

sob a orientação do(a) professor(a): Thamara Duarte Cunha Medeiros

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 10 de Novembro de 2020.



Assinatura do discente